

Mediant™ 800 MSBG

Multi-Service Business Gateway

SIP Protocol

User's Manual



Version 6.2

February 2011

Document # LTRT-12804



Table of Contents

1	Overview	25
2	Configuration Concepts	27
2.1	Configuration Tools	27
2.2	Main Operating Modes	27
2.2.1	Operating in VoIP and Data-Routing Mode	27
2.2.1.1	Configuring Data-Routing LAN Interface	28
2.2.1.2	Configuring Device's DHCP Server	29
2.2.1.3	Assigning a WAN IP Address	29
2.2.1.4	Assign WAN Interface to VoIP Traffic	31
2.2.1.5	Configuring Quality of Service	32
2.2.1.6	Configuring Virtual Routing and Forwarding	38
2.2.1.7	Enabling Remote HTTP/S Web Management	39
2.2.2	Operating in VoIP-Only Mode	39
3	Web-Based Management	41
3.1	Getting Acquainted with the Web Interface	42
3.1.1	Computer Requirements	42
3.1.2	Accessing the Web Interface	42
3.1.3	Areas of the GUI	44
3.1.4	Toolbar	44
3.1.5	Navigation Tree	45
3.1.5.1	Displaying Navigation Tree in Basic and Full View	46
3.1.5.2	Showing / Hiding the Navigation Pane	47
3.1.6	Working with Configuration Pages	48
3.1.6.1	Accessing Pages	48
3.1.6.2	Viewing Parameters	49
3.1.6.3	Modifying and Saving Parameters	51
3.1.6.4	Entering Phone Numbers	52
3.1.6.5	Working with Tables	53
3.1.7	Searching for Configuration Parameters	54
3.1.8	Creating a Login Welcome Message	56
3.1.9	Getting Help	57
3.1.10	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	63
3.2.4	Viewing Trunk Channels	64
3.3	Configuration Tab	65
3.3.1	System Settings	65
3.3.1.1	Configuring Application Settings	65
3.3.1.2	Configuring NFS Settings	66
3.3.1.3	Configuring Syslog Settings	68
3.3.1.4	Configuring Regional Settings	69
3.3.1.5	Configuring Certificates	69
3.3.1.6	Management Settings	73
3.3.2	VoIP Settings	83
3.3.2.1	Network	83
3.3.2.2	TDM	94
3.3.2.3	Security	94
3.3.2.4	PSTN	98

3.3.2.5	Media.....	103
3.3.2.6	Services.....	112
3.3.2.7	Applications Enabling.....	113
3.3.2.8	Control Network.....	113
3.3.2.9	SIP Definitions.....	130
3.3.2.10	Coders and Profiles.....	138
3.3.2.11	GW and IP to IP	145
3.3.2.12	SBC	194
3.3.2.13	SAS	216
3.3.3	Data Settings	222
3.3.3.1	Getting Acquainted with Data Configuration Pages.....	223
3.3.3.2	WAN Access	224
3.3.3.3	Firewall and ACL.....	238
3.3.3.4	QoS	252
3.3.3.5	VPN	262
3.3.3.6	Data Services.....	270
3.3.3.7	Data Routing	276
3.3.3.8	Objects and Rules.....	283
3.3.3.9	Configuring Network Connections.....	287
3.4	Maintenance Tab	333
3.4.1	Maintenance	333
3.4.1.1	Maintenance Actions.....	333
3.4.2	Software Update	337
3.4.2.1	Loading Auxiliary Files	337
3.4.2.2	Loading Software Upgrade Key	339
3.4.2.3	Software Upgrade Wizard	341
3.4.2.4	Backing Up and Loading Configuration File.....	344
3.5	Status & Diagnostics Tab.....	346
3.5.1	System Status.....	346
3.5.1.1	Viewing Device Information.....	346
3.5.1.2	Viewing Ethernet Port Information	348
3.5.1.3	Viewing WAN Port Information.....	348
3.5.1.4	Carrier-Grade Alarms	349
3.5.2	VoIP Status.....	350
3.5.2.1	Viewing Active IP Interfaces.....	350
3.5.2.2	Viewing Performance Statistics.....	350
3.5.2.3	Viewing Call Counters.....	351
3.5.2.4	Viewing SAS/SBC Registered Users	353
3.5.2.5	Viewing Call Routing Status.....	354
3.5.2.6	Viewing Registration Status	354
3.5.2.7	Viewing IP Connectivity.....	356
3.5.3	Data Status	358
3.5.3.1	Viewing WAN Status	358
3.5.3.2	Viewing Network Connection Statistics.....	359
3.5.3.3	Viewing Logged Security Events.....	360
3.5.3.4	Viewing QoS Queues Statistics	362
3.5.3.5	Viewing Logged Data Events.....	363
3.5.3.6	Running Diagnostic Tests	365
4	INI File-Based Management.....	367
4.1	INI File Format	367
4.1.1	Configuring Individual ini File Parameters	367
4.1.2	Configuring ini File Table Parameters	368
4.1.3	General ini File Formatting Rules.....	370
4.2	Modifying an ini File	370
4.3	Secured Encoded ini File	371

5	EMS-Based Management.....	373
5.1	Familiarizing yourself with EMS GUI.....	373
5.2	Adding the Device in EMS	374
5.3	Configuring Trunks.....	376
5.3.1	General Trunk Configuration	376
5.3.2	Configuring ISDN NFAS	377
5.4	Configuring Basic SIP Parameters.....	380
5.5	Provisioning SIP SRTP Crypto Offered Suites.....	382
5.6	Provisioning SIP MLPP Parameters	382
5.7	Configuring the Device to Operate with SNMPv3	383
5.7.1	Configuring SNMPv3 using SSH.....	384
5.7.2	Configuring EMS to Operate with a Pre-configured SNMPv3 System.....	385
5.7.3	Configuring SNMPv3 to Operate with Non-Configured SNMPv3 System.....	386
5.7.4	Cloning SNMPv3 Users	387
5.8	Resetting the Device	387
5.9	Upgrading the Device's Software	388
6	Restoring Factory Default Settings	391
6.1	Restoring Defaults using CLI	391
6.2	Restoring Defaults using an ini File.....	392
6.3	Restoring Defaults using Hardware Reset Button.....	392
7	Auxiliary Configuration Files	393
7.1	Call Progress Tones File.....	393
7.1.1	Distinctive Ringing	396
7.1.2	FXS Distinctive Ringing and Call Waiting Tones per Source/Destination Number.....	398
7.2	Prerecorded Tones File.....	399
7.3	CAS Files	399
7.4	Dial Plan File	400
7.5	User Information File.....	402
8	IP Telephony Capabilities.....	405
8.1	Multiple SIP Signaling and Media Interfaces.....	405
8.1.1	Signaling Routing Domains	405
8.1.1.1	Media Realms	406
8.1.1.2	SIP Interfaces.....	406
8.1.2	Multiple SIP Signaling and Media Configuration Example	408
8.2	Dynamic Jitter Buffer Operation	412
8.3	Gateway and IP-to-IP	413
8.3.1	Dialing Plan Features	413
8.3.1.1	Dialing Plan Notation for Routing and Manipulation	413
8.3.1.2	Digit Mapping	414
8.3.1.3	External Dial Plan File.....	415
8.3.1.4	Dial Plan Prefix Tags for IP-to-Tel Routing	418
8.3.2	Manipulating Number Prefix	419
8.3.3	Emergency Phone Number Services - E911	420
8.3.3.1	FXS Device Emulating PSAP using DID Loop-Start Lines	421

8.3.3.2	FXO Device Interworking SIP E911 Calls from Service Provider's IP Network to PSAP DID Lines	424
8.3.3.3	Pre-empting Existing Calls for E911 IP-to-Tel Calls	427
8.3.4	Configuring DTMF Transport Types	428
8.3.5	FXS and FXO Capabilities	430
8.3.5.1	FXS/FXO Coefficient Types	430
8.3.5.2	FXO Operating Modes	430
8.3.5.3	Remote PBX Extension Between FXO and FXS Devices	437
8.3.6	Configuring Alternative Routing (Based on Connectivity and QoS)	442
8.3.6.1	Alternative Routing Mechanism	442
8.3.6.2	Determining the Availability of Destination IP Addresses	442
8.3.6.3	PSTN Fallback	442
8.3.7	Fax and Modem Capabilities	443
8.3.7.1	Fax/Modem Operating Modes	443
8.3.7.2	Fax/Modem Transport Modes	443
8.3.7.3	V.34 Fax Support	449
8.3.7.4	V.152 Support	452
8.3.8	Working with Supplementary Services	453
8.3.8.1	Call Hold and Retrieve	453
8.3.8.2	BRI Suspend and Resume	455
8.3.8.3	Consultation Feature	455
8.3.8.4	Call Transfer	456
8.3.8.5	Call Forward	457
8.3.8.6	Call Waiting	460
8.3.8.7	Message Waiting Indication	461
8.3.8.8	Caller ID	463
8.3.8.9	Three-Way Conferencing	465
8.3.8.10	Multilevel Precedence and Preemption	467
8.3.9	SIP Call Routing Examples	469
8.3.9.1	SIP Call Flow Example	469
8.3.9.2	SIP Authentication Example	471
8.3.9.3	Establishing a Call between Two Devices	474
8.3.9.4	SIP Trunking between Enterprise and ITSPs	475
8.3.10	Mapping PSTN Release Cause to SIP Response	478
8.3.11	Querying Device Channel Resources using SIP OPTIONS	479
8.4	SBC Application	480
8.4.1	Overview	480
8.4.1.1	NAT Traversal	481
8.4.1.2	VoIP Firewall	481
8.4.1.3	Topology Hiding	481
8.4.1.4	SIP Normalization	482
8.4.1.5	Survivability	482
8.4.2	SIP Network Definitions	482
8.4.3	SIP Dialog Initiation Process	482
8.4.3.1	Determining Source and Destination URL	483
8.4.3.2	Source IP Group Classification	484
8.4.3.3	SBC IP-to-IP Routing	485
8.4.3.4	IP-to-IP Inbound and Outbound Manipulation	486
8.4.3.5	SIP Header Manipulation	488
8.4.4	User Registration and Internal Database	490
8.4.4.1	Initial Registration Request Processing	490
8.4.4.2	Internal Database	491
8.4.4.3	Routing using Internal Database	492
8.4.4.4	Registration Refreshes	492
8.4.4.5	Registration Restriction Control	492
8.4.5	SBC Media Handling	493
8.4.5.1	Media Anchoring without Transcoding (Transparent)	494
8.4.5.2	Media Anchoring with Transcoding	495
8.4.5.3	No Media Anchoring	497

8.4.5.4	Interworking DTMF Methods	498
8.4.5.5	Transcoding Modes	499
8.4.5.6	Coder Restrictions Control	499
8.4.5.7	SRTP-RTP Transcoding	501
8.4.5.8	Multiple RTP Media Streams per Call Session	502
8.4.6	SIP Dialog Admission Control	502
8.4.7	Handling SIP 3xx Redirect Responses	503
8.4.8	Interworking SIP Diversion and History-Info Headers	505
8.4.9	SIP Message Manipulation Syntax	506
8.4.9.1	Actions	506
8.4.9.2	Supported Header Types	506
8.4.9.3	Structure Definitions	529
8.4.9.4	Enum Definitions	531
8.4.9.5	Actions and Types	537
8.4.9.6	Syntax	541
8.4.10	SBC Configuration Example	546
8.4.10.1	General SBC Setup	546
8.4.10.2	Survivability and Alternative Routing	556
8.4.10.3	SBC-to-PSTN Routing	560
8.4.10.4	Basic Coder Transcoding	568
8.4.10.5	Advanced Coder Transcoding	570
8.4.10.6	RTP-SRTP Transcoding	576
8.4.10.7	SIP URI Manipulation	578
8.4.10.8	SIP Header Manipulation	579
8.5	Stand-Alone Survivability (SAS) Application	582
8.5.1	SAS Operating Modes	582
8.5.1.1	SAS Outbound Mode	583
8.5.1.2	SAS Redundant Mode	584
8.5.2	SAS Routing	586
8.5.2.1	SAS Routing in Normal State	587
8.5.2.2	SAS Routing in Emergency State	589
8.5.3	SAS Configuration	590
8.5.3.1	General SAS Configuration	590
8.5.3.2	Configuring SAS Outbound Mode	593
8.5.3.3	Configuring SAS Redundant Mode	594
8.5.3.4	Configuring Gateway Application with SAS	594
8.5.3.5	Advanced SAS Configuration	598
8.5.4	Viewing Registered SAS Users	604
8.6	Routing Based on LDAP Active Directory Queries	605
8.6.1	LDAP Overview	605
8.6.2	AD-Based Tel-to-IP Routing in Microsoft OCS 2007 Environment	606
8.7	General	608
8.7.1	Transcoding using Third-Party Call Control	608
8.7.1.1	Using RFC 4117	608
8.7.2	Supported RADIUS Attributes	609
8.7.3	Call Detail Record	611
8.7.3.1	CDR Fields	611
8.7.3.2	Release Reasons in CDR	612
9	VoIP Networking Capabilities	617
9.1	NAT (Network Address Translation) Support	617
9.1.1	First Incoming Packet Mechanism	617
9.1.2	No-Op Packets	618
9.2	Robust Receipt of Media Streams	618
9.3	Multiple Routers Support	619

9.4	Simple Network Time Protocol Support	619
9.5	Network Configuration.....	620
9.5.1	Multiple Network Interfaces and VLANs	620
9.5.1.1	Overview of Multiple Interface Table.....	621
9.5.1.2	Columns of the Multiple Interface Table.....	622
9.5.1.3	Other Related Parameters	624
9.5.1.4	Multiple Interface Table Configuration Summary and Guidelines.....	627
9.5.1.5	Troubleshooting the Multiple Interface Table.....	628
9.5.2	Static Routing Table	628
9.5.2.1	Routing Table Overview.....	628
9.5.2.2	Routing Table Columns.....	629
9.5.2.3	Routing Table Configuration Summary and Guidelines.....	630
9.5.2.4	Troubleshooting the Routing Table	631
9.5.3	Setting Up VoIP Networking	631
9.5.3.1	Using the Web Interface.....	631
9.5.3.2	Using the ini File.....	631
9.5.3.3	Networking Configuration Examples	633
10	Advanced PSTN Configuration	637
10.1	Clock Settings	637
10.1.1	Recovering Clock from PSTN Line Interface.....	637
10.1.2	Configuring Internal Clock as Clock Source.....	638
10.2	Release Reason Mapping.....	638
10.2.1	Reason Header.....	638
10.2.2	Fixed Mapping of ISDN Release Reason to SIP Response.....	639
10.2.3	Fixed Mapping of SIP Response to ISDN Release Reason.....	641
10.3	ISDN Overlap Dialing	642
10.4	ISDN Non-Facility Associated Signaling (NFAS)	643
10.4.1	NFAS Interface ID.....	644
10.4.2	Working with DMS-100 Switches	644
10.4.3	Creating an NFAS-Related Trunk Configuration	645
10.5	Redirect Number and Calling Name (Display)	646
10.6	Automatic Gain Control (AGC).....	646
11	Tunneling Applications.....	647
11.1	TDM Tunneling.....	647
11.1.1	DSP Pattern Detector	650
11.2	QSIG Tunneling	650
12	Configuration Parameters Reference	653
12.1	Networking Parameters.....	653
12.1.1	VoIP Multiple Network Interfaces and VLAN Parameters	653
12.1.2	VoIP Static Routing Parameters.....	654
12.1.3	Quality of Service Parameters.....	655
12.1.4	NAT Parameters	657
12.1.5	NFS Parameters	658
12.1.6	DNS Parameters.....	659
12.1.7	DHCP Parameters	660
12.1.8	NTP and Daylight Saving Time Parameters.....	661
12.2	Web and Telnet Parameters	662
12.2.1	General Parameters	662
12.2.2	Web Parameters.....	663
12.2.3	Telnet Parameters	664

12.3	Debugging and Diagnostics Parameters.....	665
12.3.1	General Parameters	665
12.3.2	Syslog, CDR and Debug Parameters.....	666
12.3.3	Remote Alarm Indication Parameters.....	669
12.3.4	Serial Parameters	670
12.4	Security Parameters.....	671
12.4.1	General Parameters	671
12.4.2	HTTPS Parameters	672
12.4.3	SRTP Parameters.....	673
12.4.4	TLS Parameters.....	674
12.4.5	SSH Parameters.....	676
12.4.6	OCSP Parameters	677
12.5	RADIUS Parameters	677
12.6	SNMP Parameters	679
12.7	SIP Media Realm Parameters.....	682
12.8	Control Network Parameters.....	683
12.8.1	IP Group, Proxy, Registration and Authentication Parameters	683
12.8.2	Network Application Parameters	696
12.9	General SIP Parameters	698
12.10	Coders and Profile Parameters.....	721
12.11	Channel Parameters	731
12.11.1	Voice Parameters	731
12.11.2	Coder Parameters	733
12.11.3	Fax and Modem Parameters	734
12.11.4	DTMF Parameters	739
12.11.5	RTP, RTCP and T.38 Parameters.....	740
12.12	Gateway and IP-to-IP Parameters	743
12.12.1	Fax and Modem Parameters	743
12.12.2	DTMF and Hook-Flash Parameters.....	745
12.12.3	Digit Collection and Dial Plan Parameters.....	750
12.12.4	Voice Mail Parameters.....	753
12.12.5	Supplementary Services Parameters	757
12.12.5.1	Caller ID Parameters.....	757
12.12.5.2	Call Waiting Parameters.....	762
12.12.5.3	Call Forwarding Parameters	765
12.12.5.4	Message Waiting Indication Parameters.....	767
12.12.5.5	Call Hold Parameters	769
12.12.5.6	Call Transfer Parameters	770
12.12.5.7	Three-Way Conferencing Parameters	772
12.12.5.8	Emergency Call Parameters	773
12.12.5.9	Call Cut-Through Parameters	774
12.12.5.10	Automatic Dialing Parameters	775
12.12.5.11	Direct Inward Dialing Parameters.....	776
12.12.5.12	MLPP Parameters	777
12.12.5.13	ISDN BRI Parameters	781
12.12.6	PSTN Parameters.....	783
12.12.6.1	General Parameters	783
12.12.6.2	TDM Bus and Clock Timing Parameters.....	787
12.12.6.3	CAS Parameters	789
12.12.6.4	ISDN Parameters	792
12.12.7	ISDN and CAS Interworking Parameters	799
12.12.8	Answer and Disconnect Supervision Parameters	817
12.12.9	Tone Parameters	821
12.12.9.1	Telephony Tone Parameters.....	821

12.12.9.2	Tone Detection Parameters	826
12.12.9.3	Metering Tone Parameters	828
12.12.10	Telephone Keypad Sequence Parameters	829
12.12.11	General FXO Parameters.....	833
12.12.12	FXS Parameters	835
12.12.13	Hunt Groups, Number Manipulation and Routing Parameters	836
12.12.13.1	Hunt Groups and Routing Parameters	836
12.12.13.2	Alternative Routing Parameters.....	843
12.12.13.3	Number Manipulation Parameters.....	847
12.12.13.4	LDAP Parameters.....	857
12.13	SBC Parameters	858
12.14	Standalone Survivability Parameters	873
12.15	IP Media Parameters	878
12.16	Auxiliary and Configuration Files Parameters	881
12.16.1	Auxiliary/Configuration File Name Parameters.....	881
12.16.2	Automatic Update Parameters	882
13	SIP Software Package	885
14	Technical Specifications	887

List of Figures

Figure 1-1: Typical Application	26
Figure 2-1: Connections Page.....	28
Figure 2-2: Defining LAN Data Routing IP Address	28
Figure 2-3: Configuring the DHCP Server.....	29
Figure 2-4: Selecting WAN Connection.....	30
Figure 2-5: Selecting WAN Interface for VoIP Traffic.....	31
Figure 2-6: Assigning SIP Interface to WAN	31
Figure 2-7: Assigning WAN Interface to Media Realm.....	32
Figure 2-8: Traffic Shaping Page	32
Figure 2-9: Selecting Device for Traffic Shaping.....	33
Figure 2-10: Defining Traffic Shaping.....	33
Figure 2-11: Adding Class Rule	33
Figure 2-12: Defining Shaping Class (for VoIP Tx Traffic)	34
Figure 2-13: Configured Traffic Shaping for Total WAN and VoIP Bandwidth.....	34
Figure 2-14: Match Rules Page.....	35
Figure 2-15: Adding a Traffic Priority Rule	36
Figure 2-16: Defining Incoming SIP Ports	36
Figure 2-17: Defining SIP Ports (e.g. TCP).....	36
Figure 2-18: Configured Ports for Incoming SIP	37
Figure 2-19: Traffic Matching Rule for Received SIP Signaling Traffic.....	37
Figure 2-20: Matching Rule for Received RTP Traffic	38
Figure 2-21: Traffic Matching Rule for WAN Tx/Rx RTP and SIP Signaling.....	38
Figure 2-22: Defining WAN HTTP Port	39
Figure 2-23: Removing Data-Routing Connection Interface	39
Figure 2-24: Multiple Interface Table.....	40
Figure 2-25: Multiple Interfaces with VLANs	40
Figure 2-26: Defining VLANs per LAN Port.....	40
Figure 3-1: Login Screen.....	43
Figure 3-2: Areas of the Web Interface GUI.....	44
Figure 3-3: "Reset" Displayed on Toolbar	45
Figure 3-4: Navigation Tree.....	46
Figure 3-5: Toggling Between Navigation Tree Views	47
Figure 3-6: Show / Hide Navigation Tree	48
Figure 3-7: Toggling between Basic and Advanced View.....	50
Figure 3-8: Expanding and Collapsing Parameter Groups	51
Figure 3-9: Edit Symbol after Modifying Parameter Value	51
Figure 3-10: Value Reverts to Previous Valid Value	52
Figure 3-11: Adding an Index Entry to a Table	53
Figure 3-12: Compacting a Web Interface Table	54
Figure 3-13: Searched Result Screen	55
Figure 3-14: User-Defined Web Welcome Message after Login.....	56
Figure 3-15: Help Topic for Current Page	57
Figure 3-16: Log Off Confirmation Box.....	58
Figure 3-17: Web Session Logged Off.....	58
Figure 3-18: Home Page	59
Figure 3-19: Shortcut Menu for Assigning Port Name	62
Figure 3-20: Text Box for Entering Port Name.....	62
Figure 3-21: Shortcut Menu for Resetting Port.....	62
Figure 3-22: Shortcut Menu for Viewing Port Information	63
Figure 3-23: Basic Information Screen.....	63
Figure 3-24: Trunks and Channels Status Screen	64
Figure 3-25: Applications Settings Page	65
Figure 3-26: NFS Settings Page	66
Figure 3-27: Syslog Settings Page.....	68
Figure 3-28: Regional Settings Page	69
Figure 3-29: Certificates Signing Request Page	70

Figure 3-30: WEB User Accounts Page (for Users with 'Security Administrator' Privileges)	74
Figure 3-31: Web Security Page	76
Figure 3-32: Telnet/SSH Settings Page	76
Figure 3-33: Web & Telnet Access List Page - Add New Entry	77
Figure 3-34: Web & Telnet Access List Table	77
Figure 3-35: RADIUS Parameters Page	78
Figure 3-36: SNMP Community String Page	79
Figure 3-37: SNMP Trap Destinations Page	80
Figure 3-38: SNMP Trusted Managers	81
Figure 3-39: SNMP V3 Setting Page	81
Figure 3-40: Multiple Interface Table Page	84
Figure 3-41: IP Routing Table Page	88
Figure 3-42: DiffServ Table Page	90
Figure 3-43: DNS Settings Page	91
Figure 3-44: Internal DNS Table Page	92
Figure 3-45: Internal SRV Table Page	93
Figure 3-46: TDM Bus Settings Page	94
Figure 3-47: Firewall Settings Page	95
Figure 3-48: General Security Settings Page	98
Figure 3-49: CAS State Machine Page	99
Figure 3-50: Trunk Scroll Bar (Used Only as an Example)	101
Figure 3-51: Trunk Scroll Bar (Used Only as an Example)	102
Figure 3-52: Voice Settings Page	104
Figure 3-53: Fax/Modem/CID Settings Page	105
Figure 3-54: RTP/RTCP Settings Page	106
Figure 3-55: IPMedia Settings Page	107
Figure 3-56: General Media Settings Page	108
Figure 3-57: Analog Settings Page	108
Figure 3-58: SIP Media Realm Table Page	109
Figure 3-59: Media Security Page	111
Figure 3-60: LDAP Settings Page	112
Figure 3-61: Applications Enabling Page	113
Figure 3-62: SRD Settings Page	115
Figure 3-63: SIP Interface Table Page	118
Figure 3-64: IP Group Table	120
Figure 3-65: Proxy Sets Table Page	126
Figure 3-66: SIP General Parameters Page	131
Figure 3-67: SIP General Parameters Page	132
Figure 3-68: Account Table Page	133
Figure 3-69: Proxy & Registration Page	137
Figure 3-70: Coders Page	139
Figure 3-71: Code Group Settings Page	140
Figure 3-72: Tel Profile Settings Page	142
Figure 3-73: IP Profile Settings Page	144
Figure 3-74: Hunt Group Table Page	146
Figure 3-75: Hunt Group Settings Page	148
Figure 3-76: General Settings Page	151
Figure 3-77: Source Phone Number Manipulation Table for Tel-to-IP Calls	153
Figure 3-78: Redirect Number IP to Tel Page	157
Figure 3-79: Redirect Number Tel to IP Page	159
Figure 3-80: Phone Context Table Page	160
Figure 3-81: Release Cause Mapping Page	163
Figure 3-82: Routing General Parameters Page	164
Figure 3-83: Locating SRD	166
Figure 3-84: Outbound IP Routing Table Page	168
Figure 3-85: Inbound IP Routing Table	172
Figure 3-86: Reasons for Alternative Routing Page	175
Figure 3-87: Forward on Busy Trunk Destination Page	176
Figure 3-88: DTMF & Dialing Page	177

Figure 3-89: Supplementary Services Page.....	178
Figure 3-90: Keypad Features Page	180
Figure 3-91: Metering Tones Page.....	181
Figure 3-92: Charge Codes Table Page	182
Figure 3-93: FXO Settings Page	183
Figure 3-94: Authentication Page.....	184
Figure 3-95: Automatic Dialing Page.....	185
Figure 3-96: Caller Display Information Page	186
Figure 3-97: Call Forward Table Page	187
Figure 3-98: Caller ID Permissions Page	188
Figure 3-99: Caller Waiting Page	189
Figure 3-100: Digital Gateway Parameters Page.....	190
Figure 3-101: ISDN Supp Services Table Page.....	192
Figure 3-102: ISDN Supp Services Table Page.....	193
Figure 3-103: General Settings Page.....	194
Figure 3-104: Admission Control Page	195
Figure 3-105: Allowed Coders Group Page	198
Figure 3-106: Classification Table Page	199
Figure 3-107: IP2IP Routing Table Page	202
Figure 3-108: Alternative Routing Reasons Page.....	206
Figure 3-109: Message Manipulations Page.....	207
Figure 3-110: IP to IP Inbound Manipulation Page	210
Figure 3-111: IP to IP Outbound Manipulation Page	213
Figure 3-112: SAS Configuration Page.....	217
Figure 3-113: IP2IP Routing Page	218
Figure 3-114: Working with Tables.....	223
Figure 3-115: Checkbox for Temporarily Disabling Entry	223
Figure 3-116: WAN Access	225
Figure 3-117: Manual WAN Connection.....	226
Figure 3-118: PPPoE WAN Connection.....	226
Figure 3-119: PPTP WAN Connection Type.....	226
Figure 3-120: L2TP WAN Connection Type.....	227
Figure 3-121: WAN Access Page for T1 WAN Interface.....	228
Figure 3-122: PPP Over T1	228
Figure 3-123: Settings Tab for PPP over T1	229
Figure 3-124: PPP Tab.....	229
Figure 3-125: T1 Tab.....	230
Figure 3-126: WAN Access Page for T1 WAN Interface.....	230
Figure 3-127: HDLC Over T1	231
Figure 3-128: Settings Tab HDLC over T1.....	231
Figure 3-129: WAN Access Page for T1 WAN Interface.....	232
Figure 3-130: MLP over T1 WAN	232
Figure 3-131: Settings Tab for MLP over T1	233
Figure 3-132: PPP Tab for MLP over T1 WAN	233
Figure 3-133: T1 Tab.....	234
Figure 3-134: SHDSL Line Mode Page.....	235
Figure 3-135: Adding a New Group.....	236
Figure 3-136: SHDSL RJ-45 Wire Pinouts	236
Figure 3-137: Protocol Interface Settings Page	237
Figure 3-138: Choosing Internet Connection Type	237
Figure 3-139: Configuring Internet Connection	237
Figure 3-140: Device's Firewall (Example).....	238
Figure 3-141: Configuring General Security.....	240
Figure 3-142: Configuring LAN Restriction Rules	241
Figure 3-143: Adding an Access Control Rule	241
Figure 3-144: Disabled LAN Restrictions - Cleared Check Box.....	242
Figure 3-145: Configuring Port Forwarding.....	243
Figure 3-146: Adding Port Forwarding Rule.....	243

Figure 3-147: Defining a DMZ Host.....	244
Figure 3-148: Configuring Port Triggering.....	245
Figure 3-149: Editing Port Triggering Rule.....	245
Figure 3-150: Defining Trigger Ports.....	245
Figure 3-151: Configuring Website Restrictions.....	246
Figure 3-152: Adding a Restricted Website.....	246
Figure 3-153: Configuring NAT	247
Figure 3-154: Defining Public IP Address	248
Figure 3-155: Defining NAT/NAPT Rule.....	248
Figure 3-156: Access Lists Table	249
Figure 3-157: Defining Access List Name	250
Figure 3-158: Adding an Access List Rules	250
Figure 3-159: Added Access List Rules	251
Figure 3-160: Advanced Filtering	252
Figure 3-161: Configuring General WAN Bandwidth	253
Figure 3-162: Configuring Traffic Priority	254
Figure 3-163: Adding a Traffic Priority Rule	255
Figure 3-164: Configuring Traffic Shaping	257
Figure 3-165: Adding Device for Traffic Shaping	257
Figure 3-166: Defining Device Traffic Shaping.....	258
Figure 3-167: Adding Tx Shaping Class.....	258
Figure 3-168: Class Name Added to Table	259
Figure 3-169: Defining Shaping Class.....	259
Figure 3-170: Configuring DSCP Settings.....	261
Figure 3-171: Defining DSCP to 802.1p Priority Mapping.....	261
Figure 3-172: Configuring 802.1p Settings.....	262
Figure 3-173: Configuring VPN IPsec.....	263
Figure 3-174: Recreating IPsec Public Key	263
Figure 3-175: IPsec Log Settings	264
Figure 3-176: Configuring VPN PPTP Server	265
Figure 3-177: Configuring VPN L2TP Server	266
Figure 3-178: Adding Users.....	267
Figure 3-179: Adding a New User	267
Figure 3-180: Defining Outgoing Mail Server.....	268
Figure 3-181: Adding Users.....	269
Figure 3-182: Adding a User Group	269
Figure 3-183: Configuring Dynamic DNS (DDNS) Services	270
Figure 3-184: Adding a DDNS.....	270
Figure 3-185: Configuring a DNS Server	272
Figure 3-186: Adding a DNS Server.....	272
Figure 3-187: Configuring DHCP Server.....	273
Figure 3-188: Defining IP Distribution Type	274
Figure 3-189: Defining DHCP Server Parameters	274
Figure 3-190: Defining DHCP Relay (DHCP for LAN Bridge).....	275
Figure 3-191: Defining DHCP Server's IP Address.....	275
Figure 3-192: Computers Recognized by DHCP Server.....	276
Figure 3-193: Defining New Static Connection (IP Address)	276
Figure 3-194: Configuring General Routing	278
Figure 3-195: Adding a Routing Rule	278
Figure 3-196: Editing the Default Route	279
Figure 3-197: Defining Load Balancing	279
Figure 3-198: Adding DSCP-Based Route.....	280
Figure 3-199: Defining Failover between WAN Devices	280
Figure 3-200: Page Displaying Area for Configuration File.....	282
Figure 3-201: Viewing Pre-defined Protocols.....	283
Figure 3-202: Adding a Service Protocol.....	284
Figure 3-203: Defining Service Server Ports.....	284
Figure 3-204: Configuring Network Objects	284
Figure 3-205: Defining Name for Network Object	285

Figure 3-206: Defining Network Object Type	285
Figure 3-207: Configuring Scheduler Rules	285
Figure 3-208: Defining Scheduler Rule Name.....	286
Figure 3-209: Defining Time Segment	286
Figure 3-210: Defining Hour Range	286
Figure 3-211: Configuring Network Connections	288
Figure 3-212: Defining a New Connection	288
Figure 3-213: Defining Internet Connection Type	289
Figure 3-214: Internet Connection Types.....	289
Figure 3-215: Defining Virtual Private Network over Internet.....	290
Figure 3-216: VPN Connection Types.....	290
Figure 3-217: Advanced Connection Wizard Tree	292
Figure 3-218: General Tab - LAN Switch	292
Figure 3-219: Switch Tab	293
Figure 3-220: Assigning VLAN to Port	293
Figure 3-221: Defining VLANs.....	293
Figure 3-222: STP Tab	294
Figure 3-223: Ethernet Connection Option.....	295
Figure 3-224: Selecting Internet Ethernet Connection	295
Figure 3-225: Internet Connection for External Cable Modem Added	296
Figure 3-226: Ethernet Connection Option.....	296
Figure 3-227: Selecting Internet Ethernet Connection	296
Figure 3-228: Manual IP Address Configuration	297
Figure 3-229: Manual WAN Ethernet Added Successfully.....	297
Figure 3-230: Defining Internet Connection Type	298
Figure 3-231: Selecting Underlying Device	298
Figure 3-232: Defining PPPoE Properties.....	298
Figure 3-233: PPPoE Connection Added Successfully.....	298
Figure 3-234: Selecting LAN Interfaces for Bridge Connection	300
Figure 3-235: LAN Bridge Successfully Added	301
Figure 3-236: Adding a VLAN Interface	301
Figure 3-237: Assigning VLAN to LAN Ports.....	302
Figure 3-238: VLAN Added Successfully	302
Figure 3-239: VLAN Interface Advanced Tab	303
Figure 3-240: Defining DSCP Remarkings.....	303
Figure 3-241: Defining PPTP Properties	304
Figure 3-242: PPTP Connection Added Successfully	304
Figure 3-243: Selecting VPN Type for IPSec	305
Figure 3-244: Selecting Protocol to Connect to Remote VPN Server.....	305
Figure 3-245: Defining PPTP VPN Properties.....	305
Figure 3-246: PPTP VPN Successfully Added.....	306
Figure 3-247: PPP Tab.....	306
Figure 3-248: PPTP Tab.....	307
Figure 3-249: VPN Connection Type	308
Figure 3-250: Selecting the VPN Protocol - PPTP Server	308
Figure 3-251: Defining Remote Client Address Range	308
Figure 3-252: PPTP Server Added Successfully	309
Figure 3-253: Editing VPN Server	309
Figure 3-254: Defining L2TP Properties.....	310
Figure 3-255: L2TP Connection Added Successfully.....	310
Figure 3-256: Selecting VPN Type for IPSec.....	311
Figure 3-257: Selecting L2TP to Connect to Remote VPN Server	311
Figure 3-258: Defining L2TP Properties.....	311
Figure 3-259: L2TP Successfully Added	312
Figure 3-260: PPP Tab.....	312
Figure 3-261: L2TP Tab	314
Figure 3-262: VPN Connection Type	314
Figure 3-263: Selecting L2TP Server VPN Protocol	314

Figure 3-264: Defining L2TP Properties	315
Figure 3-265: L2TP Server Added Successfully	315
Figure 3-266: Defining Advanced L2TP Properties	315
Figure 3-267: Selecting VPN Type for IPSec	316
Figure 3-268: Selecting IPSec	316
Figure 3-269: Defining IPSec Properties	317
Figure 3-270: IPSec Added Successfully	317
Figure 3-271: IPSec Tab	318
Figure 3-272: IPSec Tab - IPSec Automatic Phase 1	320
Figure 3-273: IPSec Tab - IPSec Automatic Phase 2	321
Figure 3-274: IPSec Tab - IPSec Manual	322
Figure 3-275: VPN Connection Type	322
Figure 3-276: VPN Protocols	323
Figure 3-277: IPSec Shared Secret Key	323
Figure 3-278: IPSec Connection Added Successfully	323
Figure 3-279: Configuring General IPIP Parameters	324
Figure 3-280: IPIP Added Successfully	324
Figure 3-281: IPIP Tab	325
Figure 3-282: Configuring General IPIP Parameters	325
Figure 3-283: GRE Connection Successfully Added	325
Figure 3-284: Editing GRE Remote Endpoint IP Address	326
Figure 3-285: Example Scenario Setup	327
Figure 3-286: Defining GRE Tunnel for Device A	327
Figure 3-287: Defining GRE Tunnel for Device B	328
Figure 3-288: Editing Network Connection - General Tab	329
Figure 3-289: Editing Network Connection - Settings Tab	329
Figure 3-290: Editing Network Connection - Routing Tab	331
Figure 3-291: Editing Network Connection - Advanced Tab	332
Figure 3-292: Maintenance Actions Page	333
Figure 3-293: Reset Confirmation Message Box	335
Figure 3-294: Device Lock Confirmation Message Box	335
Figure 3-295: Load Auxiliary Files Page	338
Figure 3-296: Software Upgrade Key Status Page	340
Figure 3-297: Software Upgrade Key with Multiple S/N Lines	341
Figure 3-298: Start Software Upgrade Wizard Screen	342
Figure 3-299: End Process Wizard Page	344
Figure 3-300: Configuration File Page	345
Figure 3-301: Device Information Page	347
Figure 3-302: Ethernet Port Information Page	348
Figure 3-303: WAN Port Information Page	349
Figure 3-304: Active Alarms Page	349
Figure 3-305: IP Interface Status Page	350
Figure 3-306: Basic Statistics Page	351
Figure 3-307: Calls Count Page	351
Figure 3-308: SAS/SBC Registered Users Page	353
Figure 3-309: Call Routing Status Page	354
Figure 3-310: Registration Status Page	355
Figure 3-311: IP Connectivity Page	356
Figure 3-312: WAN Status	358
Figure 3-313: Running Internet Connectivity Diagnostics Tests	359
Figure 3-314: Connection Statistics Page	360
Figure 3-315: Firewall - Log Page	360
Figure 3-316: Log Settings Page	361
Figure 3-317: QoS Queues Statistics Page	362
Figure 3-318: System Log Page	363
Figure 3-319: Adding a New Filter	364
Figure 3-320: System - Diagnostics Page	365
Figure 5-1: Areas of the EMS GUI	373
Figure 5-2: EMS Login Screen	374

Figure 5-3: Adding a Region.....	375
Figure 5-4: Defining the IP Address	375
Figure 5-5: DS1 Trunks List Table	376
Figure 5-6: Trunks Channels Table.....	376
Figure 5-7: General Settings Screen.....	377
Figure 5-8: EMS ISDN Settings Screen.....	378
Figure 5-9: SIP Protocol Definitions Frame.....	380
Figure 5-10: Authentication & Security Screen	382
Figure 5-11: MLPP Screen.....	383
Figure 5-12: MG Information Screen.....	385
Figure 5-13: SNMP Configuration Screen.....	386
Figure 5-14: Confirmation for Saving Configuration and Resetting Device	387
Figure 5-15: Software Manager Screen	388
Figure 5-16: Add Files Screen.....	388
Figure 5-17: Files Manager Screen.....	389
Figure 7-1: Example of a User Information File.....	402
Figure 8-1: Example Showing SIP Interfaces per Application within SRD.....	406
Figure 8-2: Back-to-Back SBC Call Flow (RTP and Signaling).....	407
Figure 8-3: Back-to-Back SBC Call Flow (RTP and Signaling).....	407
Figure 8-4: Multiple SIP Signaling/RTP Interfaces Example.....	408
Figure 8-5: Defining a Trunk Group for PSTN.....	409
Figure 8-6: Defining IP Interfaces.....	409
Figure 8-7: Defining Media Realms.....	409
Figure 8-8: Defining SRDs.....	410
Figure 8-9: Defining SIP Interfaces	410
Figure 8-10: Defining Proxy Set	410
Figure 8-11: Defining IP Groups.....	411
Figure 8-12: Defining IP-to-Trunk Group Routing	411
Figure 8-13: Defining Trunk Group to IP Group Routing.....	411
Figure 8-14: Configuring Dial Plan File Label for IP-to-Tel Routing.....	419
Figure 8-15: Configuring Manipulation for Removing Label.....	419
Figure 8-16: Prefix to Add Field with Notation.....	420
Figure 8-17: FXS Device Emulating PSAP using DID Loop-Start Lines.....	421
Figure 8-18: FXO Device Interfacing between E911 Switch and PSAP	424
Figure 8-19: Call Flow for One-Stage Dialing.....	431
Figure 8-20: Call Flow for Two-Stage Dialing.....	432
Figure 8-21: Call Flow for Automatic Dialing.....	434
Figure 8-22: Call Flow for Collecting Digits Mode	435
Figure 8-23: FXO-FXS Remote PBX Extension (Example)	438
Figure 8-24: MWI for Remote Extensions	439
Figure 8-25: Call Waiting for Remote Extensions	440
Figure 8-26: Assigning Phone Numbers to FXS Endpoints	440
Figure 8-27: Automatic Dialing for FXS Ports	440
Figure 8-28: FXS Tel-to-IP Routing Configuration	441
Figure 8-29: Assigning Phone Numbers to FXO Ports	441
Figure 8-30: FXO Automatic Dialing Configuration	441
Figure 8-31: FXO Tel-to-IP Routing Configuration.....	441
Figure 8-32: Double Hold SIP Call Flow.....	454
Figure 8-33: Call Forward Reminder with Application Server	458
Figure 8-34: SIP Call Flow.....	469
Figure 8-35: Assigning Phone Numbers to Device 10.2.37.10	474
Figure 8-36: Assigning Phone Numbers to Device 10.2.37.20	474
Figure 8-37: Routing Calls Between Devices.....	474
Figure 8-38: Routing between ITSP and Enterprise PBX Example	475
Figure 8-39: Configuring Proxy Set ID #1 in the Proxy Sets Table Page	476
Figure 8-40: Configuring IP Groups #1 and #2 in the IP Group Table Page	477
Figure 8-41: Assigning Channels to Hunt Groups.....	477
Figure 8-42: Configuring Registration Mode for Hunt Groups and Assigning to IP Group	477

Figure 8-43: Configuring Username and Password for Authenticating Channels 5-8	477
Figure 8-44: Configuring Account for Registration to ITSP 1	478
Figure 8-45: Configuring ITSP-to-Hunt Group Routin	478
Figure 8-46: Configuring Hunt Group to ITSP Routing	478
Figure 8-47: Routing Process.....	483
Figure 8-48: Classification Process (Identifying IP Group or Rejecting Call).....	485
Figure 8-49: IP-to-IP Routing Types.....	486
Figure 8-50: SIP URI Manipulation in IP-to-IP Routing	487
Figure 8-51: SIP INVITE (Manipulations) from LAN to WAN	488
Figure 8-52: SIP Header Manipulation Example	489
Figure 8-53: Blocking Incoming Calls from Unregistered Users	493
Figure 8-54: SDP Offer/Answer Example.....	495
Figure 8-55: Transcoding using Extended Coders (Example)	496
Figure 8-56: SBC SIP Signaling without RTP Media Flow	497
Figure 8-57: SIP 3xx Response Handling	504
Figure 8-58: SBC Example Scenario	547
Figure 8-59: Multiple Interface Table.....	547
Figure 8-60: Selecting WAN Interface for VoIP Traffic.....	548
Figure 8-61: Applications Enabling Page	549
Figure 8-62: Defining Number of SBC Sessions	549
Figure 8-63: LAN and WAN Media Realms in SIP Media Realm Table	550
Figure 8-64: SRDs for LAN and WAN in SRD Table	551
Figure 8-65: LAN and WAN SIP Interfaces in the SIP Interface Table	551
Figure 8-66: Proxy Sets Table Page	552
Figure 8-67: IP Group 1 (for Enterprise Users) in IP Group Table.....	553
Figure 8-68: IP Group 2 (for WAN ITSP) in IP Group Table	554
Figure 8-69: IP Group Classification Rule for LAN Users	555
Figure 8-70: IP-to-IP Routing Rules	556
Figure 8-71: Survivability Example Setup	557
Figure 8-72: Enabling Proxy Keep-Alive	558
Figure 8-73: Configuring IP-to-IP Routing Rules.....	559
Figure 8-74: SBC-to-PSTN Routing Example Setup	560
Figure 8-75: Configuring SIP Interface for PSTN (GW)	561
Figure 8-76: Defining Device as Proxy Set	562
Figure 8-77: Defining IP Group for PSTN Users	563
Figure 8-78: Dfining IP-to-IP Routing Rules	565
Figure 8-79: Defining Trunk Groups.....	566
Figure 8-80: Defining Channel Select Mode	567
Figure 8-81: Defining IP-to-Tel Routing Rules	568
Figure 8-82: Configuring the Coder Group.....	569
Figure 8-83: Configuring the IP Profile for Coder Transcoding	569
Figure 8-84: Defining IP Profile for USER IP Group	570
Figure 8-85: Advanced Transcoding Example Scenario	571
Figure 8-86: Defining Coder Group for LAN Users	571
Figure 8-87: Defining Coder Group for ITSP.....	572
Figure 8-88: Defining Allowed Coder Group	572
Figure 8-89: Defining IP Profile for LAN Users.....	573
Figure 8-90: Defining IP Profile for ITSP	574
Figure 8-91: Assigning IP Profile to LAN Users IP Group.....	575
Figure 8-92: Assigning IP Profile to ITSP IP Group	576
Figure 8-93: RTP-SRTP Transcoding Mode for LAN Users	577
Figure 8-94: RTP-to-SRTP Transcoding for ITSP.....	577
Figure 8-95: Manipulation of SIP URI Host Part.....	578
Figure 8-96: Manipulation of SIP URI User Part	579
Figure 8-97: SIP Header Manipulation Example	581
Figure 8-98: Assigning Manipulation Rule to IP Group	581
Figure 8-99: SAS Outbound Mode in Normal State (Example).....	583
Figure 8-100: SAS Outbound Mode in Emergency State (Example).....	584
Figure 8-101: SAS Redundant Mode in Normal State (Example).....	585

Figure 8-102: SAS Redundant Mode in Emergency State (Example)	586
Figure 8-103: Flowchart of INVITE from UA's in SAS Normal State	587
Figure 8-104: Flowchart of INVITE from Primary Proxy in SAS Normal State.....	588
Figure 8-105: Flowchart for SAS Emergency State	589
Figure 8-106: Enabling the SAS Application	590
Figure 8-107: Configuring Common Settings	592
Figure 8-108: Defining UAs' Proxy Server	593
Figure 8-109: Enabling Proxy Server for Gateway Application	595
Figure 8-110: Defining Proxy Server for Gateway Application.....	595
Figure 8-111: Disabling user=phone in SIP URL	596
Figure 8-112: Enabling Proxy Server for Gateway Application	596
Figure 8-113: Defining Proxy Servers for Gateway Application	597
Figure 8-114: Disabling user=phone in SIP URL	597
Figure 8-115: Manipulating User Part in Incoming REGISTER	599
Figure 8-116: Manipulating INVITE Destination Number	600
Figure 8-117: Blocking Unregistered SAS Users	602
Figure 8-118: Configuring SAS Emergency Numbers	603
Figure 8-119: Active Directory-based Routing Rules in Outbound IP Routing Table	607
Figure 9-1: Multiple Network Interfaces.....	620
Figure 9-2: Interface Column.....	630

Table of Tables

Table 2-1: Default LAN Data-Routing IP Address	28
Table 3-1: Description of Toolbar Buttons	44
Table 3-2: ini File Parameter for Welcome Login Message	56
Table 3-3: Areas of the Home Page	60
Table 3-4: Color-Coding Status for Trunk Channels	64
Table 3-5: NFS Settings Parameters	67
Table 3-6: Web User Accounts Access Levels and Privileges	73
Table 3-7: Default Attributes for the Web User Accounts	74
Table 3-8: SNMP Community String Parameters Description	79
Table 3-9: SNMP Trap Destinations Parameters Description	80
Table 3-10: SNMP V3 Users Parameters	82
Table 3-11: Multiple Interface Table Parameters Description	85
Table 3-12: IP Routing Table Description	88
Table 3-13: Internal Firewall Parameters	96
Table 3-14: CAS State Machine Parameters Description	100
Table 3-15: SIP Media Realm Table Parameters	109
Table 3-16: SRD Table Parameters	115
Table 3-17: SIP Interface Table Parameters	118
Table 3-18: IP Group Parameters	121
Table 3-19: Proxy Sets Table Parameters	127
Table 3-20: Account Table Parameters Description	134
Table 3-21: Hunt Group Table Parameters	146
Table 3-22: Hunt Group Settings Parameters	149
Table 3-23: Number Manipulation Parameters Description	154
Table 3-24: Redirect Number IP to Tel Parameters Description	157
Table 3-25: Redirect Number Tel to IP Parameters Description	159
Table 3-26: Phone-Context Parameters Description	161
Table 3-27: NPI/TON Values for ISDN ETSI	162
Table 3-28: Outbound IP Routing Table Parameters	169
Table 3-29: Inbound IP Routing Table Description	173
Table 3-30: Call Forward Table	187
Table 3-31: ISDN Supp Services Table Parameters	192
Table 3-32: Admission Control Parameters	196
Table 3-33: Classification Table Parameters	200
Table 3-34: IP2IP Routing Table Parameters	202
Table 3-35: Message Manipulations Parameters	208
Table 3-36: IP to IP Inbound Manipulation Parameters	211
Table 3-37: IP to IP Outbound Manipulation Table Parameters	213
Table 3-38: SAS IP2IP Routing Table Parameters	219
Table 3-39: Description of Table Action Icons	223
Table 3-40: Description of the Main Configuration Buttons	224
Table 3-41: Auxiliary Files Descriptions	337
Table 3-42: Ethernet Port Information Parameters	348
Table 3-43: Call Counters Description	352
Table 3-44: SAS/SBC Registered Users Parameters	353
Table 3-45: Call Routing Status Parameters	354
Table 3-46: IP Connectivity Parameters	356
Table 7-1: User Information Items	402
Table 8-1: Dialing Plan Notations	413
Table 8-2: Digit Map Pattern Notations	414
Table 8-3: Dialed MF Digits Sent to PSAP	423
Table 8-4: Dialed Number by Device Depending on Calling Number	425
Table 8-5: MLPP Call Priority Levels (Precedence) and DSCP Configuration Parameters	467
Table 8-6: Handling of SIP Diversion and History-Info Headers	505
Table 8-7: Message Manipulation Actions	506
Table 8-8: Event Structure	529
Table 8-9: Host Structure	529

Table 8-10: MLPP Structure	529
Table 8-11: Reason Structure	530
Table 8-12: URL Structure.....	530
Table 8-13: Enum Agent Role	531
Table 8-14: Enum Event Package.....	531
Table 8-15: Enum MLPP Reason Type.....	532
Table 8-16: Enum Number Plan.....	532
Table 8-17: Enum Number Type	532
Table 8-18: Enum Privacy	533
Table 8-19: Enum Reason.....	533
Table 8-20: Enum Reason (Reason Structure).....	533
Table 8-21: Enum Reason (RPI)	536
Table 8-22: Enum Refresher	536
Table 8-23: Enum Screen.....	536
Table 8-24: Enum ScreenInd	536
Table 8-25: Enum TransportType	537
Table 8-26: Enum Type.....	537
Table 8-27: Supported RADIUS Attributes.....	609
Table 8-28: Supported CDR Fields	611
Table 9-1: Multiple Interface Table.....	621
Table 9-2: Application Types	622
Table 9-3: Configured Default Gateway Example.....	623
Table 9-4: Separate Routing Table Example	624
Table 9-5: Quality of Service Parameters	625
Table 9-6: Traffic/Network Types and Priority	625
Table 9-7: Application Type Parameters	626
Table 9-8: IP Routing Table Layout.....	628
Table 9-9: Multiple Interface Table - Example 1	633
Table 9-10: Routing Table - Example 1.....	633
Table 9-11: Multiple Interface Table - Example 2.....	634
Table 9-12: Routing Table - Example2.....	634
Table 9-13: Multiple Interface Table - Example 3.....	635
Table 9-14: Routing Table - Example 3.....	635
Table 10-1: Mapping of ISDN Release Reason to SIP Response	639
Table 10-2: Mapping of SIP Response to ISDN Release Reason.....	641
Table 10-3: Calling Name (Display)	646
Table 10-4: Redirect Number	646
Table 12-1: IP Network Interfaces and VLAN Parameters.....	653
Table 12-2: Static Routing Parameters	654
Table 12-3: QoS Parameters	655
Table 12-4: NAT Parameters	657
Table 12-5: NFS Parameters	658
Table 12-6: DNS Parameters	659
Table 12-7: DHCP Parameters	660
Table 12-8: NTP and Daylight Saving Time Parameters	661
Table 12-9: General Web and Telnet Parameters	662
Table 12-10: Web Parameters	663
Table 12-11: Telnet Parameters.....	664
Table 12-12: General Debugging and Diagnostic Parameters	665
Table 12-13: Syslog, CDR and Debug Parameters	666
Table 12-14: RAI Parameters.....	669
Table 12-15: Serial Parameters	670
Table 12-16: General Security Parameters.....	671
Table 12-17: HTTPS Parameters.....	672
Table 12-18: SRTP Parameters	673
Table 12-19: TLS Parameters	674
Table 12-20: SSH Parameters	676
Table 12-21: OCSP Parameters	677

Table 12-22: RADIUS Parameters	677
Table 12-23: SNMP Parameters	679
Table 12-24: SIP Media Realm Parameters	682
Table 12-25: Proxy, Registration and Authentication SIP Parameters	683
Table 12-26: SIP Network Application Parameters	696
Table 12-27: General SIP Parameters	698
Table 12-28: Profile Parameters	721
Table 12-29: Voice Parameters	731
Table 12-30: Coder Parameters	733
Table 12-31: Fax and Modem Parameters	734
Table 12-32: DTMF Parameters	739
Table 12-33: RTP/RTCP and T.38 Parameters	740
Table 12-34: Fax and Modem Parameters	743
Table 12-35: DTMF and Hook-Flash Parameters	745
Table 12-36: Digit Collection and Dial Plan Parameters	750
Table 12-37: Voice Mail Parameters	753
Table 12-38: Caller ID Parameters	757
Table 12-39: Call Waiting Parameters	762
Table 12-40: Call Forwarding Parameters	765
Table 12-41: MWI Parameters	767
Table 12-42: Call Hold Parameters	769
Table 12-43: Call Transfer Parameters	770
Table 12-44: Three-Way Conferencing Parameters	772
Table 12-45: Emergency Call Parameters	773
Table 12-46: Call Cut-Through Parameters	774
Table 12-47: Automatic Dialing Parameters	775
Table 12-48: DID Parameters	776
Table 12-49: MLPP Parameters	777
Table 12-50: Automatic Dialing Parameters	781
Table 12-51: General PSTN Parameters	783
Table 12-52: TDM Bus and Clock Timing Parameters	787
Table 12-53: CAS Parameters	789
Table 12-54: ISDN Parameters	792
Table 12-55: ISDN and CAS Interworking Parameters	799
Table 12-56: Answer and Disconnect Parameters	817
Table 12-57: Tone Parameters	821
Table 12-58: Tone Detection Parameters	826
Table 12-59: Metering Tone Parameters	828
Table 12-60: Keypad Sequence Parameters	829
Table 12-61: General FXO Parameters	833
Table 12-62: General FXS Parameters	835
Table 12-63: Routing Parameters	836
Table 12-64: Alternative Routing Parameters	843
Table 12-65: Number Manipulation Parameters	847
Table 12-66: LDAP Parameters	857
Table 12-67: SBC Parameters	858
Table 12-68: SAS Parameters	873
Table 12-69: IP Media Parameters	878
Table 12-70: Auxiliary and Configuration File Parameters	881
Table 12-71: Automatic Update of Software and Configuration Files Parameters	882
Table 13-1: Software Package	885
Table 14-1: Technical Specifications	887

Notice

This document describes the AudioCodes Mediant 800 Multi-Service Business Gateway (MSBG).

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

© Copyright 2011 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: February-21-2011

Trademarks

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

WEEE EU Directive

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

Customer Support

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

Abbreviations and Terminology

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

Related Documentation

Manual Name
SIP CPE Release Notes
Product Reference Manual for SIP CPE Devices
Mediant 800 MSBG Installation Manual
MSBG CLI Reference Guide



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



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



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



Note: The terms *IP-to-Tel* and *Tel-to-IP* refer to the direction of the call relative to the device. *IP-to-Tel* refers to calls received from the IP network and destined to the PSTN/PBX (i.e., telephone connected directly or indirectly to the device); *Tel-to-IP* refers to calls received from the PSTN/PBX and destined for the IP network.



Notes:

- FXO (Foreign Exchange Office) is the interface replacing the analog telephone and connects to a Public Switched Telephone Network (PSTN) line from the Central Office (CO) or to a Private Branch Exchange (PBX). The FXO is designed to receive line voltage and ringing current, supplied from the CO or the PBX (just like an analog telephone). An FXO VoIP device interfaces between the CO/PBX line and the Internet.
- FXS (Foreign Exchange Station) is the interface replacing the Exchange (i.e., the CO or the PBX) and connects to analog telephones, dial-up modems, and fax machines. The FXS is designed to supply line voltage and ringing current to these telephone devices. An FXS VoIP device interfaces between the analog telephone devices and the Internet.

1 Overview

The Mediant 800 Multi-Service Business Gateway (MSBG) is a networking device that combines multiple service functions such as a Media Gateway, Session Border Controller (SBC), Data Router and Firewall, LAN switch, WAN access, Stand Alone Survivability (SAS) and an integrated general-purpose server.

The device's data routing capabilities support static and dynamic routing protocols such as RIP/OSPF and BGP, Virtual Routing and Forwarding (VRF-Lite) where interfaces can be clustered into a VRF to provide segregated routing domains. In addition, the device supports copper Gigabit Ethernet, T1 WAN, and Symmetric High-Speed Digital Subscriber Line (SHDSL) WAN interfaces, providing flexibility in connecting to Service Providers.

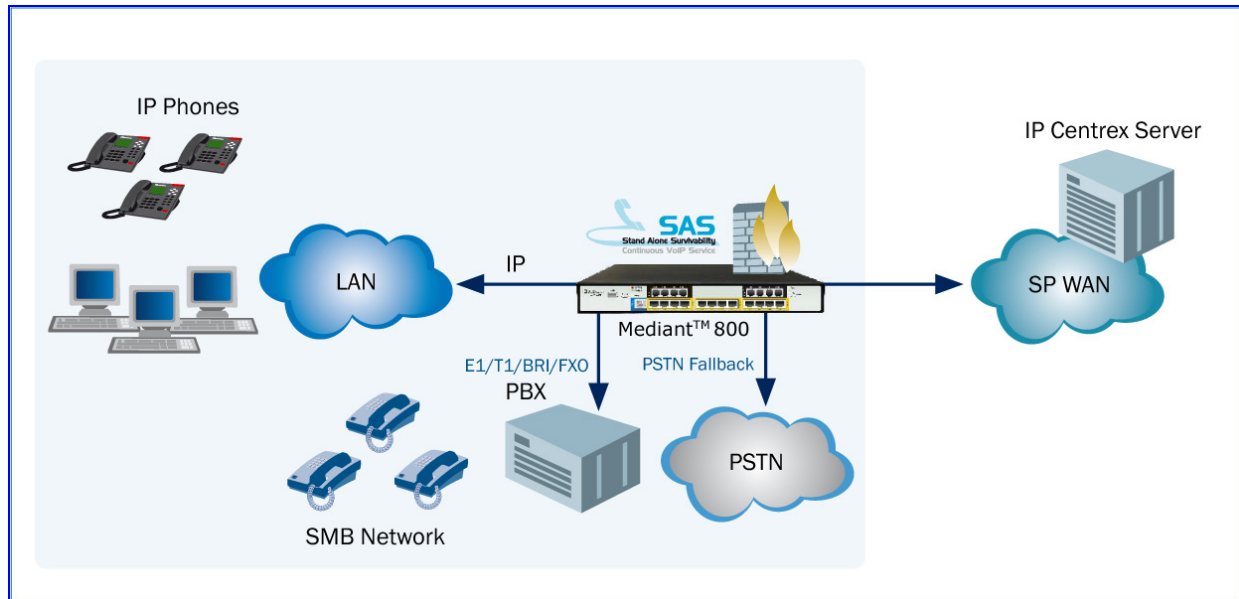
- The T1 WAN connection is through a dual T1 line interface (according to ANSI T1.403-1999). The device uses its dual T1 WAN Data Service Unit/Channel Service Unit (DSU/CSU) port interface to transmit and receive data using IP over Point-to-Point Protocol (PPP), IP over High-Level Data Link Control (HDLC), or or IP over Multilink Point-to-Point Protocol (MLPPP) framing.
- The SHDSL WAN connection supports up to four copper wire pairs according to G.991.2, acting as a remote-terminal CPE device. Both ATM and EFM modes are supported. In the ATM mode, a variety of protocols are supported, including PPPoE, PPPoA, and RFC 2684 in both bridged (Ethernet-over-ATM) and routed (IP-over-ATM) variants. In the EFM mode, the SHDSL port functions as a logical Ethernet device.

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

The device's SAS functionality offers service continuity to enterprises served by a centralized SIP-based IP-Centrex server or branch offices of distributed enterprises. SAS enables internal office communication between SIP clients, along with PSTN fallback in the case of disconnection from the centralized SIP IP-Centrex server or IP-PBX.

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

Figure 1-1: Typical Application



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

The device supports up to four ISDN Basic Rate Interface (BRI) S/T interfaces (RJ-45 ports), supporting up to eight voice channels. These connect ISDN terminal equipment such as ISDN telephones. The device also provides an optional, single E1/T1 interface port, supporting Transparent, CAS and ISDN protocols.

The device is optimized for wire-speed delivery of data, providing up to 12 Ethernet LAN ports for connecting equipment such as computers and IP phones. These ports are divided into Gigabit Ethernet and Fast Ethernet interfaces (the number depends on the ordered configuration), and provide power-over-Ethernet (PoE) capabilities. The device is equipped with a WAN interface supporting 10/100/1000Base-T copper for connecting to Service Provider networks.

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

2 Configuration Concepts

This section discusses the device's configuration tools and configuration concepts.

2.1 Configuration Tools

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

- The device's HTTP-based Embedded Web Server (Web interface), using any standard Web browser (described in "Web-based Management" on page 41).
- A configuration *ini* file loaded to the device (see "ini File Configuration" on page 367).
- AudioCodes' Element Management System (see "Element Management System (EMS)" on page 373).
- Simple Network Management Protocol (SNMP) browser software (refer to the *Product Reference Manual*).
- Command Line Interface (CLI) for configuring the Data-Routing functionality (refer to the MSBG Series CLI Reference Guide)

2.2 Main Operating Modes

The device can operate in one of the following main modes:

- VoIP and Data-Routing mode
- VoIP-only mode



Note: This section assumes that you already have IP connectivity to the device (i.e., that you can access its Web interface), as described in the *Installation Manual*.

2.2.1 Operating in VoIP and Data-Routing Mode

If you wish to use the device as a VoIP gateway with data-routing functionality, you need to configure the following data-routing features:

1. Connect the device's WAN port to the WAN network (refer to the *Installation Manual*).
2. Configure the Data-Router LAN interface (see "Configuring Data-Routing LAN Interface" on page 28)
3. Configure the DHCP server (see "Configuring Device's DHCP Server" on page 29)
4. Configure the WAN IP address (see "Assigning a WAN IP Address" on page 29)
5. Assign the WAN interface to the VoIP traffic
6. Configure Quality of Service - optional (see "Configuring Quality of Service" on page 32)
7. Configure VRF - optional (see "Configuring Virtual Routing and Forwarding" on page 38)
8. Enable remote Web management (see "Enabling Remote HTTP/S Web Management" on page 39)

2.2.1.1 Configuring Data-Routing LAN Interface

The default IP addresses of the LAN data-routing interface is listed in the table below.

Table 2-1: Default LAN Data-Routing IP Address

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











Note: The data-routing interface's IP address must be in the same subnet as the VoIP and Management interface.

➤ To define the device's LAN data-routing IP address:

1. Access the 'Connections' page (**Configuration** tab > **Data** menu > **Data System** > **Connections**).

Figure 2-1: Connections Page

Name	Status	Action
 LAN switch	1 Ports Connected	
 WAN Ethernet	Connected	
 LAN switch VLAN 1	Connected	 
New Connection		


2. Click the **Edit**  button corresponding to the "LAN Switch VLAN 1" connection, and then click the **Settings** tab.
3. In the 'IP Address' and 'Subnet Mask' fields, enter the required IP address and subnet respectively.

Figure 2-2: Defining LAN Data Routing IP Address

Device Name:	eth0.1
Status:	Connected
Schedule:	Always
Network:	LAN
Connection Type:	Ethernet
Physical Address:	00:90:8f:22:2e:31
MTU:	Automatic 1500
Underlying Connection:	LAN switch

Internet Protocol	Use the Following IP Address
IP Address:	10 . 8 . 6 . 85
Subnet Mask:	255 . 255 . 0 . 0

4. Click **OK** to save your settings.

2.2.1.2 Configuring Device's DHCP Server

The device's embedded DHCP server for the LAN is enabled, and with default IP pool addresses relating to the default subnet LAN. After reconfiguring the LAN IP addresses, the IP pool addresses should be changed accordingly. You can either disable the DHCP server or modify the IP address pool. The device (acting as a DHCP server), uses this setting to allocate IP addresses to all the computers connected to its LAN interface.

➤ **To configure DHCP on the device:**


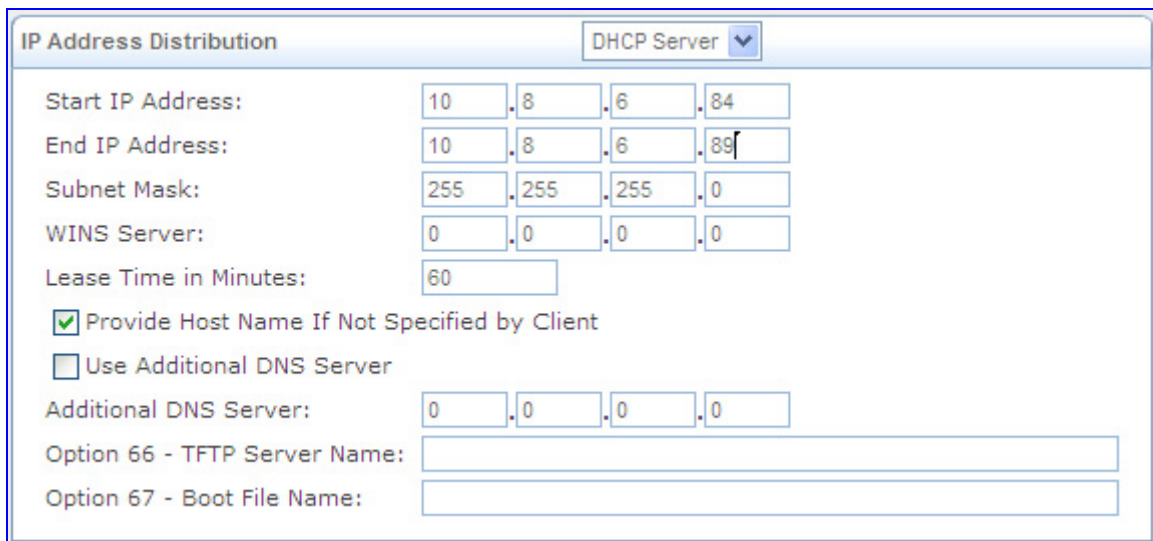
1. Access the 'DHCP Server' page (**Configuration** tab > **Data** menu > **Data Services** > **DHCP Server**).
2. Click the **Edit**  button corresponding to the **LAN Switch VLAN 1** connection.
3. From the 'IP Address Distribution' drop-down list, select "DHCP Server".
4. Define the IP address pool.

Figure 2-3: Configuring the DHCP Server



5. Click **OK**.
6. If required, refresh the address by disconnecting the cable and then reconnecting it again, or by performing the following in Windows' command line interface:

```
ipconfig /release
ipconfig /renew
```

2.2.1.3 Assigning a WAN IP Address

Once you have configured the device's LAN interfaces, you can then define the device's WAN interface (for connecting to the Internet). The WAN interface connection can be Ethernet, T1 WAN, or SHDSL. This section describes how to configure the Ethernet WAN interface manually.

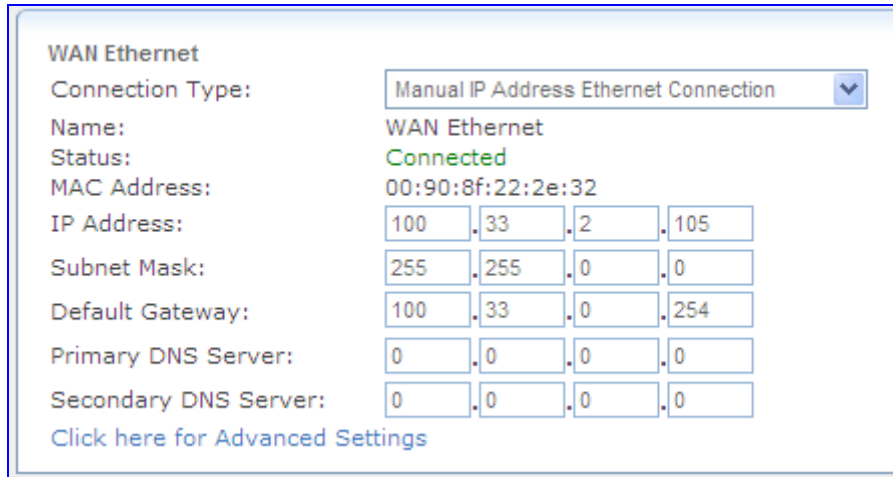


Note: Before you configure the WAN interface connection, ensure that you have all the required information from your Internet Service Provider (ISP).

➤ **To assign a WAN IP address:**

1. Cable the device to the WAN network (i.e., ADSL or Cable modem), using the WAN port.
2. Access the device's Web interface with the Voice and Management IP address.
3. Access the 'Settings' page (**Configuration** tab > **Data** menu > **WAN Access** > **Settings**).
4. From the 'Connection Type' drop-down lists, select the required connection type for the WAN, and then configure the subsequent parameters.

Figure 2-4: Selecting WAN Connection



WAN Ethernet

Connection Type: Manual IP Address Ethernet Connection

Name: WAN Ethernet

Status: Connected

MAC Address: 00:90:8f:22:2e:32

IP Address: 100 33 2 105

Subnet Mask: 255 255 0 0

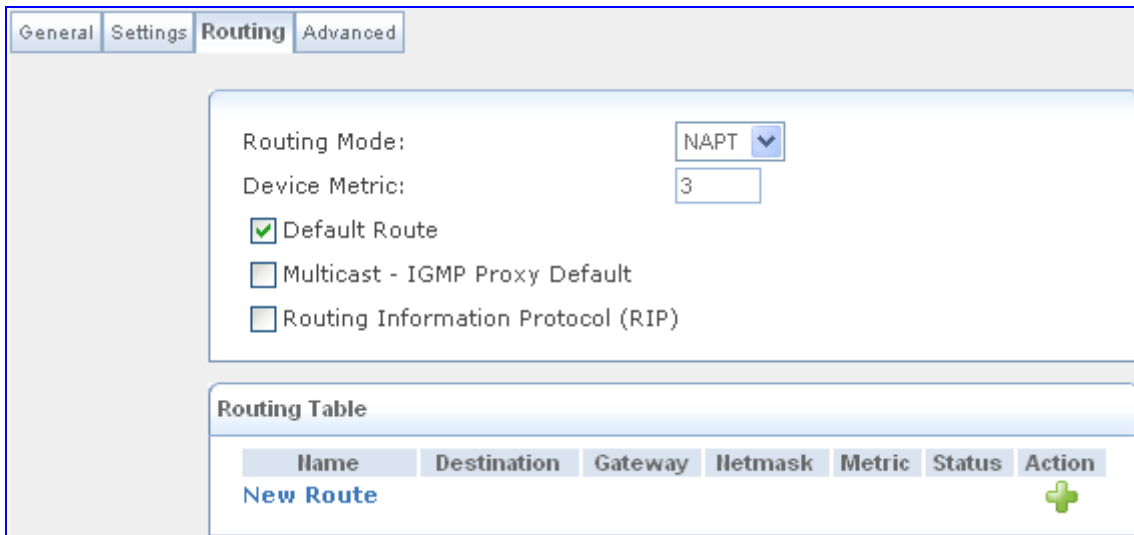
Default Gateway: 100 33 0 254

Primary DNS Server: 0 0 0 0

Secondary DNS Server: 0 0 0 0

[Click here for Advanced Settings](#)

5. Configure the WAN interface operating mode for Network Address Port Translation (NAPT):
 - a. Click the **Click here for Advanced Settings** link, and then select the **Routing** tab; the 'Routing' page appears:



General Settings **Routing** Advanced

Routing Mode: NAPT


Device Metric: 3

☒ Default Route

☐ Multicast - IGMP Proxy Default

☐ Routing Information Protocol (RIP)

Routing Table

Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						

- b. From the 'Routing Mode' drop-down list, select 'NAPT'.
- c. Select the 'Default Route' check box.
- d. Click **OK**.

2.2.1.4 Assign WAN Interface to VoIP Traffic

Once you have defined the WAN IP address for the data-routing interface, you then need to associate it with VoIP traffic (i.e., SIP signaling and media / RTP interfaces). The available WAN interfaces depend on the hardware configuration (i.e., Ethernet, T1, or SHDSL) and/or whether VLANs are defined for the WAN interface. If VLANs are defined, then you can select the WAN VLAN on which you want to run the SIP signaling and media interfaces. Once this association is set, VoIP traffic is sent on the WAN and incoming traffic is identified as coming from the WAN. The device also automatically configures the required port forwarding and static NAT rules.



Note: If you do not assign the WAN interface to SIP and media interfaces, then the WAN interface may not be used for VoIP traffic. In such scenarios, the VoIP traffic can be sent and received within the LAN, or sent to the WAN via a third-party LAN router. If a third-party router is used as the interface to the WAN, then you need to define NAT rules (using the NATTranslation parameter) to translate the VoIP LAN IP addresses (defined in the Multiple Interface table and associated with SIP and media interfaces) into global, public IP addresses.

➤ To assign a WAN interface to VoIP traffic:

1. Select the WAN interface:
 - a. Open the 'Multiple Interface Table' page (**Configuration** tab > **VoIP** menu > **Network** submenu > **IP Settings**).

Figure 2-5: Selecting WAN Interface for VoIP Traffic

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP + Media + Control	IPv4 Manual	10.8.6.86	16	10.8.0.1	1	Voice

WAN Interface Name

WAN Ethemet

Selecting WAN Interface

- b. From the 'WAN Interface Name' drop-down list, select the WAN interface for VoIP traffic.
 - c. Click **Done**, and then reset the device for your setting to take effect.
2. Assign the selected WAN interface to SIP signaling and RTP (media) interfaces. This is done in the SIP Interface and SIP Media Realm tables respectively (whereby the WAN interface is denoted as "WAN"):
 - a. Open the 'SIP Interface Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SIP Interface** Table) and define SIP interface(s) on the WAN interface.

Figure 2-6: Assigning SIP Interface to WAN

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	WAN	SBC	5060	5060	5061	1
2	Voice	SBC	5080	5080	5067	2

SIP Interface Assigned to WAN Interface

- b. Open the 'SIP Media Realm Table' page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Realm** Configuration) and define media interface(s) on the WAN interface.

Figure 2-7: Assigning WAN Interface to Media Realm

Index	Media Realm Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End
1	Realm1	Voice	6000	20	6190
2	Realm2	WAN	7000	101	8000

Media Realm Assigned to WAN Interface

- c. Define SRDs and associate them with these SIP signaling and media interfaces. Configure other SIP settings as required.

2.2.1.5 Configuring Quality of Service

This section describes how to configure the device to guarantee appropriate handling of VoIP services, which are delay-sensitive. Therefore, VoIP traffic needs to be prioritized over other classes of traffic. This is achieved by configuring Quality of Service (QoS).

The QoS configuration includes the following stages:

- Defining the total WAN bandwidth assigned, for example, by your Internet Telephony Service Provider (ITSP) - see "Defining Total WAN Bandwidth" on page 32
- Defining traffic shaping classes with the minimum bandwidth guaranteed for VoIP traffic (see "Defining VoIP Tx Shaping Class" on page 33)
- Assigning the above VoIP traffic class to VoIP RTP media packets and VoIP signaling (UDP, TCP, and TLS) traffic matching rules ("Defining VoIP Traffic Matching Rules" on page 35)

2.2.1.5.1 Defining Total WAN Bandwidth

To define traffic shaping on the device so that packets will not be "dropped" by your ITSP, you should configure your device with the total WAN bandwidth allocated by your ITSP. In other words, the ITSP can be considered the bottleneck of the network and thus, the device needs to accommodate its outgoing traffic to this bandwidth.

➤ **To define the WAN bandwidth traffic shaping class:**

1. Open the 'Traffic Shaping' page (**Configuration** tab > **Data** menu > **QoS** > **Traffic Shaping**).

Figure 2-8: Traffic Shaping Page

Device	Tx Bandwidth (Kbps)	Rx Bandwidth (Kbps)	TCP Serialization	Action
New Entry				+


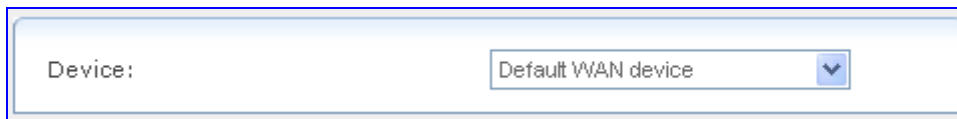
- Click the **New**  button; the following page appears.

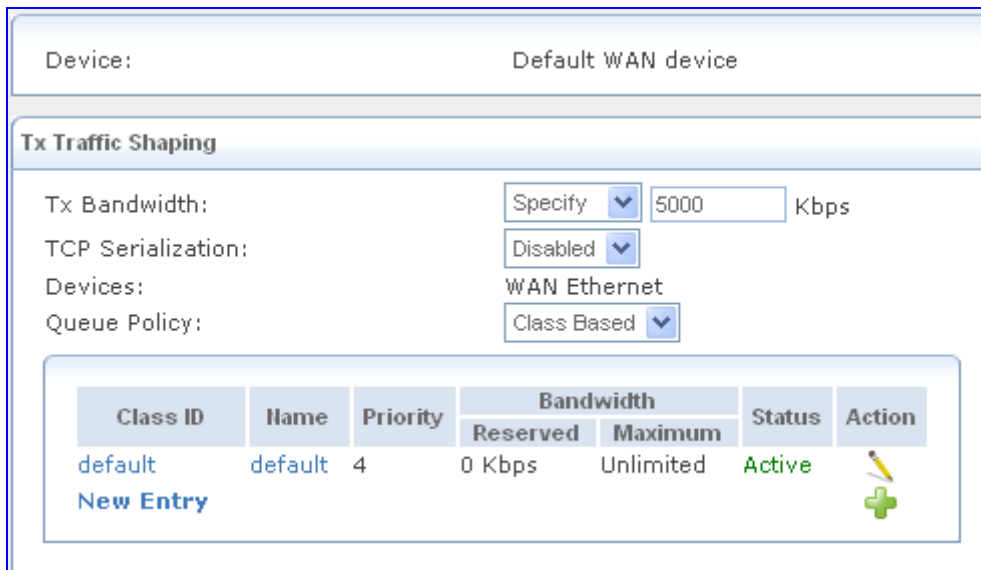
Figure 2-9: Selecting Device for Traffic Shaping



Device: Default WAN device

- From the 'Device' drop-down list, select 'Default WAN device', and then click **OK**; the following page appears:

Figure 2-10: Defining Traffic Shaping



Device: Default WAN device


Tx Traffic Shaping


Tx Bandwidth: Specify 5000 Kbps

TCP Serialization: Disabled

Devices: WAN Ethernet

Queue Policy: Class Based

Class ID	Name	Priority	Bandwidth		Status	Action
			Reserved	Maximum		
default	default	4	0 Kbps	Unlimited	Active	

[New Entry](#) 

- In the 'Tx Bandwidth' field, specify the total WAN bandwidth (in Kbps) allocated by your ISP. For example, 5 Mbps (5000 Kbps), as shown in the figure above.
- Click **OK**.

2.2.1.5.2 Defining VoIP Tx Traffic Shaping Classes

Once you have defined the total bandwidth allocated to the device's WAN interface, you need to define a traffic shaping class to reserve a minimum bandwidth (e.g., of 1 Mbps) for Tx VoIP traffic (SIP signaling and RTP packets) out of the total bandwidth (e.g., 5 Mbps).

➤ To define traffic shaping class for VoIP traffic:



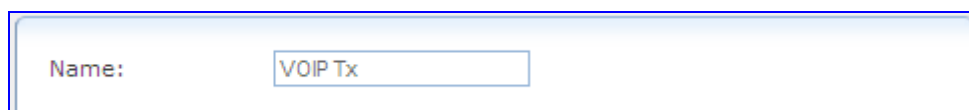
- Open the 'Traffic Shaping' page (see "Defining Total WAN Bandwidth" on page 32) and click the **Edit**  button corresponding to the 'Default WAN Device' entry.
- In the 'Tx Traffic Shaping' group, click the **New**  button.
- Assign a name to the new class (e.g., "VOIP Tx"), and then click **OK**; the page closes and you are returned to the previous page.

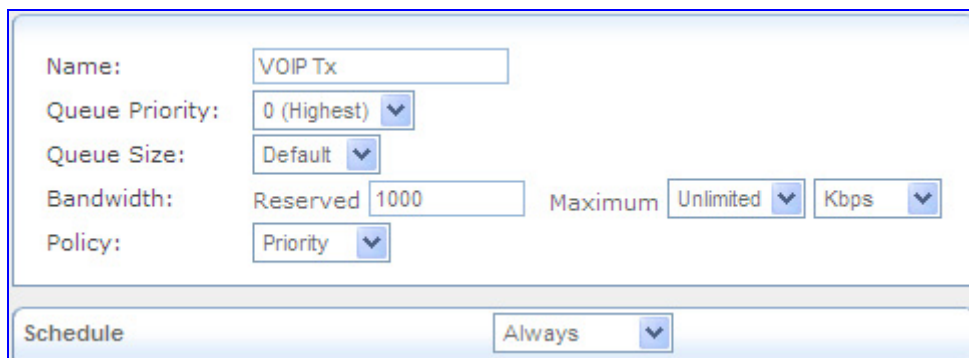
Figure 2-11: Adding Class Rule



Name: VOIP Tx

4. Click the newly added class name; the following page appears:

Figure 2-12: Defining Shaping Class (for VoIP Tx Traffic)

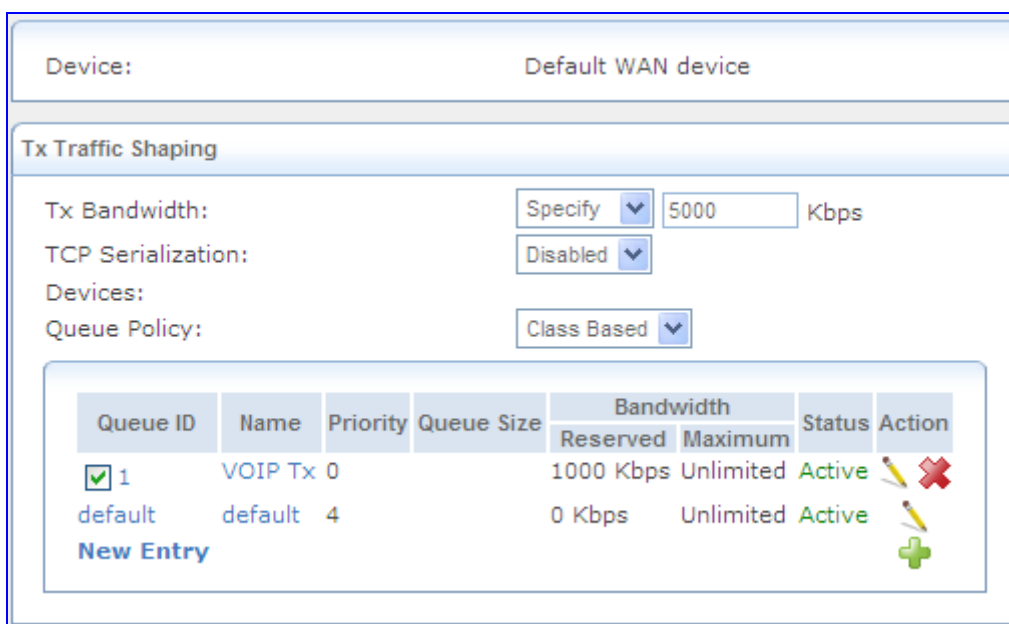


Name:
 Queue Priority:
 Queue Size:
 Bandwidth:
 Policy:
 Schedule:





5. Configure the following:
 - a. From the 'Queue Priority' drop-down list, select '0 (Highest)', i.e., the highest priority.
 - b. In the 'Bandwidth - Reserved' field, enter "1000" (i.e., 1 Mbps).
 - c. From the 'Maximum' drop-down list, select 'Unlimited'.
 - d. From the 'Policy' drop-down list, select 'Priority'.
 - e. Click **OK**.

The figure below shows an example of the configured traffic shaping classes for Tx VoIP traffic.

Figure 2-13: Configured Traffic Shaping for Total WAN and VoIP Bandwidth



Device:
Tx Traffic Shaping
 Tx Bandwidth: Kbps
 TCP Serialization:
 Devices:
 Queue Policy:

Queue ID	Name	Priority	Queue Size	Bandwidth		Status	Action
				Reserved	Maximum		
<input checked="" type="checkbox"/> 1	VOIP Tx	0		1000 Kbps	Unlimited	Active	 
default	default	4		0 Kbps	Unlimited	Active	
New Entry 							

2.2.1.5.3 Defining VoIP Traffic Matching Rules

Once you have defined the VoIP Tx traffic shaping class (e.g., "VOIP Tx") in "Defining VoIP Tx Shaping Class" on page 33, you need to define traffic matching rules (QoS outbound rules) for VoIP RTP media traffic as well as for SIP signaling traffic, and then assign the shaping class to these traffic rules.

The following matching rules need to be configured:

■ **SIP TCP connections:**

- Incoming TCP connection to WAN port 5060-5061 must be matched to Traffic Shaping class "VOIP Tx". Outbound packets sent on this connection will originate from port 5060.
- Outbound TCP connections from WAN port 5060-5061 sent to any destination must be matched to Traffic Shaping class "VOIP Tx". Outbound packets on this connection will originate from an arbitrary port, but will be destined to port 5060-5061.

■ **SIP UDP connections:** Outbound UDP packets sent from WAN port 5060 to any destination must be matched to Traffic Shaping class "VOIP Tx".

■ **RTP UDP:** Outbound UDP packets sent from WAN port 7000-8000 to any destination must be matched to Traffic Shaping class "VOIP Tx".

➤ **To define VoIP traffic matching rules:**

1. Open the 'Match Rules' page (**Configuration** tab > **Data** menu > **QoS** > **Match Rules**).

Figure 2-14: Match Rules Page

QoS Input Rules						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
All Devices						
New Entry						+
WAN Ethernet Rules						
New Entry						+
LAN switch VLAN 4001 Rules						
New Entry						+
QoS Output Rules						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
All Devices						
New Entry						+
WAN Ethernet Rules						
New Entry						+
LAN switch VLAN 4001 Rules						
New Entry						+


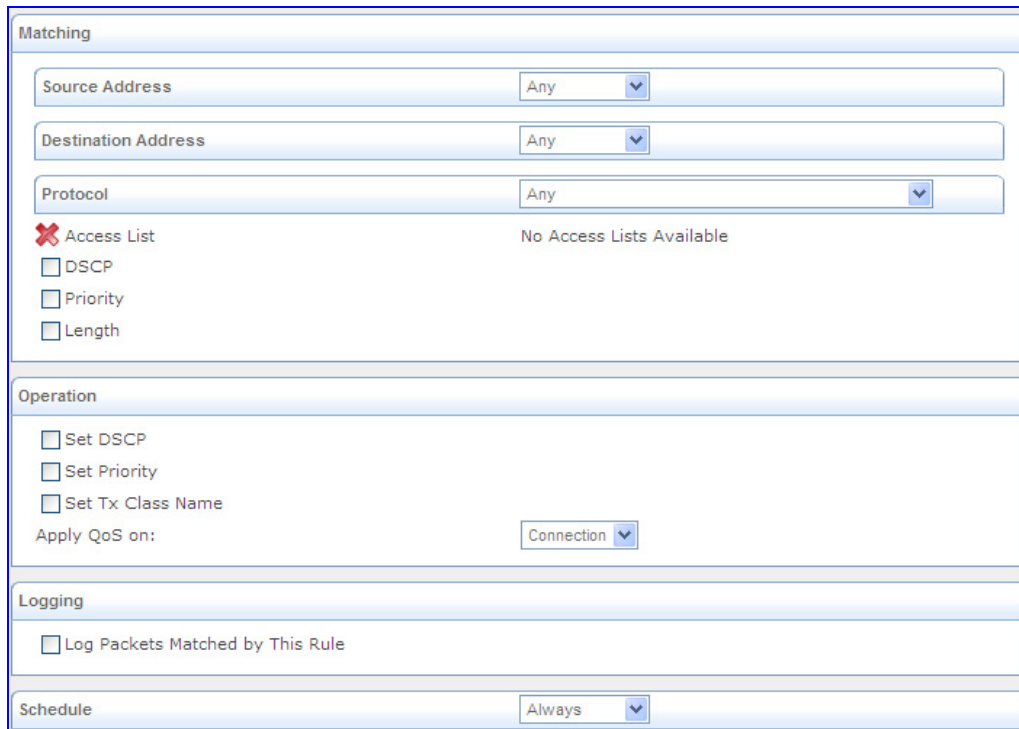
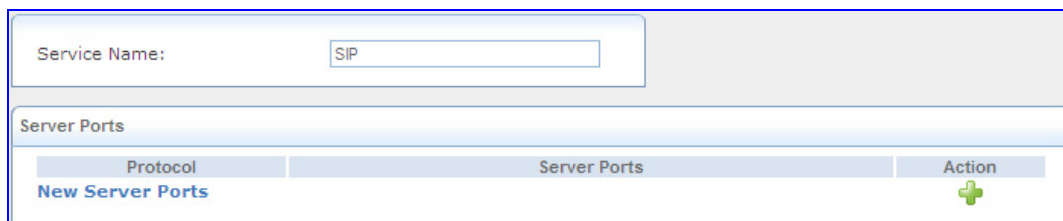
2. Under the 'QoS Output Rules' table, click the **New**  button corresponding to the 'WAN Ethernet Rules' rule ID; the following page appears:

Figure 2-15: Adding a Traffic Priority Rule



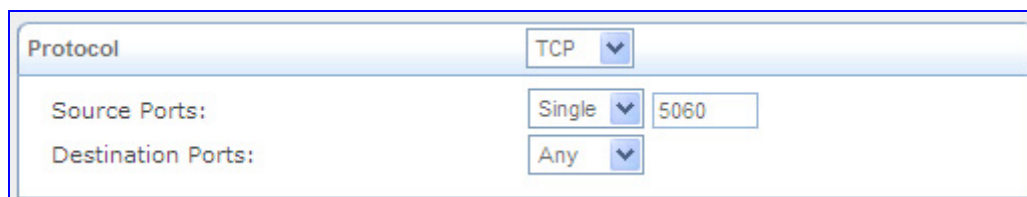
3. Add a new output traffic rule for VoIP SIP signaling to the WAN:
 - a. From the 'Protocol' drop-down list, select 'Show All Services' to view all protocols and then select 'SIP'; "SIP" is displayed under the 'Protocol' group.
 - b. From the drop-down list appearing below "SIP", select 'User Defined'; the following appears.

Figure 2-16: Defining Incoming SIP Ports



- c. In the 'Service Name' field, enter the service, and then click **New Server Ports**; the following page appears.

Figure 2-17: Defining SIP Ports (e.g. TCP)



- d. Define the TCP and UDP ports, and then click **OK**; the following page appears displaying the configured ports.

Figure 2-18: Configured Ports for Incoming SIP

Protocol	Server Ports	Action
TCP	Any -> 5060-5061	
UDP	Any -> 5060	

New Server Ports

- a. Click **OK** again.
- b. Perform steps 2b through 2e to configure ports for outgoing SIP packets.
- c. Under the 'Operation' group, select the 'Set Tx Class Name' check box, and then from the corresponding drop-down list, select the traffic shaping class 'VOIP Tx', which you defined for Rx packets (in "Defining VoIP Tx Shaping Class" on page 33).

The configured incoming and outgoing SIP ports are shown below:

Figure 2-19: Traffic Matching Rule for Received SIP Signaling Traffic

Matching

Source Address: Any

Destination Address: Any

Protocol

Name	Ports	Action
SIP (Inbound TCP)	TCP 5060-5061 -> Any	
SIP (Outbound TCP)	TCP Any -> 5060-5061	
SIP (UDP)	UDP 5060 -> Any	

Add...

Access List: No Access Lists Available

☐ DSCP

☐ Priority

☐ Length

Operation

☐ Set DSCP

☐ Set Priority

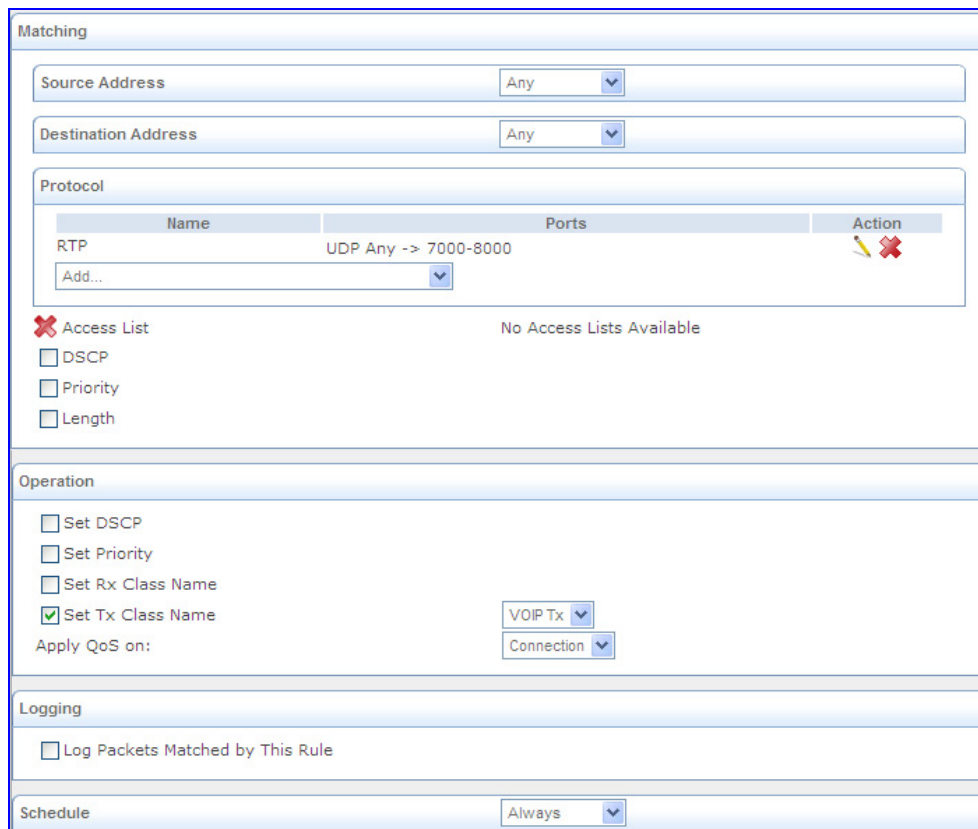
☒ Set Tx Class Name: VOIP Tx

Apply QoS on: Connection

- e. Click **OK**.

4. Add a new traffic matching rule for transmitted (Tx) VoIP RTP packets to the WAN. Perform steps 2 through 3, except for the 'Protocol' group, select the protocol 'RTP' and only port 'UDP', as shown below.

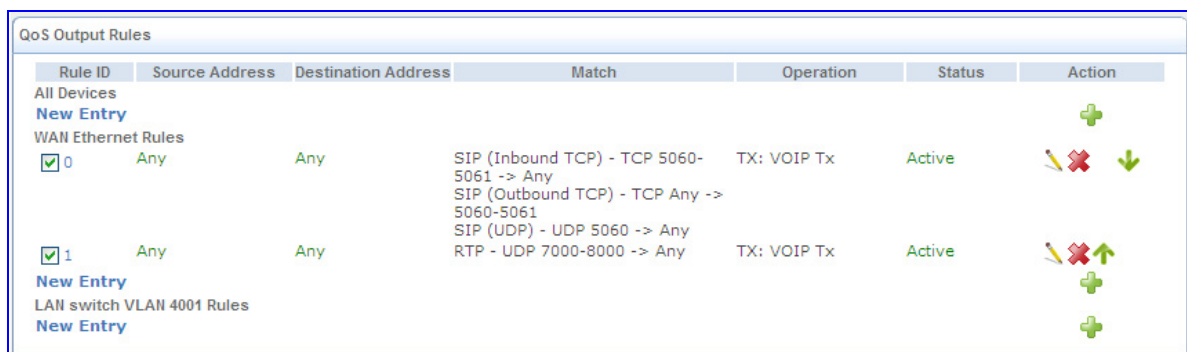
Figure 2-20: Matching Rule for Received RTP Traffic









The screenshot shows the 'Matching' tab of a configuration window. It includes fields for 'Source Address' and 'Destination Address', both set to 'Any'. The 'Protocol' section shows a table with one entry: 'RTP' with 'Ports' 'UDP Any -> 7000-8000'. Below this are checkboxes for 'Access List', 'DSCP', 'Priority', and 'Length', all of which are unchecked. The 'Operation' section has checkboxes for 'Set DSCP', 'Set Priority', 'Set Rx Class Name', and 'Set Tx Class Name'. The 'Set Tx Class Name' checkbox is checked, and a dropdown menu next to it is set to 'VOIP Tx'. Below this, 'Apply QoS on:' is set to 'Connection'. The 'Logging' section has a checkbox for 'Log Packets Matched by This Rule' which is unchecked. The 'Schedule' section has a dropdown menu set to 'Always'.

The final traffic matching rule configuration for WAN Tx RTP and SIP signaling is shown below.

Figure 2-21: Traffic Matching Rule for WAN Tx/Rx RTP and SIP Signaling



Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
All Devices						
New Entry						
WAN Ethernet Rules						
<input checked="" type="checkbox"/> 0	Any	Any	SIP (Inbound TCP) - TCP 5060-5061 -> Any SIP (Outbound TCP) - TCP Any -> 5060-5061 SIP (UDP) - UDP 5060 -> Any	TX: VOIP Tx	Active	  
<input checked="" type="checkbox"/> 1	Any	Any	RTP - UDP 7000-8000 -> Any	TX: VOIP Tx	Active	  
New Entry						
LAN switch VLAN 4001 Rules						
New Entry						

2.2.1.6 Configuring Virtual Routing and Forwarding

The Virtual Routing and Forwarding (VRF) Lite feature enables the ability to use a single physical router as several logical routers. Each VRF is associated with its own routing table. To create fully separated logical routers on the same physical router, every interface can be mapped to a specified VRF and static routes can be added to it.

For VRF configuration, refer to the *MSBG Series CLI Reference Guide*.

2.2.1.7 Enabling Remote HTTP/S Web Management

If you want to access the device's Web interface remotely through HTTP or HTTPS, you need to define the WAN HTTP/S port.

➤ To define WAN HTTP/S port for remote Web management:

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

Figure 2-22: Defining WAN HTTP Port

HTTP Authentication Mode	Digest When Possible	
Secured Web Connection (HTTPS)	HTTP and HTTPS	
WAN HTTP Port	80	
WAN HTTPS Port	443	

2. In the 'WAN HTTP Port' or 'WAN HTTPS Port' field, define the WAN port.
3. Click **Submit**.

2.2.2 Operating in VoIP-Only Mode

If you wish to use the device for VoIP functionality only (i.e., without data-routing functionality), you need to disable the data-routing interface as described below.



Note: When operating in VoIP-only mode, do not use the device's WAN port.

➤ To operate the device as a VoIP gateway only:

1. Disconnect the network cable from the WAN port and then connect one of the device's LAN ports to the network.
2. Remove the data-routing IP network interface:
 - a. Access the 'Connections' page (**Configuration** tab > **Data** menu > **Data System** > **Connections**).
 - b. Delete the "LAN Switch VLAN 1" connection by clicking the corresponding **Remove** button, and then clicking **OK** to confirm deletion.

Figure 2-23: Removing Data-Routing Connection Interface

Name	Status	Action
LAN switch	1 Ports Connected	
WAN Ethernet	Cable Disconnected	
LAN switch VLAN 1	Connected	
New Connection		

3. Configure VoIP IP network interfaces in the 'Multiple Interface' table (**Configuration** tab > **VoIP** menu > **Network Settings** > **IP Settings**) - see "Configuring IP Interface Settings" on page 83. The configuration depends on whether or not you want to implement VLANs:



Note: For the VoIP network interface, ensure that the Default Gateway is defined with an IP address other than the default IP address (in the 'Multiple Interface' table).

- **Without VLANs:** In the 'Multiple Interface' table, define a single IP network interface for application types "OAMP + Media + Control".

Figure 2-24: Multiple Interface Table

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	<input type="radio"/> OAMP + Media + Control	10.8.6.86	16	10.8.0.1	1	Voice

- **With VLANs:**
 - a. In the 'Multiple Interface' table, define multiple IP network interfaces, each with a unique VLAN ID (e.g. OAMP interface with VLAN ID 501, Media interface with VLAN ID 2012, and Control interface with VLAN ID 2014).

Figure 2-25: Multiple Interfaces with VLANs

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	<input type="radio"/> OAMP	10.8.6.86	16	10.8.0.1	501	Mng
1	<input type="radio"/> Media + Control	10.32.174.50	24	10.33.174.1	2012	MediaControl
2	<input type="radio"/> Media	10.33.174.50	24	10.33.174.1	2013	Media
3	<input type="radio"/> Control	10.34.174.50	24	10.33.174.1	2014	Control




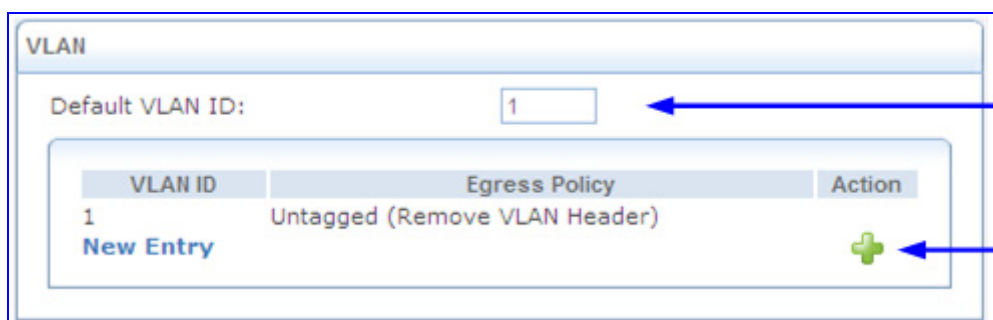
- b. Define VLANs for each port: In the 'Connections' page (**Configuration** tab > **Data** menu > **Data Settings** > **Connections**), click the **Edit**  button corresponding to the "LAN Switch" connection.
- c. Select the **Switch** tab; a list of the device's ports is displayed.
- d. Click the **Edit**  button corresponding to a required port.
- e. In the 'Default VLAN ID' field, enter the VLAN ID ("Native" VLAN ID/PVID) to assign to untagged received packets.
- f. Click the **New**  button and define a VLAN ID for the port.

Figure 2-26: Defining VLANs per LAN Port



- g. Click **OK** to save settings.

3 Web-Based Management

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

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



Notes:

- For a detailed description of all the parameters in the Web interface, see "Configuration Parameters Reference" on page [653](#).
- 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 [653](#).
- 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 [653](#).
- 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 [339](#).

3.1 Getting Acquainted with the Web Interface

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

3.1.1 Computer Requirements

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

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



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

3.1.2 Accessing the Web Interface

The Web interface can be opened using any standard Web browser (see "Computer Requirements" on page 42). When initially accessing the Web interface, use the default user name ('Admin') and password ('Admin'). For changing the login user name and password, see "Configuring the Web User Accounts" on page 73).

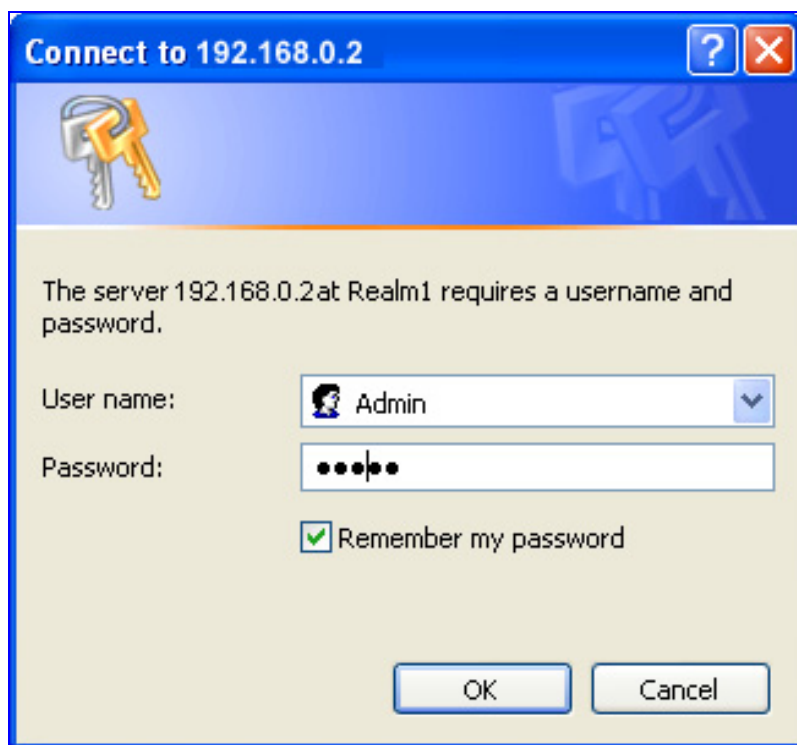


Note: For assigning an IP address to the device, refer to the *Installation Manual*.

➤ **To access the Web interface:**

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

Figure 3-1: Login Screen



3. In the 'User Name' and 'Password' fields, enter the case-sensitive, user name and password.
4. Click the **OK** button; the Web interface is accessed, displaying the 'Home' page (for a detailed description of the 'Home' page, see "Using the Home Page" on page 59).



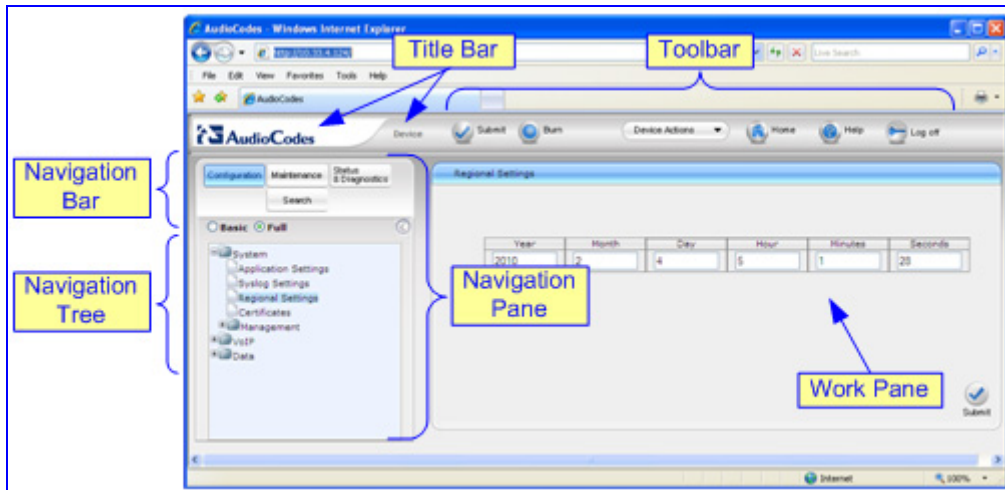
Note: If access to the device's Web interface is denied ("Unauthorized") due to Microsoft Internet Explorer security settings, perform the following:

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

3.1.3 Areas of the GUI

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

Figure 3-2: Areas of the Web Interface GUI





The Web GUI is composed of the following main areas:

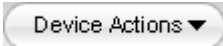



- **Title bar:** Displays the corporate logo and product name.
- **Toolbar:** Provides frequently required command buttons for configuration (see "Toolbar" on page 44).
- **Navigation Pane:** Consists of the following areas:
 - **Navigation bar:** Provides tabs for accessing the configuration menus (see "Navigation Tree" on page 45) and searching *ini* file parameters that have corresponding Web interface parameters (see "Searching for Configuration Parameters" on page 54).
 - **Navigation tree:** Displays the elements pertaining to the tab selected on the Navigation bar (tree-like structure of the configuration menus or Search engine).
- **Work pane:** Displays configuration pages where configuration is performed (see "Working with Configuration Pages" on page 48).

3.1.4 Toolbar

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

Table 3-1: Description of Toolbar Buttons

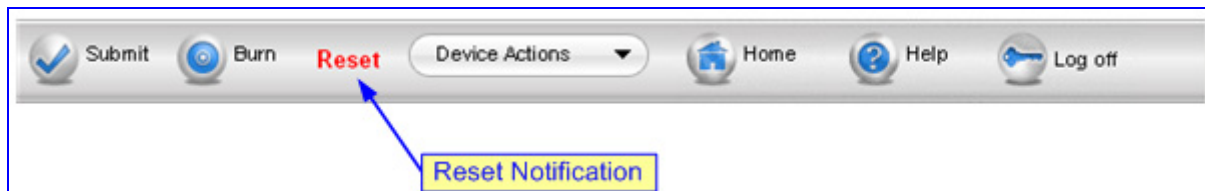
Icon	Button Name	Description
	Submit	Applies parameter settings to the device (see "Saving Configuration" on page 336). Note: This icon is grayed out when not applicable to the currently opened page.
	Burn	Saves parameter settings to flash memory (see "Saving Configuration" on page 336).

Icon	Button Name	Description
	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 344). ▪ Save Configuration File: opens the 'Configuration File' page for saving the <i>ini</i> file to a PC (see "Backing Up and Loading Configuration File" on page 344). ▪ Reset: opens the 'Maintenance Actions' page for resetting the device (see "Resetting the Device" on page 334). ▪ Software Upgrade Wizard: opens the 'Software Upgrade Wizard' page for upgrading the device's software (see "Software Upgrade Wizard" on page 341).
	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 in the Work pane (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 the word "Reset" (in red color), as shown in the figure below. This is a reminder to later save ('burn') your settings to flash memory and reset the device.

Figure 3-3: "Reset" Displayed on Toolbar



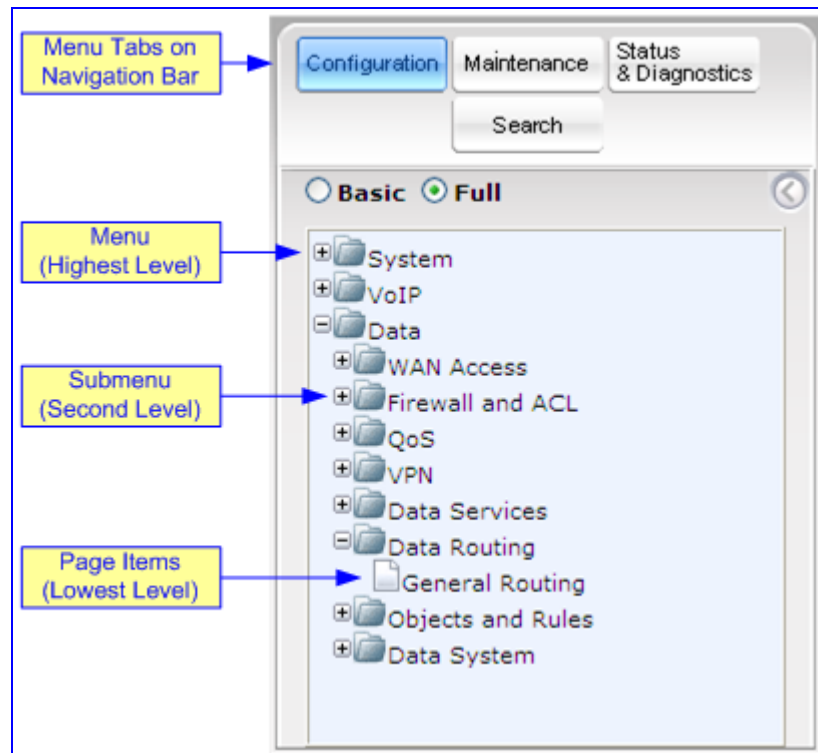
3.1.5 Navigation Tree

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

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

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

Figure 3-4: Navigation Tree



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

- On the Navigation bar, select the required tab:
 - **Configuration** (see "Configuration Tab" on page 65)
 - **Maintenance** (see "Maintenance Tab" on page 333)
 - **Status & Diagnostics** (see "Status & Diagnostics Tab" on page 346)

➤ **To navigate to a page:**

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

3.1.5.1 Displaying Navigation Tree in Basic and Full View

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

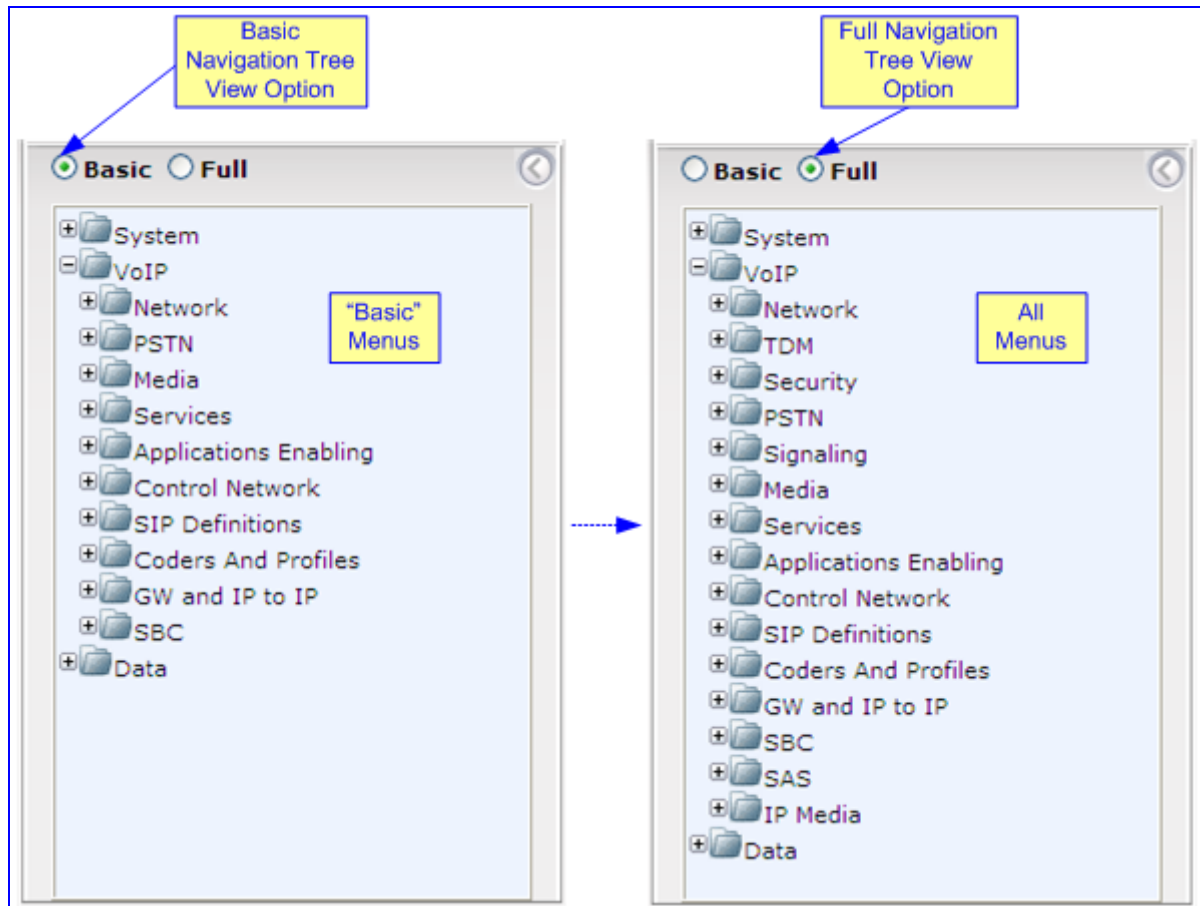
The Navigation tree menu can be displayed in one of two views:

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

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

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

Figure 3-5: Toggling Between Navigation Tree Views



3.1.5.2 Showing / Hiding the Navigation Pane

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



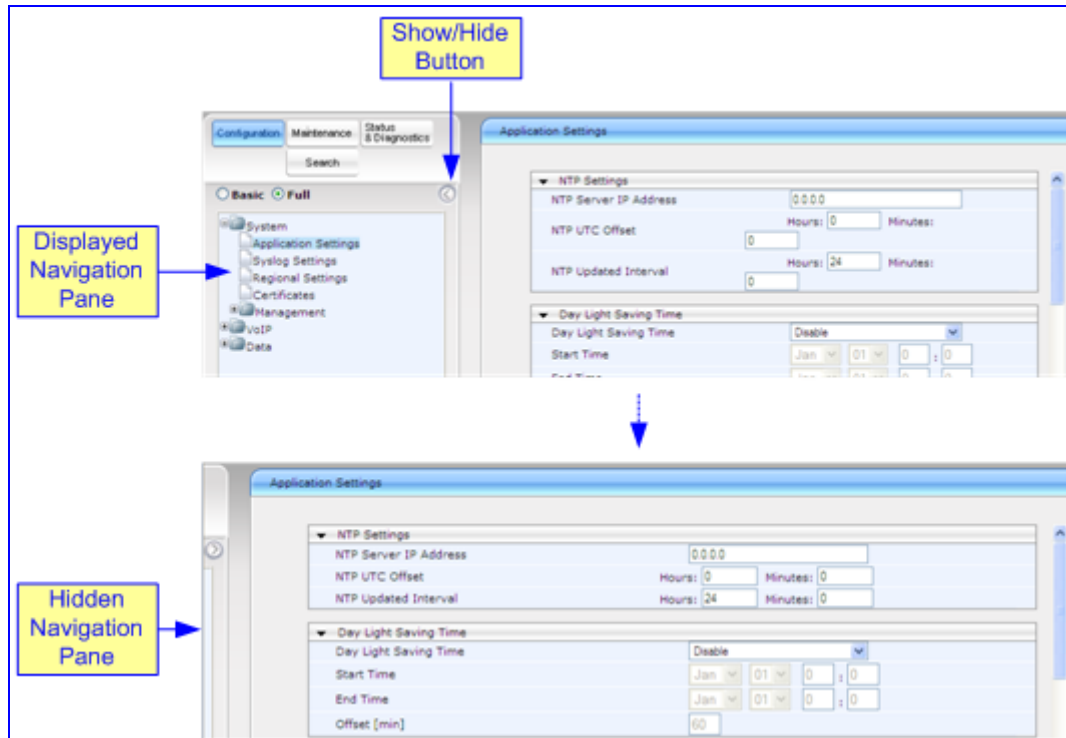
- **To hide the Navigation pane:** click the left-pointing arrow ; the pane is hidden and the button is replaced by the right-pointing arrow button.
- **To show the Navigation pane:** click the right-pointing arrow ; the pane is displayed and the button is replaced by the left-pointing arrow button.

Figure 3-6: Show / Hide Navigation Tree



3.1.6 Working with Configuration Pages

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

3.1.6.1 Accessing Pages

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

➤ To open a configuration page in the Work pane:

1. On the Navigation bar, click the required tab:
 - **Configuration** (see "Configuration Tab" on page 65)
 - **Maintenance** (see "Maintenance Tab" on page 333)
 - **Status & Diagnostics** (see "Status & Diagnostics Tab" on page 346)

The menus of the selected tab appear in the Navigation tree.

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

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

**Notes:**

- You can also access certain pages from the **Device Actions** button located on the toolbar (see "Toolbar" on page 44).
- 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 46).
- 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 73). If a page is read-only, 'Read-Only Mode' is displayed at the bottom of the page.

3.1.6.2 Viewing Parameters

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

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

- Display of "basic" and "advanced" parameters (see "Displaying Basic and Advanced Parameters" on page 50)
- Display of parameter groups (see "Showing / Hiding Parameter Groups" on page 51)

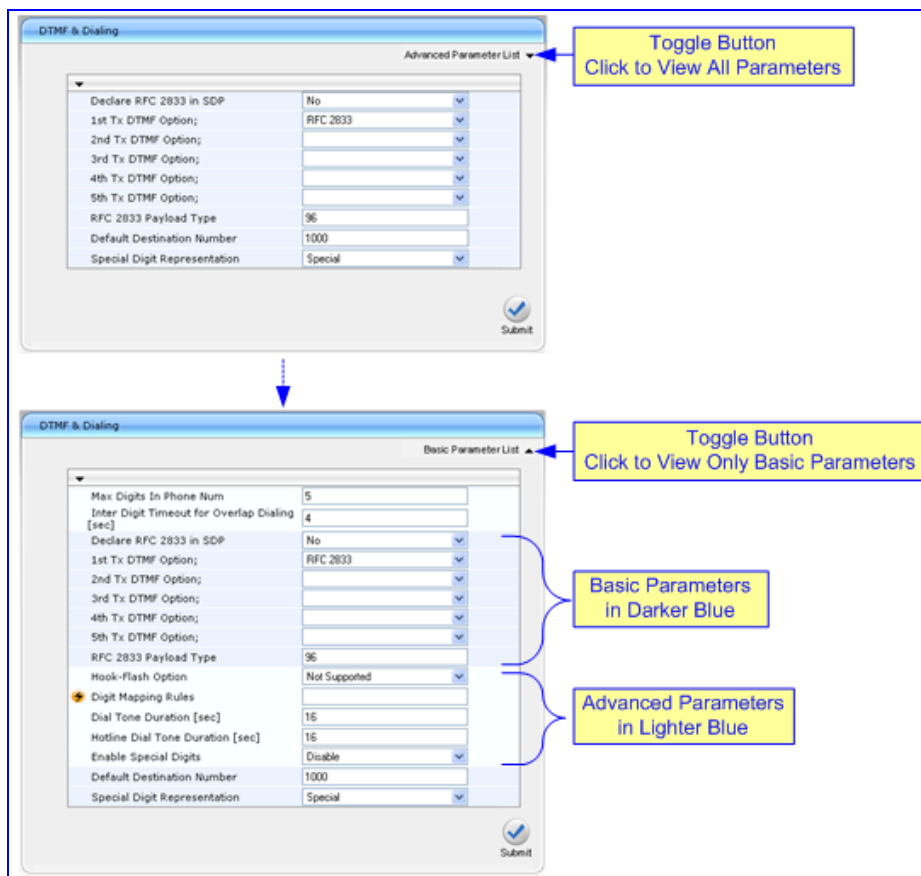
3.1.6.2.1 Displaying Basic and Advanced Parameters

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



The figure illustrates the toggling between Basic and Advanced views for the 'DTMF & Dialing' configuration page. It consists of two screenshots connected by a downward arrow.

Top Screenshot (Advanced View): The 'Advanced Parameter List' button is selected, showing a list of parameters including 'Declare RFC 2833 in SDP', '1st Tx DTMF Option', '2nd Tx DTMF Option', '3rd Tx DTMF Option', '4th Tx DTMF Option', '5th Tx DTMF Option', 'RFC 2833 Payload Type', 'Default Destination Number', and 'Special Digit Representation'. A yellow callout box points to the 'Advanced Parameter List' button with the text: 'Toggle Button Click to View All Parameters'.

Bottom Screenshot (Basic View): The 'Basic Parameter List' button is selected, showing the same list of parameters plus additional basic parameters like 'Max Digits In Phone Num', 'Inter Digit Timeout for Overlap Dialing', 'Hook-Flash Option', 'Digit Mapping Rules', 'Dial Tone Duration', 'Hotline Dial Tone Duration', and 'Enable Special Digits'. A yellow callout box points to the 'Basic Parameter List' button with the text: 'Toggle Button Click to View Only Basic Parameters'. Two other yellow callout boxes on the right side of the parameter list identify 'Basic Parameters in Darker Blue' and 'Advanced Parameters in Lighter Blue'.

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



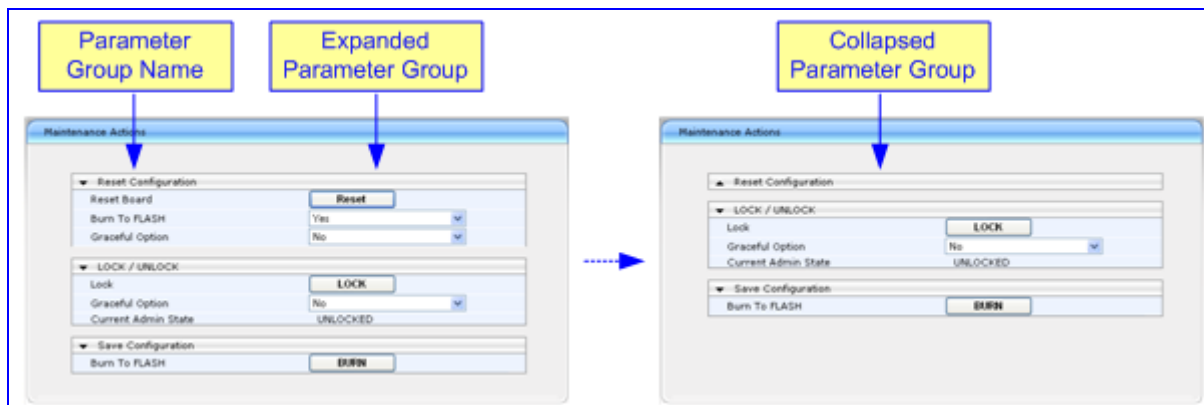
Notes:

- When the Navigation tree is in 'Full' mode (see "Navigation Tree" on page 45), configuration pages display all their parameters (i.e., the 'Advanced Parameter List' view is displayed).
- If a page contains only basic parameters, the **Basic Parameter List** button is not displayed.

3.1.6.2.2 Showing / Hiding Parameter Groups

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

Figure 3-8: Expanding and Collapsing Parameter Groups



3.1.6.3 Modifying and Saving Parameters


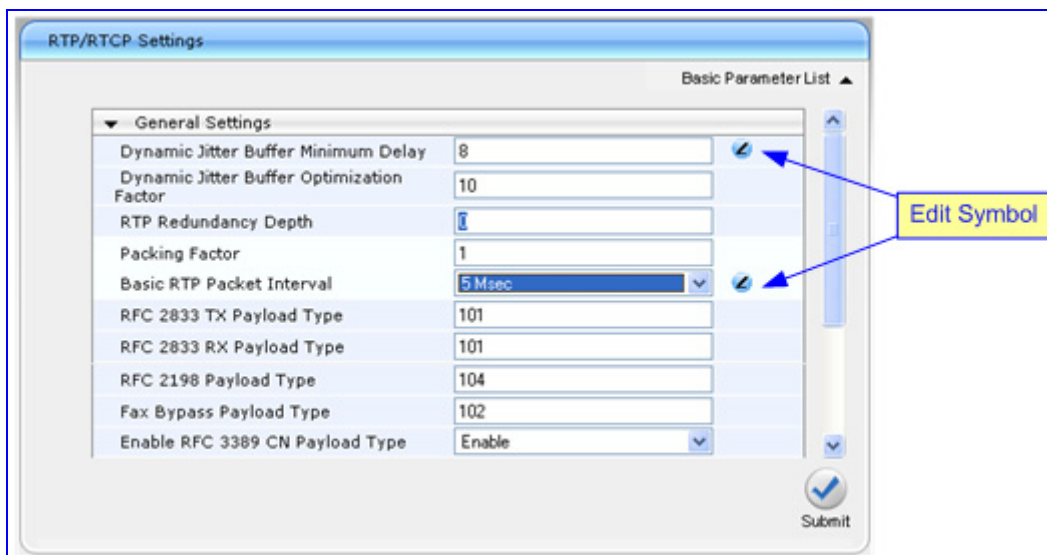


When you change parameter values on a page, the **Edit**  symbol appears to the right of these parameters. This is especially useful for indicating the parameters that you have currently modified (before applying the changes). After you save your parameter modifications (refer to the procedure described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

Figure 3-9: Edit Symbol after Modifying Parameter Value



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

- Click the **Submit**  button, which is located near the bottom of the page in which you are working; modifications to parameters with on-the-fly capabilities are immediately applied to the device and take effect; other parameters (displayed on the page with the lightning  symbol) are not changeable on-the-fly and require a device reset (see "Resetting the Device" on page 334) before taking effect.

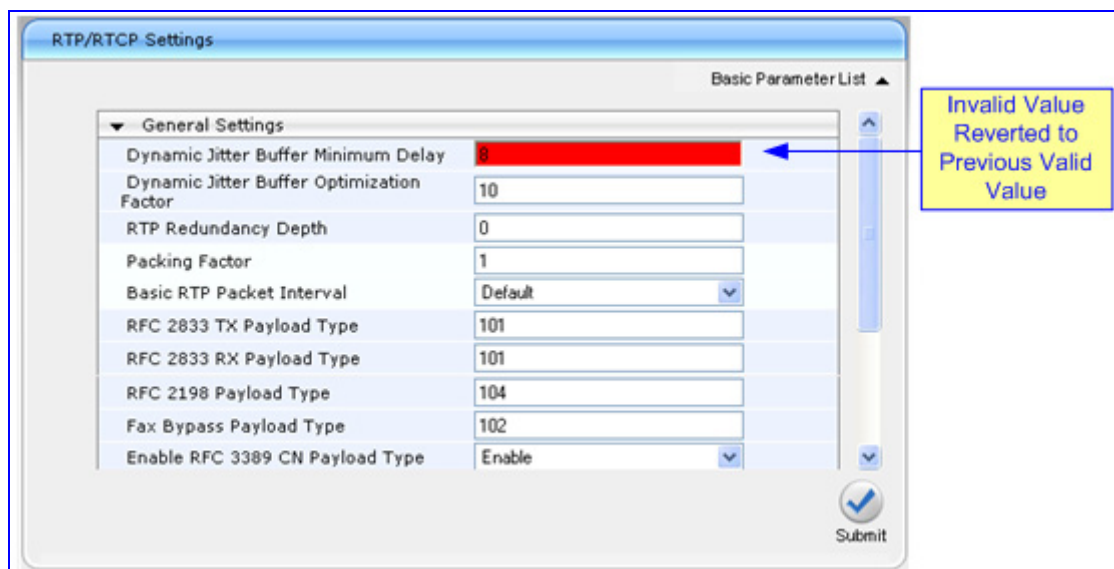


Notes:

- Parameters saved to the volatile memory (by clicking **Submit**), revert to their previous settings after a hardware or software reset (or if the device is powered down). Therefore, to ensure parameter changes (whether on-the-fly or not) are retained, you need to save ('burn') them to the device's non-volatile memory, i.e., flash (see "Saving Configuration" on page 336).
- If you modify a parameter value and then attempt to navigate away from the page without clicking **Submit**, a message box appears notifying you of this. Click **Yes** to save your modifications or **No** to ignore them.

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

Figure 3-10: Value Reverts to Previous Valid Value



3.1.6.4 Entering Phone Numbers

Phone numbers or prefixes that you need to configure throughout the Web interface must be entered only as digits without any other characters. For example, if you wish to enter the phone number 555-1212, it must be entered as 5551212 without the hyphen (-). If the hyphen is entered, the entry is invalid.

3.1.6.5 Working with Tables

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

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

➤ **To add an entry to a table:**

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

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

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:

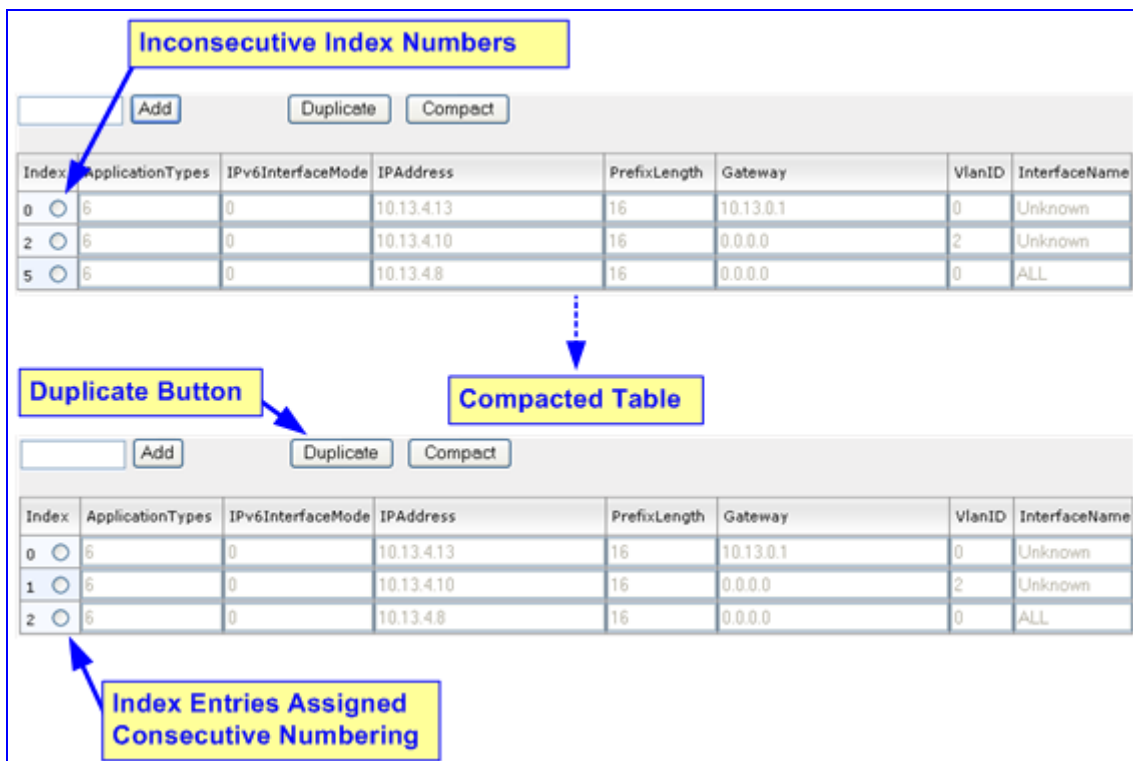
- Before you can add another index entry, you must ensure that you have applied the previously added index entry (by clicking **Apply**).
- If you leave the 'Add' field blank and then click **Add Index**, the existing index entries are all incremented by one and the newly added index entry is assigned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

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

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

- **To edit an existing index table entry:**
 1. In the 'Index' column, select the index corresponding to the table row that you want to edit.
 2. Click **Edit**; the fields in the corresponding index row become available.
 3. Modify the values as required, and then click **Apply**; the new settings are applied.
- **To organize the index entries in ascending, consecutive order:**
 - Click **Compact**; the index entries are organized in ascending, consecutive order, starting from index 0. For example, if you added three index entries 0, 4, and 6, then the index entry 4 is re-assigned index number 1 and the index entry 6 is re-assigned index number 2.

Figure 3-12: Compacting a Web Interface Table



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 where the indices are compacted to be consecutive.

Top Screenshot: 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

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

3.1.7 Searching for Configuration Parameters

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

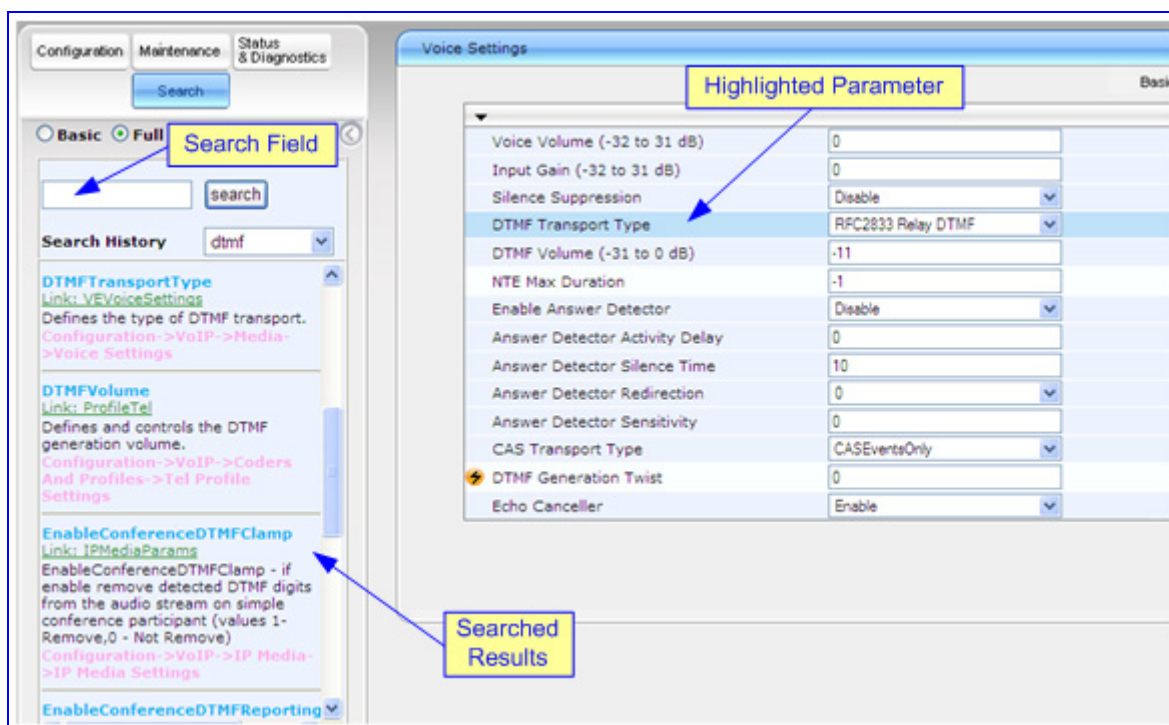
➤ **To search for *ini* file parameters configurable in the Web interface:**

1. On the Navigation bar, click the **Search** tab; the Search engine appears in the Navigation pane.
2. In the 'Search' field, enter the parameter name or sub-string of the parameter name that you want to search. If you have performed a previous search for such a parameter, instead of entering the required string, you can use the 'Search History' drop-down list to select the string (saved from a previous search).
3. Click **Search**; a list of located parameters based on your search appears in the Navigation pane.

Each searched result displays the following:

- *ini* file parameter name
 - Link (in green) to its location (page) in the Web interface
 - Brief description of the parameter
4. In the searched list, click the required parameter (link in green) to open the page in which the parameter appears; the relevant page opens in the Work pane and the searched parameter is highlighted for easy identification, as shown in the figure below:

Figure 3-13: Searched Result Screen



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

3.1.8 Creating a Login Welcome Message

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

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

Figure 3-14: User-Defined Web Welcome Message after Login

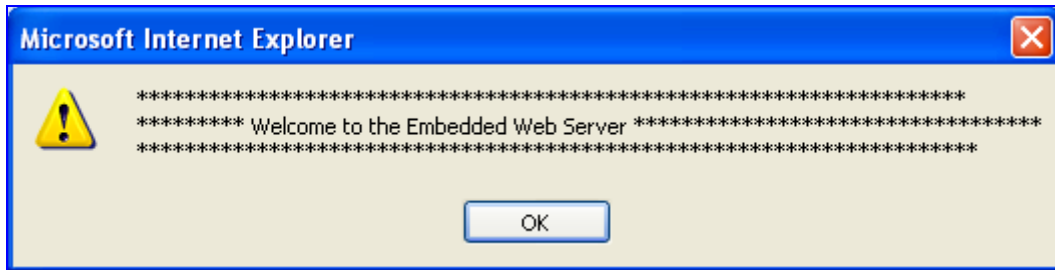


Table 3-2: ini File Parameter for Welcome Login Message

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

3.1.9 Getting Help

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

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


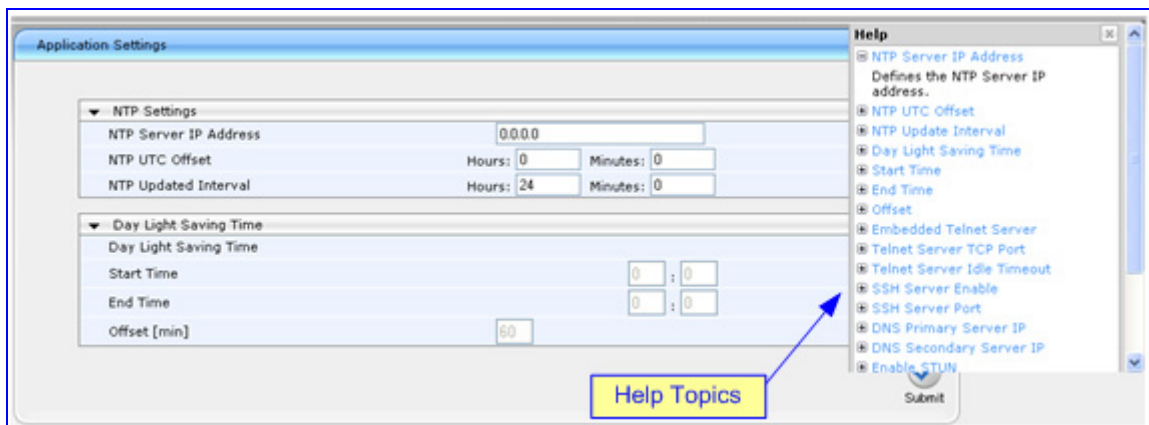




1. Using the Navigation tree, open the required page for which you want Help.
2. On the toolbar, click the **Help**  button; the Help topic pertaining to the opened page appears, as shown below:

Figure 3-15: Help Topic for Current Page



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



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

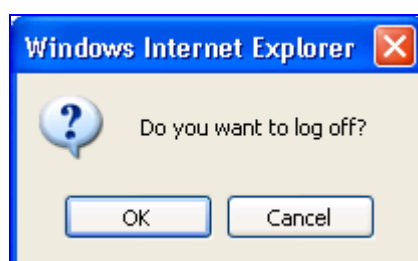
3.1.10 Logging Off the Web Interface

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

➤ **To log off the Web interface:**

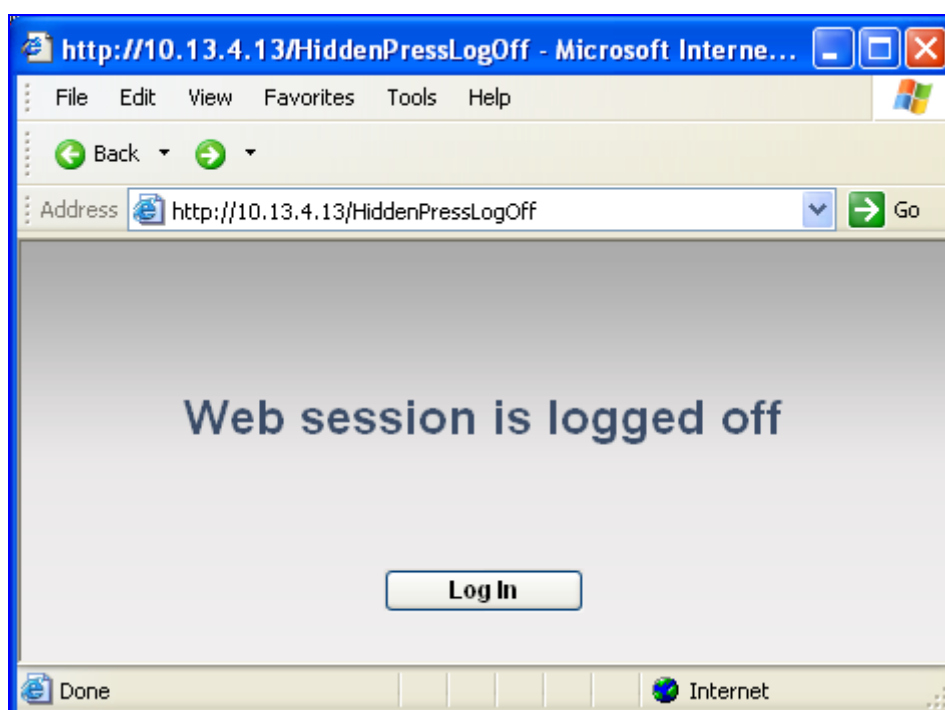
1. On the toolbar, click the **Log Off**  button; the Log Off confirmation message box appears:

Figure 3-16: Log Off Confirmation Box



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

Figure 3-17: Web Session Logged Off



To log in again, simply click the **Log In** button, and then in the 'Enter Network Password' dialog box, enter your user name and password (see "Accessing the Web Interface" on page 42).

3.2 Using the Home Page

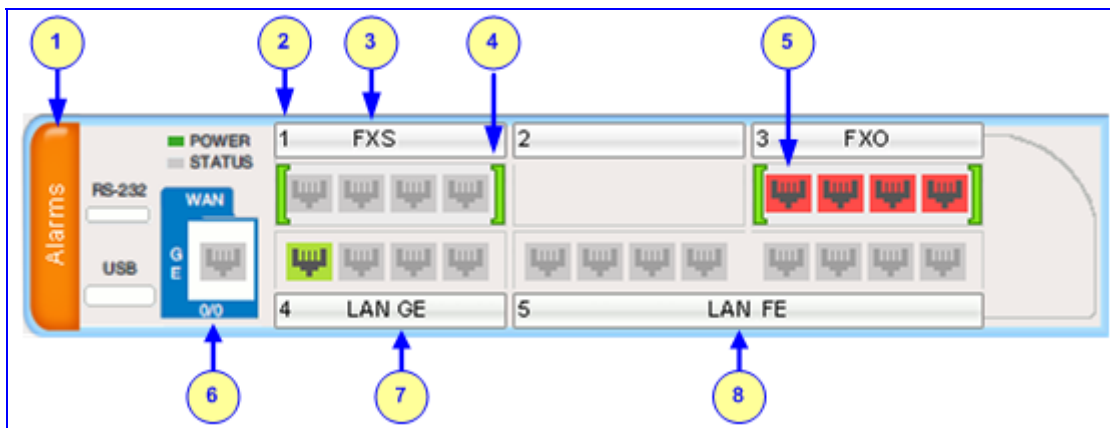
The 'Home' page provides you with a graphical display of the device's front panel, displaying color-coded status icons for monitoring the functioning of the device. The 'Home' page also displays general device information (in the 'General Information' pane) such as the device's IP address and firmware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

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

➤ **To access the Home page:**

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

Figure 3-18: Home Page



Note: The displayed number and type of telephony interface modules depends on the device's hardware configuration. The displayed WAN port type depends on the ordered hardware configuration (i.e., Gigabit Ethernet, T1, or SHDSL).

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 and FXO) ports (appears only if the device houses an FXS or FXO module)
- **Firmware Version:** software version currently running on the device
- **Protocol Type:** signaling protocol currently used by the device (i.e. SIP)
- **Gateway Operational State:** operational state of the device:













- LOCKED - device is locked (i.e. no new calls are accepted)
- UNLOCKED - device is not locked
- SHUTTING DOWN - device is currently shutting down

To perform these operations, see "Maintenance Actions" on page 333.

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

Table 3-3: 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 349), click the Alarms area.		
2	Module slot number (1 to 3).		
3	Module interface type: FXS, FXO, DIGITAL (i.e., E1/T1 PRI), and BRI.		
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.		
	Icon	Trunk Description (Digital Module)	Channel Description (Analog Modules)
	 (gray)	Disable: Trunk not configured (not in use)	Idle: 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 (FXO only)
	 (blue)	AIS Alarm: Alarm Indication Signal (AIS), also known as the Blue Alarm	Handset Offhook: Channel is off-hook, but there is no active RTP session
	 (orange)	D-Channel Alarm: D-channel alarm	-

Item #	Description
	<p>For trunk ports, you can view the status of trunk channels by clicking the trunk port icon (see Viewing Trunks' Channels on page 64).</p> <p>If you right-click a port, a shortcut menu appears allowing you to perform the following:</p> <ul style="list-style-type: none"> ▪ (Analog ports only) Reset the channel port (see Resetting an Analog Channel on page 62) ▪ View the channel's port settings (see "Viewing Analog Port Information" on page 63) ▪ Assign a name to the port (see "Assigning a Port Name" on page 62)
6	<p>WAN port status icons:</p> <ul style="list-style-type: none"> ▪  (green): link is working ▪  (gray): link is not configured ▪  (red): link error <p>To view port information, see Viewing WAN Port Information on page 348. Depending on ordered hardware configuration, the WAN port can be Gigabit Ethernet, T1, or SHDSL:</p> <div style="display: flex; justify-content: space-around; align-items: flex-end;"> <div style="text-align: center;"> <p>Gigabit Ethernet</p>  <p>One Port</p> </div> <div style="text-align: center;"> <p>T1 WAN</p>  <p>Two Ports</p> </div> <div style="text-align: center;"> <p>SHDSL</p>  <p>Four Ports</p> </div> </div>
7	<p>Gigabit Ethernet LAN port status icons:</p> <ul style="list-style-type: none"> ▪  (green): link is working ▪  (gray): link is not configured ▪  (red): link error <p>To view detailed port information, click the port icon (see Viewing Ethernet Port Information on page 348).</p>
8	<p>Fast Ethernet LAN port status icons:</p> <ul style="list-style-type: none"> ▪  (green): link is working ▪  (gray): link is not configured ▪  (red): link error <p>To view detailed port information, click the port icon (see Viewing Ethernet Port Information on page 348).</p>

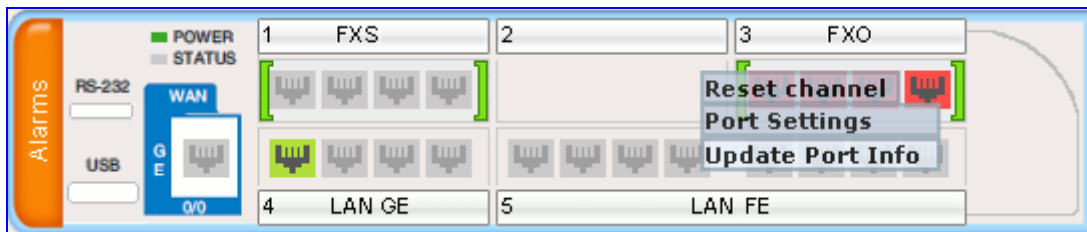
3.2.1 Assigning a Port Name

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

➤ **To add a port description:**

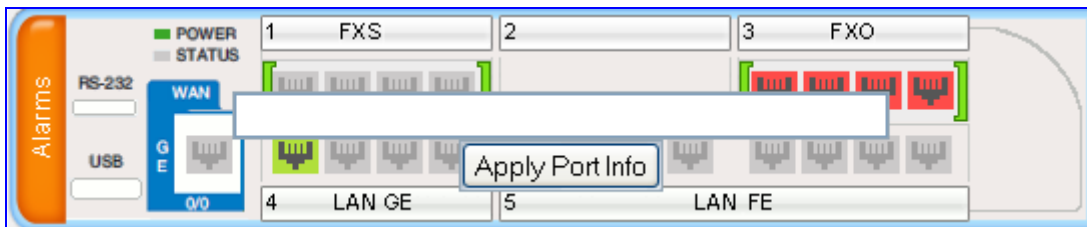
1. Click the required port icon; a shortcut menu appears, as shown below:

Figure 3-19: Shortcut Menu for Assigning Port Name



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

Figure 3-20: Text Box for Entering Port Name



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

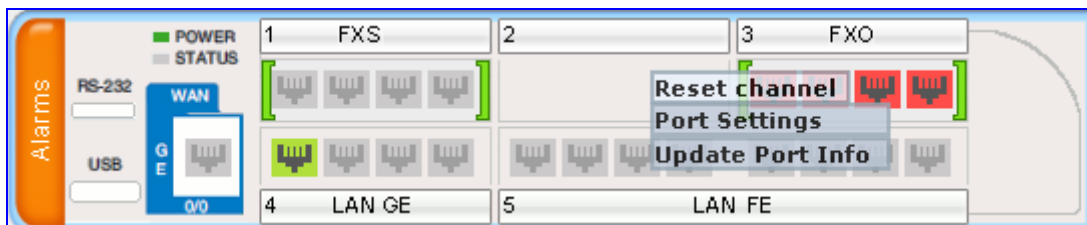
3.2.2 Resetting an Analog Channel

The 'Home' page allows you to inactivate (*reset*) an FXO or FXS analog channel. This is sometimes useful, for example, when the device (FXO) is connected to a PBX and the communication between the two can't be disconnected (e.g., when using reverse polarity).

➤ **To reset a channel:**

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

Figure 3-21: Shortcut Menu for Resetting Port



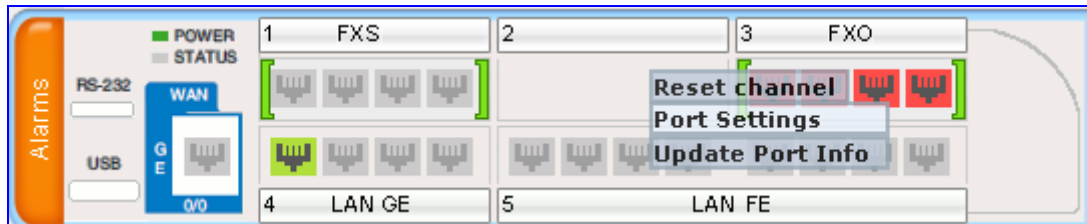
3.2.3 Viewing Analog Port Information

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

➤ **To view detailed port information:**

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

Figure 3-22: Shortcut Menu for Viewing Port Information



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

Figure 3-23: 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

3. 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 also view the trunk's configuration.

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







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

Figure 3-24: 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																																	

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 (Currently 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 detailed information on configuring the trunk in this page, see [Configuring the Trunk Settings](#) on page 101.)

3.3 Configuration Tab

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

- System (see "System Settings" on page 65)
- VoIP (see VoIP Settings on page 83)
- Data (see Data Settings on page 222)

3.3.1 System Settings

The **System** menu includes the following:

- Application Settings item (see "Configuring Application Settings" on page 65)
- Syslog Settings item (see "Configuring Syslog Settings" on page 68)
- Regional Settings item (see "Configuring Regional Settings" on page 69)
- Certificates item (see "Configuring Certificates" on page 69)
- Management submenu (see "Management Settings" on page 73)

3.3.1.1 Configuring Application Settings

The 'Application Settings' page is used for configuring various application parameters such as Network Time Protocol (NTP), daylight saving time, and Network File System (NFS). For a description of these parameters, see "Configuration Parameters Reference" on page 653.


➤ **To configure application settings:**

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

Figure 3-25: Applications Settings Page

The screenshot displays the 'Applications Settings' page with the following sections:

- NTP Settings**
 - NTP Server IP Address: 0.0.0.0
 - NTP UTC Offset: Hours: 0, Minutes: 0
 - NTP Updated Interval: Hours: 24, Minutes: 0
- Day Light Saving Time**
 - Day Light Saving Time: Disable (dropdown)
 - Start Time: Jan 01 0:00
 - End Time: Jan 01 0:00
 - Offset [min]: 60
- NFS Settings**
 - NFS Table: [icon]
- DHCP Settings**
 - Enable DHCP: Disable (dropdown)
 - Enable DHCP Lease Renewal: Disable (dropdown)

2. Configure the parameters as required.
3. For configuring NFS, under the 'NFS Settings' group, click the **NFS Table**  button; the 'NFS Settings' page appears. For a description of configuring this page, see "Configuring NFS Settings" on page 66.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.1.2 Configuring NFS Settings

Network File System (NFS) enables the device to access a remote server's shared files and directories, and to handle them as if they're located locally. You can configure up to 16 different NFS file systems. As a file system, the NFS is independent of machine types, operating systems, and network architectures. NFS is used by the device to load the *cmp*, *ini*, and auxiliary files, using the Automatic Update mechanism (refer to the *Product Reference Manual*). Note that an NFS file server can share multiple file systems. There must be a separate row for each remote file system shared by the NFS file server that needs to be accessed by the device.

➤ To add remote NFS file systems:


1. Open the 'Application Settings' page (see "Configuring Application Settings" on page 65).
2. Under the NFS Settings group, click the **NFS Table**  button; the 'NFS Settings' page appears.

Figure 3-26: NFS Settings Page

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

3. In the 'Add' field, enter the index number of the remote NFS file system, and then click **Add**; an empty entry row appears in the table.
4. Configure the NFS parameters according to the table below.
5. Click the **Apply** button; the remote NFS file system is immediately applied, which can be verified by the appearance of the 'NFS mount was successful' message in the Syslog server.
6. To save the changes to flash memory, see "Saving Configuration" on page 336.



Notes:

- To avoid terminating current calls, a row must not be deleted or modified while the device is currently accessing files on that remote NFS file system.
- The combination of 'Host Or IP' and 'Root Path' must be unique for each row in the table. For example, the table must include only one row with a Host/IP of 192.168.1.1 and Root Path of /audio.
- For an explanation on configuring Web interface tables, see "Working with Tables" on page 53.
- You can also configure the NFS table using the *ini* file table parameter NFSServers (see "NFS Parameters" on page 658).

Table 3-5: 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) Note: This parameter applies only if VLANs are enabled or if Multiple IPs is configured (see "Network Configuration" on page 620).

3.3.1.3 Configuring Syslog Settings

The 'Syslog Settings' page allows you to configure the device's embedded Syslog client. For a detailed description on the Syslog parameters, see "Syslog, CDR and Debug Parameters" on page 666. For a detailed description on Syslog messages and using third-party Syslog servers, refer to the *Product Reference Manual*.

➤ **To configure the Syslog client:**

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

Figure 3-27: Syslog Settings Page

▼ Syslog Settings	
Enable Syslog	Disable ▼
Syslog Server IP Address	
Syslog Server Port	514
Debug Level	0 ▼
Analog Ports Filter	-1
Trunks Ports Filter	-1

▼ 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 the **Submit** button to apply your changes.
3. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.1.4 Configuring Regional Settings

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

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

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

Figure 3-28: 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 SNTP server (see "Configuring Application Settings" on page 65), the fields on this page are read-only and cannot be modified.
- For an explanation on SNTP, see "Simple Network Time Protocol Support" on page 619.
- After performing a hardware reset, the date and time are returned to their defaults and therefore, should be updated.

3.3.1.5 Configuring Certificates

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

- Replacing the server certificate (see "Server Certificate Replacement" on page 70)
- Replacing the client certificates (see "Client Certificates" on page 71)
- Regenerating Self-Signed Certificates (see "Self-Signed Certificates" on page 72)
- Automatic update of the Private key (installed automatically from a file located on an HTTPS server, defined using the HTTPSPkeyFileName parameter). For a detailed description on automatic update methods, refer to the *Product Reference Manual*.



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

3.3.1.5.1 Server Certificate Replacement

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

➤ **To replace the device's self-signed certificate:**

1. Your network administrator should allocate a unique DNS name for the device (e.g., dns_name.corp.customer.com). This DNS name is used to access the device and therefore, must be listed in the server certificate.
2. If the device is operating in HTTPS mode, then set the HTTPSONly parameter to 'HTTP and HTTPS' (0) - see "Configuring Web Security Settings" on page 76. This ensures that you have a method for accessing the device in case the new certificate doesn't work. Restore the previous setting after testing the configuration.
3. Open the 'Certificates Signing Request' page (**Configuration** tab > **System** menu > **Certificates**).

Figure 3-29: Certificates Signing Request Page



4. In the 'Subject Name' field, enter the DNS name, and then click **Generate CSR**. A textual certificate signing request that contains the SSL device identifier is displayed.
5. Copy this text and send it to your security provider. The security provider (also known as Certification Authority or CA) signs this request and then sends you a server certificate for the device.
6. Save the certificate to a file (e.g., cert.txt). Ensure that the file is a plain-text file containing the 'BEGIN CERTIFICATE' header, as shown in the example of a Base64-Encoded X.509 Certificate below:

```
-----BEGIN CERTIFICATE-----
```

```
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJGUj
ETMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBTZXJ2ZXVy
MB4XDTE4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRLIxEz
ARBgNVBAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9zdGUxGzU2VydMVIcjcC
ASEwDQYJKoZIhvcNAQEBBQADggEADCCAQkCggEAPqd4MziR4spWldGRx8bQrhZkon
WnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7
JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRefiXDmuOe+FhJ
gHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
```

```
-----END CERTIFICATE-----
```

7. In the 'Certificates Files' group, click the **Browse** button corresponding to 'Send Server Certificate...', navigate to the cert.txt file, and then click **Send File**.
8. After the certificate successfully loads to the device, save the configuration (see "Saving Configuration" on page 336) and restart the device; the Web interface uses the provided certificate.
9. If the device was originally operating in HTTPS mode and you disabled it in Step 2, then return it to HTTPS by setting the parameter 'Secured Web Connection (HTTPS)' to 'HTTPS Only' (1) - see "Configuring Web Security Settings" on page 76.



Notes:

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

3.3.1.5.2 Client Certificates

By default, Web servers using SSL provide one-way authentication. The client is certain that the information provided by the Web server is authentic. When an organizational PKI is used, two-way authentication may be desired: both client and server should be authenticated using X.509 certificates. This is achieved by installing a client certificate on the managing PC, and loading the same certificate (in base64-encoded X.509 format) to the device's Trusted Root Certificate Store. The Trusted Root Certificate file should contain both the certificate of the authorized user and the certificate of the CA.

Since X.509 certificates have an expiration date and time, the device must be configured to use NTP (see "Simple Network Time Protocol Support" on page 619) to obtain the current date and time. Without the correct date and time, client certificates cannot work.

➤ To enable two-way client certificates:

1. Set the parameter 'Secured Web Connection (HTTPS)' to 'HTTPS Only' (0) in "Configuring Web Security Settings" on page 76 to ensure you have a method of accessing the device in case the client certificate doesn't work. Restore the previous setting after testing the configuration.
2. Open the 'Certificates Signing Request' page (see "Server Certificate Replacement" on page 70).

3. In the 'Certificates Files' group, click the **Browse** button corresponding to 'Send "Trusted Root Certificate Store" file ...', navigate to the file, and then click **Send File**.
4. When the operation is complete, set the `HTTPSRequireClientCertificate` *ini* file parameter to 1.
5. Save the configuration (see "Saving Configuration" on page 336), and then restart the device.

When a user connects to the secured Web server:

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



Notes:

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

3.3.1.5.3 Self-Signed Certificates

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

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

1. Before you begin, ensure the following:
 - You have a unique DNS name for the device (e.g., `dns_name.corp.customer.com`). This name is used to access the device and should therefore, be listed in the server certificate.
 - No traffic is running on the device. The certificate generation process is disruptive to traffic and should be executed during maintenance time.
2. Open the 'Certificates' page (see "Server Certificate Replacement" on page 70).
3. In the 'Subject Name' field, enter the fully-qualified DNS name (FQDN) as the certificate subject, and then click **Generate Self-signed**; after a few seconds, a message appears displaying the new subject name.
4. Save configuration (see "Saving Configuration" on page 336), and then restart the device for the new certificate to take effect.

3.3.1.6 Management Settings

The **Management** submenu includes the following:

- WEB User Accounts item (see "Configuring Web User Accounts" on page 73)
- Web Security Settings item (see "Configuring Web Security Settings" on page 76)
- Telnet/SSH Settings item (see "Configuring Telnet and SSH Settings" on page 76)
- WEB & Telnet Access List item (see "Configuring Web and Telnet Access List" on page 77)
- RADIUS Settings item (see "Configuring RADIUS Settings" on page 78)
- SNMP settings submenu (see "SNMP Settings" on page 78)

3.3.1.6.1 Configuring Web User Accounts

To prevent unauthorized access to the Web interface, two Web user accounts are available (primary and secondary) with assigned user name, password, and access level. When you login to the Web interface, you are requested to provide the user name and password of one of these Web user accounts. If the Web session is idle (i.e., no actions are performed) for more than five minutes, the Web session expires and you are once again requested to login with your user name and password. Up to five Web users can simultaneously open (log in to) a session on the device's Web interface.

Each Web user account is composed of three attributes:

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

Table 3-6: 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:

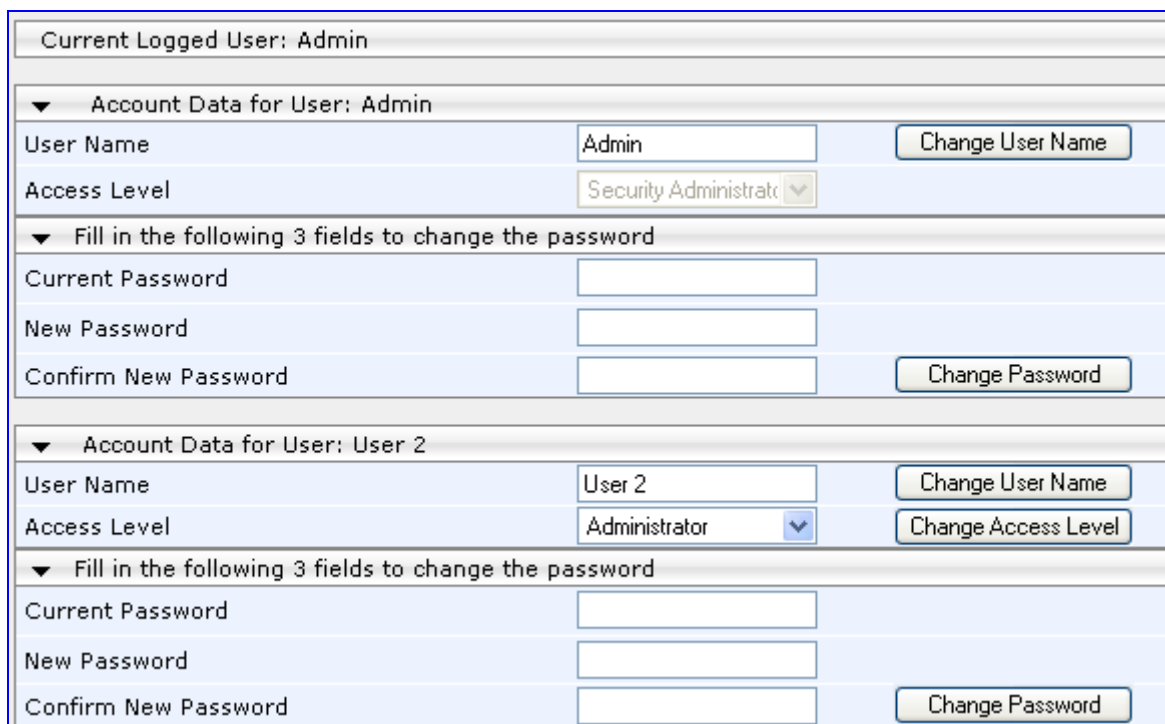
Table 3-7: Default Attributes for the Web User Accounts

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 3-30: WEB User Accounts Page (for Users with 'Security Administrator' Privileges)



The screenshot displays the 'WEB User Accounts' page. At the top, it shows 'Current Logged User: Admin'. Below this, there are two main sections for user configuration. The first section is for 'Admin', showing 'User Name' as 'Admin' and 'Access Level' as 'Security Administrator'. There is a 'Change User Name' button. The second section is for 'User 2', showing 'User Name' as 'User 2' and 'Access Level' as 'Administrator'. There is a 'Change Access Level' button. Both sections include a 'Fill in the following 3 fields to change the password' section with 'Current Password', 'New Password', and 'Confirm New Password' fields, and a 'Change Password' button.

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

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

**Notes:**

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

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

**Notes:**

- For security, it's recommended that you change the default user name and password.
- A Web user with access level 'Security Administrator' can change all attributes of all the Web user accounts. Web users with an access level other than 'Security Administrator' can only change their own password and user name.
- To reset the two Web user accounts' user names and passwords to default, set the *ini* file parameter ResetWebPassword to 1.
- To access the Web interface with a different account, click the **Log off** button located on the toolbar, click any button or page item, and then re-access the Web interface with a different user name and password.
- You can set the entire Web interface to read-only (regardless of Web user account's access level), by using the *ini* file parameter DisableWebConfig (see "Web and Telnet Parameters" on page 662).
- Access to the Web interface can be disabled, by setting the ini file parameter DisableWebTask to 1. By default, access is enabled.
- You can define additional Web user accounts using a RADIUS server (refer to the *Product Reference Manual*).
- For secured HTTP connection (HTTPS), refer to the *Product Reference Manual*.

3.3.1.6.2 Configuring Web Security Settings

The 'WEB Security Settings' page is used to define a secure Web access communication method. For a description of these parameters, see "Web and Telnet Parameters" on page 662.

➤ **To define Web access security:**

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

Figure 3-31: Web Security Page

HTTP Authentication Mode	Digest When Possible
Secured Web Connection (HTTPS)	HTTP and HTTPS
WAN HTTP Port	0
WAN HTTPS Port	0

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.1.6.3 Configuring Telnet and SSH Settings

The 'Telnet/SSH Settings' page is used to define Telnet and Secure Shell (SSH). For a description of these parameters, see "Web and Telnet Parameters" on page 662.

➤ **To define Telnet and SSH:**

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

Figure 3-32: Telnet/SSH Settings Page

Telnet Settings	
Embedded Telnet Server	Disable
Telnet Server TCP Port	23
Telnet Server Idle Timeout	5
SSH Server Enable	Disable
SSH Server Port	22
WAN Telnet Server Port	0
WAN SSH Server Port	0

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.1.6.4 Configuring Web and Telnet Access List

The 'Web & Telnet Access List' page is used to define IP addresses (up to ten) that are permitted to access the device's Web, Telnet, and SSH interfaces. Access from an undefined IP address is denied. If no IP addresses are defined, this security feature is inactive and the device can be accessed from any IP address. The Web and Telnet Access List can also be defined using the *ini* file parameter `WebAccessList_x` (see "Web and Telnet Parameters" on page 662).

➤ **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 3-33: Web & Telnet Access List Page - Add New Entry

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

Figure 3-34: Web & Telnet Access List Table

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

3. To delete authorized IP addresses, select the Delete Row check boxes corresponding to the IP addresses that you want to delete, and then click **Delete Selected Addresses**; the IP addresses are removed from the table and these IP addresses can no longer access the Web and Telnet interfaces.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.



Notes:

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

3.3.1.6.5 Configuring RADIUS Settings

The 'RADIUS Settings' page is used for configuring the Remote Authentication Dial In User Service (RADIUS) accounting parameters. For a description of these parameters, see "Configuration Parameters Reference" on page 653.

➤ **To configure RADIUS:**

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

Figure 3-35: 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.1.6.6 SNMP Settings

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

- SNMP Community Settings (see "Configuring SNMP Community Strings" on page 78)
- SNMP Trap Destinations (see "Configuring SNMP Trap Destinations" on page 80)
- SNMP Trusted Managers (see "Configuring SNMP Trusted Managers" on page 81)
- SNMP V3 Users (see "Configuring SNMP V3 Users" on page 81)

3.3.1.6.6.1 Configuring SNMP Community Strings

The 'SNMP Community String' page allows you to configure up to five read-only and up to five read-write SNMP community strings, and to configure the community string that is used for sending traps. For detailed information on SNMP community strings, refer to the *Product Reference Manual*. For detailed description on the SNMP parameters, see "SNMP Parameters" on page 679.

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

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

Figure 3-36: SNMP Community String Page

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

Disable SNMP

Trap Community String

Trap Manager Host Name

WAN SNMP Port

2. Configure the SNMP community strings parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

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

Table 3-8: 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'.

3.3.1.6.6.2 Configuring SNMP Trap Destinations

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

➤ **To configure SNMP trap destinations:**

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

Figure 3-37: 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.



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

Table 3-9: 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).

3.3.1.6.6.3 Configuring SNMP Trusted Managers

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

➤ **To configure SNMP Trusted Managers:**

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

Figure 3-38: 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 the **Submit** button to apply your changes.
5. To save the changes, see "Saving Configuration" on page 336.

3.3.1.6.6.4 Configuring SNMP V3 Users

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

➤ **To configure the SNMP v3 users:**

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

Figure 3-39: SNMP V3 Setting Page

Index	User Name	Authentication Protocol	Privacy Protocol	Authentication Key	Privacy Key	Group
1 <input type="radio"/>	SueM	MD5	DES	*	*	Read-Write
2 <input type="radio"/>	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 336.


Notes:

- For a description of the web interface's table command buttons (e.g., **Duplicate** and **Delete**), see "Working with Tables" on page 53.
- You can also configure SNMP v3 users using the *ini* file table parameter `SNMPUsers` (see "SNMP Parameters" on page 679).

Table 3-10: SNMP V3 Users Parameters

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

3.3.2 VoIP Settings

The VoIP menu includes the following main submenus:

- Network (see "Network" on page [83](#))
- TDM (see TDM on page [94](#))
- Security (see "Security" on page [94](#))
- PSTN (see PSTN on page [98](#))
- Media (see "Media" on page [103](#))
- Services (see Configuring LDAP Settings on page [112](#))
- Applications Enabling (see Enabling Applications on page [113](#))
- Control Network (see "Control Network" on page [113](#))
- SIP Definitions (see "SIP Definitions" on page [130](#))
- Coders And Profiles (see "Coders and Profiles" on page [138](#))
- GW and IP to IP (see "GW and IP to IP" on page [145](#))
- SBC (see SBC on page [194](#))
- SAS (see SAS on page [216](#))

3.3.2.1 Network

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

- IP Settings (see "Configuring IP Interface Settings" on page [83](#))
- IP Routing Table (see "Configuring the IP Routing Table" on page [88](#))
- QoS Settings (see "Configuring QoS Settings" on page [89](#))
- DNS (see "DNS" on page [91](#))

3.3.2.1.1 Configuring IP Interface Settings

The 'Multiple Interface Table' page allows you to configure up to 12 (up to 11 Control/Media interfaces and a single OAMP interface) logical VoIP network interfaces. Each interface can be defined with its own IP address, unique VLAN ID, arbitrary interface name, default gateway, and one of the following application types permitted on the interface:

- Control - call control signaling traffic (i.e., SIP)
- Media - RTP traffic
- Operations, Administration, Maintenance and Provisioning (OAMP) - management (such as Web- and SNMP-based management)

A combination of multiple IP addresses of IPv4 and IPv6 interfaces can be defined. However, only one interface (of IPv4 type) must be defined for OAMP; the rest being Media, Control, or a combination of Media and Control. The IPv6 Internet Layer protocol is based on the definition of a 128-bit address (as opposed to 32 bits for IPv4).

The default VoIP interface is as follows:

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

When using data-routing functionality, the network interfaces for the data-router are configured using the Data Settings menu (see Data Settings on page 222).



Notes:

- IPv6 interfaces are supported when the device operates with voice functionality only (i.e., without data-routing functionality). This support requires a special Software Upgrade Key for the device. For further information, contact AudioCodes.
- When operating with both voice and data-routing functionalities, it is recommended to define the default gateway IP address for the VoIP network interfaces in the same subnet and with the same VLAN ID as the IP address defined in the data-routing configuration section.
- For a detailed description and examples of VoIP network interfaces configuration, see "Network Configuration" on page 620.
- You can define firewall rules (access list) to deny (block) or permit (allow) packets received from a specific IP interface configured in this table. These rules are configured using the AccessList parameter (see "Configuring the Access List" on page 249).
- You can view currently active configured IP interfaces in the 'IP Active Interfaces' page (see "Viewing Active IP Interfaces" on page 350).
- You can also configure this table using the *ini* file table parameter InterfaceTable (see "Networking Parameters" on page 653).
- For an explanation on configuring Web interface tables, see "Working with Tables" on page 53.

➤ To configure VoIP network interfaces:

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

Figure 3-40: Multiple Interface Table Page

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	
0	<input type="radio"/>	OAMP + Media + Control	IPv4 Manual	10.33.4.124	16	10.33.0.1	1	Voice

WAN Interface Name

WAN Ethernet

2. In the 'Add Index' field, enter the desired index number for the new interface, and then click **Add Index**; the index row is added to the table.
3. Configure the interface according to the table below.
4. Click the **Apply** button; the interface is added to the table and the **Done** button appears.

5. Click **Done** to validate the interface. If the interface is not valid (e.g., if it overlaps with another interface in the table or if it does not adhere to the other rules as summarized in "Multiple Interface Table Configuration Summary and Guidelines" on page 627), a warning message is displayed.
6. Save the changes to flash memory and reset the device (see "Saving Configuration" on page 336).


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 350.

Table 3-11: Multiple Interface Table Parameters Description

Parameter	Description
Table parameters	
Index	Index of each interface. The range is 0 to 11.
Web: Application Type EMS: Application Types [InterfaceTable_ApplicationTypes]	<p>Types of applications that are allowed on the specific interface.</p> <ul style="list-style-type: none"> ▪ [0] OAMP = Only Operations, Administration, Maintenance and Provisioning (OAMP) applications (e.g., Web, Telnet, SSH, and SNMP) are allowed on the interface. ▪ [1] Media = Only Media (i.e., RTP streams of voice) is allowed on the interface. ▪ [2] Control = Only Call Control applications (e.g., SIP) are allowed on the interface. ▪ [3] OAMP + Media = Only OAMP and Media applications are allowed on the interface. ▪ [4] OAMP + Control = Only OAMP and Call Control applications are allowed on the interface. ▪ [5] Media + Control = Only Media and Call Control applications are allowed on the interface. ▪ [6] OAMP + Media + Control = All application types are allowed on the interface. <p>Notes:</p> <ul style="list-style-type: none"> ▪ A single OAMP interface (and only one) 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 interface for Media traffic and at least one interface for Control traffic must be configured. These interfaces can be combined (i.e., Media + Control, or OAMP + Media + Control). ▪ At least one IPv4 interface must be configured.

Parameter	Description
Web: Interface Mode [InterfaceTable_InterfaceMode]	<p>Determines the method that this interface uses to calculate its IP address.</p> <ul style="list-style-type: none"> ▪ [3] IPv6 Manual Prefix = IPv6 manual prefix IP address assignment. ▪ [4] IPv6 Manual = IPv6 manual IP address assignment. ▪ [10] IPv4 Manual = IPv4 manual IP address assignment. <p>Note: IPv6 interfaces are supported when the device operates with voice functionality only (i.e., without data-routing functionality). This support requires a special Software Upgrade Key for the device. For further information, contact AudioCodes.</p>
Web/EMS: IP Address [InterfaceTable_IPAddress]	<p>The IPv4/IPv6 IP address in dotted-decimal notation.</p>
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). The prefix length is a Classless Inter-Domain Routing (CIDR) style presentation of a dotted-decimal subnet notation. The CIDR-style presentation is the latest method for interpretation of IP addresses. Specifically, instead of using eight-bit address blocks, it uses the variable-length subnet masking technique to allow allocation on arbitrary-length prefixes (refer to http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing for more information). For IPv4 Interfaces, the prefix length values range from 0 to 31. For IPv6 interfaces, the prefix length must be set to 64.</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.
Web/EMS: VLAN ID [InterfaceTable_VlanID]	<p>Defines the VLAN ID for each interface.</p> <p>Note: The VLAN ID must be unique for each interface.</p>

Parameter	Description
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 'SIP Media Realm' and 'SIP Interface' tables.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is mandatory. ▪ The name must be unique for each interface.
WAN Interface Name [WanInterfaceName]	<p>Associates the WAN interface with the VoIP traffic (i.e., SIP signaling and media / RTP interfaces). The available WAN interface options depends on the hardware configuration (e.g., Ethernet, T1, or SHDSL) and/or whether VLANs are defined for the WAN interface (see Virtual LAN Interface (VLAN) on page 301). If VLANs are configured, for example, for the Ethernet WAN interface (see Data Settings on page 222), then you can select the WAN VLAN on which you want to run these SIP signaling and/or media interfaces.</p> <p>The WAN interface can be assigned to SIP signaling and media interfaces in the SIP Interface table (see Configuring SIP Interface Table on page 117) and SIP Media Realm table (see Configuring Media Realms on page 109), where the WAN interface is denoted as "WAN".</p> <p>Once this association is set, VoIP traffic is sent via the WAN and incoming traffic is identified as coming from the WAN. The device also automatically configures the required port forwarding and static NAT rules.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ If you do not assign the WAN interface to SIP and media interfaces, then the WAN interface may not be used for VoIP traffic. In such scenarios, the VoIP traffic can be sent and received within the LAN, or sent to the WAN via a third-party LAN router. If a third-party router is used as the interface to the WAN, then you need to define NAT rules (using the NATTranslation parameter) to translate the VoIP LAN IP addresses (defined in the Multiple Interface table and associated with SIP and media interfaces) into global, public IP addresses. ▪ This parameter is applicable only if the data-routing functionality is supported (i.e., relevant Software Upgrade Feature Key is installed on the device).

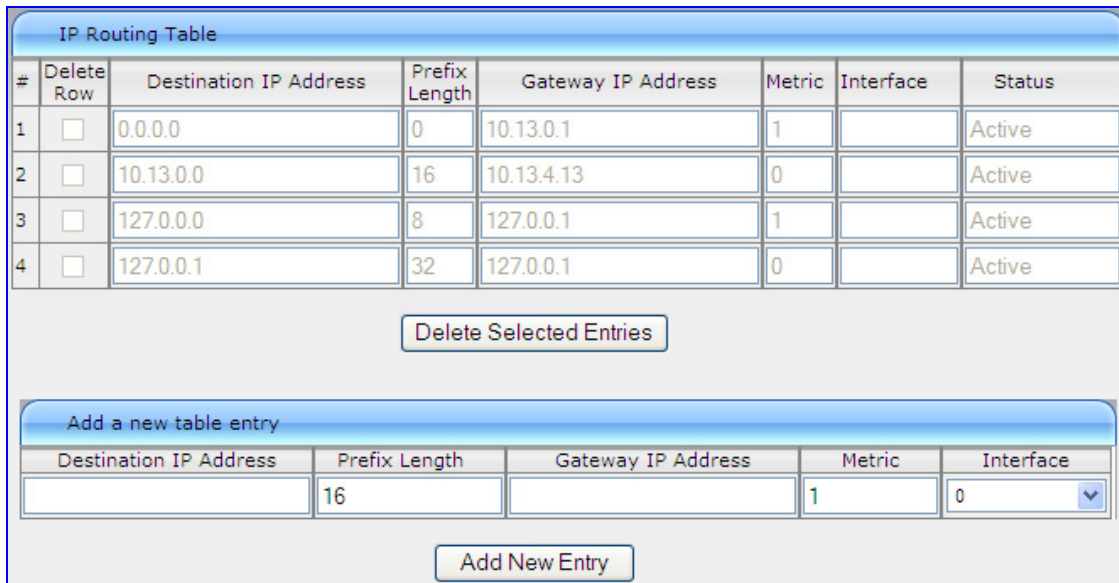
3.3.2.1.2 Configuring the IP Routing Table

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

➤ **To configure static IP routing:**

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

Figure 3-41: IP Routing Table Page



#	Delete Row	Destination IP Address	Prefix Length	Gateway IP Address	Metric	Interface	Status
1	<input type="checkbox"/>	0.0.0.0	0	10.13.0.1	1		Active
2	<input type="checkbox"/>	10.13.0.0	16	10.13.4.13	0		Active
3	<input type="checkbox"/>	127.0.0.0	8	127.0.0.1	1		Active
4	<input type="checkbox"/>	127.0.0.1	32	127.0.0.1	0		Active

Delete Selected Entries

Add a new table entry

Destination IP Address	Prefix Length	Gateway IP Address	Metric	Interface
	16		1	0

Add New Entry

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

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



Notes:

- You can delete only inactive routing rules.
- You can also configure the IP Routing table using the *ini* file table parameter StaticRouteTable.

Table 3-12: 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.

Parameter	Description
	<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. .</p>
Interface [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 83).</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

3.3.2.1.3 Configuring QoS Settings

The 'Diff Serv Table' page is used for configuring the Layer-2 and Layer-3 Quality of Service (QoS) parameters for VoIP. 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 Differentiated Services (DiffServ) to four classes of traffic (Media Premium, Control Premium, Gold, and Bronze) and to assign VLAN priorities (IEEE 802.1p) to various values of DiffServ. For a detailed description of the parameters appearing on this page, see "Networking Parameters" on page 653. For a description on QoS and the mapping of each application to a class of service, see "Quality of Service Parameters" on page 624.



Notes:

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

➤ **To configure QoS:**

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

Figure 3-42: DiffServ Table Page

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

▼ Differentiated Services

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

2. Configure DiffServ to VLAN priority mapping (Layer-2 QoS):
 - a. Enter an index entry, and then click Add.
 - b. In the 'Differentiated Services' field, enter the DiffServ value (0-63) and its corresponding VLAN priority level (0-7).
 - c. Click Apply.
3. Configure the desired DiffServ (Layer-3 QoS) values for the following traffic classes:
 - Media Premium QoS: this affects Media RTP packets sent by the VoIP towards the LAN.
 - Control Premium QoS: this affects Control Protocol (SIP) packets sent by the VoIP towards the LAN.
 - Gold QoS: this affects HTTP Streaming packets sent by the VoIP towards the LAN.
 - Bronze QoS: this affects OAMP packets sent by the VoIP towards the LAN.
4. Click the **Submit** button to save your changes.
5. Save the changes to flash memory and reset the device (see "Saving Configuration" on page 336).

3.3.2.1.4 DNS

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

- DNS Settings (refer to "Configuring DNS Settings" on page 91)
- Internal DNS Table (refer to "Configuring the Internal DNS Table" on page 91)
- Internal SRV Table (refer to "Configuring the Internal SRV Table" on page 92)

3.3.2.1.4.1 Configuring DNS Settings

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



Note: For a detailed description of the DNS parameters, refer to "DNS Parameters" on page 659.

➤ To define the DNS server:

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

Figure 3-43: DNS Settings Page

VoIP DNS Settings	
⚡ DNS Primary Server IP	<input type="text"/>
⚡ DNS Secondary Server IP	<input type="text"/>

2. In the 'DNS Primary Server IP' field, enter the IP address of the primary DNS server (in dotted-decimal notation, for example, 10.8.2.255).
3. Optionally, in the 'DNS Secondary Server IP', enter the IP address of the second DNS server (in dotted-decimal notation).
4. Click the **Submit** button to apply your changes.
5. Save the changes to flash memory (refer to "Saving Configuration" on page 336).

3.3.2.1.4.2 Configuring the Internal DNS Table

The 'Internal DNS Table' page, similar to a DNS resolution translates up to 20 host (domain) names into IP addresses (e.g., when using the '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).



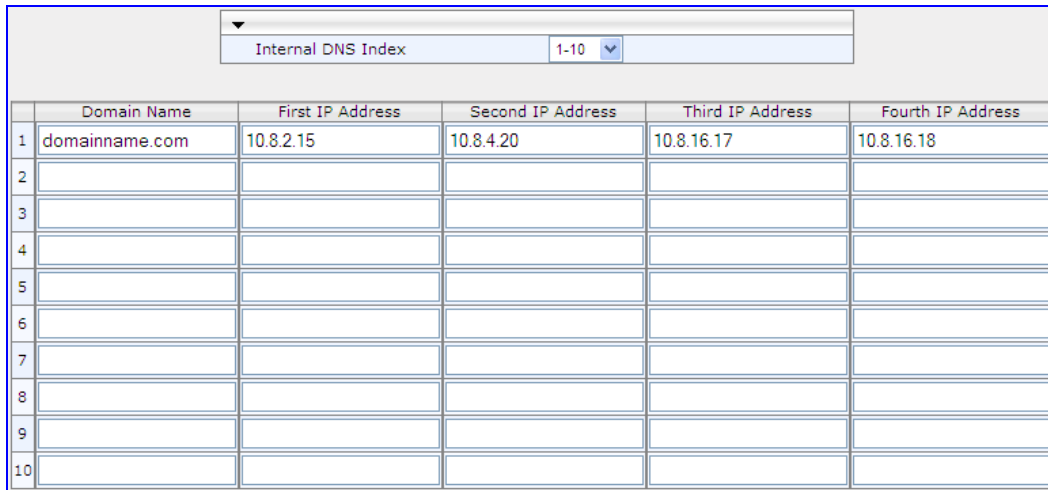
Notes:

- 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 "Configuring DNS Settings" on page 91).
- You can also configure the DNS table using the *ini* file table parameter DNS2IP (see "DNS Parameters" on page 659).

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

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

Figure 3-44: Internal DNS Table Page



	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 the **Submit** button to save your changes.
6. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.1.4.3 Configuring the Internal SRV Table

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



Notes:

- If the Internal SRV table is configured, the device initially attempts to resolve a domain name using this table. If the domain name isn't found, the device performs a Service Record (SRV) resolution using an external DNS server (defined in "Configuring DNS Settings" on page 91).
- You can also configure the Internal SRV table using the *ini* file table parameter SRV2IP (see "DNS Parameters" on page 659).

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

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

Figure 3-45: Internal SRV Table Page

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

2. In the 'Domain Name' field, enter the host name to be translated. You can enter a string of up to 31 characters.
3. From the 'Transport Type' drop-down list, select a transport type.
4. In the 'DNS Name 1' field, enter the first DNS A-Record to which the host name is translated.
5. In the 'Priority', 'Weight' and 'Port' fields, enter the relevant values
6. Repeat steps 4 through 5, for the second and third DNS names, if required.
7. Repeat steps 2 through 6, for each entry.
8. Click the **Submit** button to save your changes.
9. To save the changes so they are available after a hardware reset or power fail, see "Saving Configuration" on page 336.

3.3.2.2 TDM

The **TDM** submenu contains the following item:

- TDM (see Configuring TDM Bus Settings on page 94)

3.3.2.2.1 Configuring TDM Bus Settings

The 'TDM Bus Settings' page allows you to configure the device's Time-Division Multiplexing (TDM) bus settings. For detailed information on configuring the device's clock settings, see "Clock Settings" on page 637. For a description of these parameters, see "Configuration Parameters Reference" on page 653.

➤ To configure the TDM Bus settings:

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

Figure 3-46: TDM Bus Settings Page

PCM Law Select	ALaw	▼
TDM Bus Type	Framers	▼
Idle PCM Pattern	213	
Idle ABCD Pattern	0x0F	▼
TDM Bus Local Reference	1	
TDM Bus PSTN Auto FallBack Clock	Disable	▼
TDM Bus Clock Source	Network	▼

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. Save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.3 Security

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

- Firewall Settings (see "Configuring Firewall Settings" on page 94)
- General Security Settings (see "Configuring General Security Settings" on page 98)

3.3.2.3.1 Configuring Firewall Settings

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

The access list provides the following firewall rules:

- Block traffic from known malicious sources
- Only allow traffic from known friendly sources, and block all others
- Mix allowed and blocked network sources

- Limit traffic to a pre-defined rate (blocking the excess)
- Limit traffic to specific protocols, and specific port ranges on the device

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



Notes:

- It is recommended to add a rule at the end of your table that blocks all traffic and add firewall rules above it (in the table) that allow traffic (with bandwidth limitations). To block all traffic, the following must be set:
 - IP address to 0.0.0.0
 - Prefix length of 0 (implies the rule can match any IP address)
 - Local port range 0-65535
 - Protocol "Any"
 - Action Upon Match "block"
- You can also configure the firewall settings using the *ini* file table parameter AccessList (see "Security Parameters" on page 671).

➤ **To add firewall rules:**

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

Figure 3-47: Firewall Settings Page

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

2. In the 'Add' field, enter the index of the access rule that you want to add, and then click **Add**; a new firewall rule index appears in the table.
3. Configure the firewall rule's parameters according to the table below.
4. Click one of the following buttons:
 - **Apply**: saves the new rule (without activating it).
 - **Duplicate Rule**: adds a new rule by copying a selected rule.
 - **Activate**: saves the new rule and activates it.
 - **Delete**: deletes the selected rule.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

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 336.

➤ **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 336.

Table 3-13: Internal Firewall Parameters

Parameter	Description
Rule Status	A read-only field indicating whether the rule is active or not. Note: After device reset, all rules are active.
Source IP [AccessList_Source_IP]	IP address (or DNS name) or a specific host name of the source network (i.e., from where the incoming packet is received).
Prefix Length [AccessList_PrefixLen]	IP network mask. 32 for a single host, or the appropriate value for the source IP addresses. <ul style="list-style-type: none"> ▪ A value of 8 corresponds to IPv4 subnet class A

Parameter	Description
	<p>(network mask of 255.0.0.0).</p> <ul style="list-style-type: none"> 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>
Local Port Range [AccessList_Start_Port] [AccessList_End_Port]	<p>The destination UDP/TCP ports (on this device) to which packets are sent. The valid range is 0 to 65535. Note: When the protocol type isn't TCP or UDP, the entire range must be provided.</p>
Protocol [AccessList_Protocol]	<p>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>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 83).</p>
Packet Size [AccessList_Packet_Size]	<p>Maximum allowed packet size. The valid range is 0 to 65535.</p> <p>Note: When filtering fragmented IP packets, this field relates to the overall (re-assembled) packet size, and not to the size of each fragment.</p>
Byte Rate [AccessList_Byte_Rate]	<p>Expected traffic rate (bytes per second). This field defines the allowed bandwidth for the specified protocol. In addition to this field, the 'Burst Bytes' field provides additional allowance such that momentary bursts of data may utilize more than the defined byte rate, without being interrupted.</p> <p>For example, if 'Byte Rate' is set to 40000 and 'Burst Bytes' to 50000, then this implies the following: the allowed bandwidth is 40000 bytes/sec with extra allowance of 50000 bytes; if, for example, the actual traffic rate is 45000</p>

Parameter	Description
	bytes/sec, then this allowance would be consumed within 10 seconds, after which all traffic exceeding the allocated 40000 bytes/sec is dropped. If the actual traffic rate then slowed to 30000 bytes/sec, then the allowance would be replenished within 5 seconds.
Burst Bytes [AccessList_Byte_Burst]	Tolerance of traffic rate limit (number of bytes).
Action Upon Match [AccessList_Allow_Type]	Action upon match (i.e., 'Allow' or 'Block').
Match Count [AccessList_MatchCount]	A read-only field displaying the number of packets accepted/rejected by the specific rule.

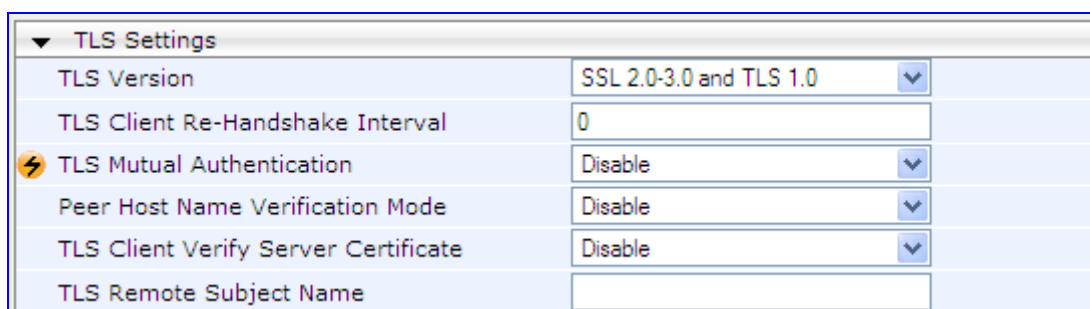
3.3.2.3.2 Configuring General Security Settings

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 653.

➤ To configure the general security parameters:

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

Figure 3-48: General Security Settings Page



TLS Settings	
TLS Version	SSL 2.0-3.0 and TLS 1.0
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	

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 336.

3.3.2.4 PSTN

The **PSTN** submenu allows you to configure various PSTN settings and includes the following page items:

- CAS State Machines (see "Configuring CAS State Machines" on page 99)
- Trunk Settings (see "Configuring Trunk Settings" on page 101)

3.3.2.4.1 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



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 a detailed description of the CAS Protocol table, refer to the *Product Reference Manual*.

➤ To modify the CAS state machine parameters:

1. Open the 'CAS State Machine' page (**Configuration** tab > **VoIP** menu > **PSTN** submenu > **CAS State Machines**).

Figure 3-49: CAS State Machine Page

CAS Protocol Enable Apply									
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 101), 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 334).



Table 3-14: 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).
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).
Collect 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.

3.3.2.4.2 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 783.



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**).

Figure 3-50: Trunk Scroll Bar (Used Only as an Example)

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

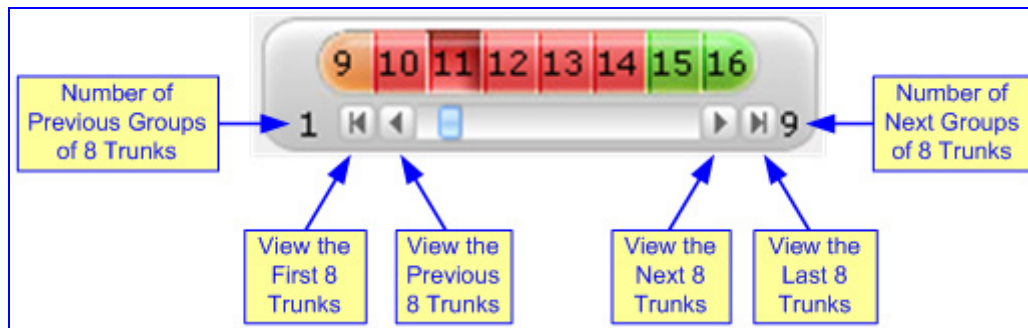
ISDN Configuration	
--------------------	--

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 3-51: 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 336.
7. To reset the device, see "Resetting the Device" on page 334.

**Notes:**

- If the 'Protocol Type' field displays 'NONE' (i.e., no protocol type is selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the device.
- The displayed parameters depend on the protocol selected.
- All PRI trunks of the device must be of the same line type (i.e., E1 or T1). However, different variants of the same line type can be configured on different trunks, for example, E1 Euro ISDN and E1 CAS (subject to the constraints in the device's Release Notes).
- BRI trunks can operate with E1 or T1 trunks.
- If the protocol type is CAS, you can assign or modify a dial plan (in the 'Dial Plan' field) and perform this without stopping the trunk.
- If the trunk can't be stopped because it provides the device's clock (assuming the device is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the device's clock or enable 'TDM Bus PSTN Auto Clock' in the 'TDM Bus Settings' page (see "TDM" on page 94).
- To delete a previously configured trunk, set the parameter 'Protocol Type' to 'None'.

3.3.2.5 Media

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

- Voice Settings (see "Configuring Voice Settings" on page 104)
- Fax/Modem/CID Settings (see Configuring Fax/Modem/CID Settings on page 105)
- RTP/RTCP Settings (see "Configuring RTP/RTCP Settings" on page 106)
- IPMedia Settings (see Configuring the IP Media Settings on page 107)
- General Media Settings (see "Configuring General Media Settings" on page 108)
- Analog Settings (see Configuring Analog Settings on page 108)
- Media Realms (see Configuring Media Realms on page 109)
- Media Security (see "Configuring Media Security" on page 111)



Note: Some channel parameters can be configured per channel or call routing, using profiles (see Coders and Profile Definitions on page 138).

3.3.2.5.1 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 653.

➤ **To configure the voice parameters:**

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

Figure 3-52: 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"/>
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"/>
Enable Answer Detector	<input type="text" value="Disable"/> ▼
Answer Detector Activity Delay	<input type="text" value="0"/>
Answer Detector Silence Time	<input type="text" value="10"/>
Answer Detector Redirection	<input type="text" value="0"/> ▼
Answer Detector Sensitivity	<input type="text" value="0"/>
⚡ DTMF Generation Twist	<input type="text" value="0"/>
Echo Canceller	<input type="text" value="Enable"/> ▼

2. Configure the Voice parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.5.2 Configuring Fax/Modem/CID Settings

The 'Fax/Modem/CID Settings' page is used for configuring fax, modem, and Caller ID (CID) parameters. For a detailed description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 653.

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

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

Figure 3-53: Fax/Modem/CID Settings Page

General Settings	
Fax Transport Mode	ByPassEnable
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
T38 Version	T.38 version 0
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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.



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 452).

3.3.2.5.3 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 653.

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

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

Figure 3-54: RTP/RTCP Settings Page

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

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 336.

3.3.2.5.4 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 653.

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

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

Figure 3-55: IPMedia Settings Page

▼ 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

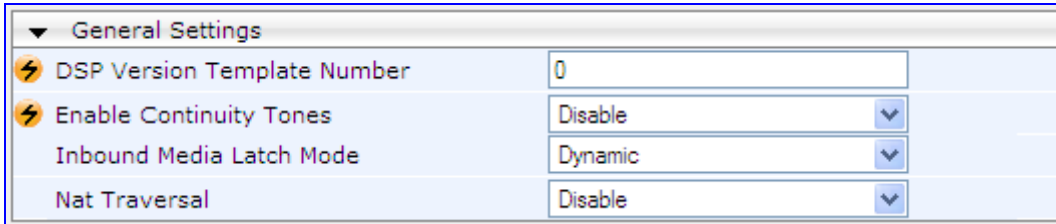
3.3.2.5.5 Configuring General Media Settings

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 653.

➤ **To configure general media parameters:**

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

Figure 3-56: General Media Settings Page



General Settings	
DSP Version Template Number	0
Enable Continuity Tones	Disable
Inbound Media Latch Mode	Dynamic
Nat Traversal	Disable

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.5.6 Configuring Analog Settings

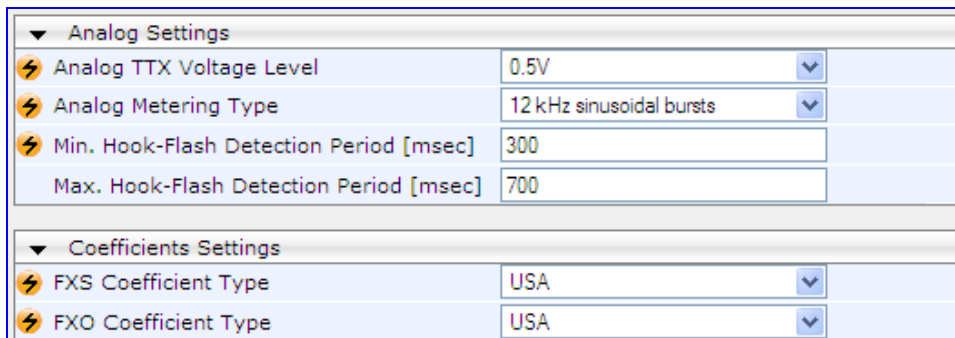
The 'Analog Settings' page allows you to configure various analog parameters. For a detailed description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 653.

This page also selects the type (USA or Europe) of FXS and/or FXO coefficient information. The FXS coefficient contains the analog telephony interface characteristics such as DC and AC impedance, feeding current, and ringing voltage.

➤ **To configure the analog parameters:**

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

Figure 3-57: 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.5.7 Configuring Media Realms

The 'SIP Media Realm Table' page allows you to define a pool of up to 64 SIP media interfaces, termed *Media Realms*. This table allows you to divide a Media-type interface (defined in the 'Multiple Interface' table - see "Configuring IP Interface Settings" on page 83) into several realms, where each realm is specified by a UDP port range. Once created, the Media Realm can be assigned to other elements such as an IP Group (in the 'IP Group' table) or an SRD (in the 'SRD' table).



Notes:

- You can also configure the Media Realm table using the *ini* file table parameter CpMediaRealm.
- 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.

➤ **To define a Media Realm:**

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

Figure 3-58: SIP Media Realm Table Page

2. In the 'Add Index' field, enter the required index number, and then click **Add Index**.
3. Configure the parameters according to the table below.
4. Click **Apply**; the entry is validated.
5. Click **Submit**.
6. Reset the device to save the changes to flash memory (see "Saving Configuration" on page 336).

Table 3-15: SIP Media Realm Table Parameters

Parameter	Description
Media Realm Name [CpMediaRealm_MediaRealmName]	<p>Defines an arbitrary, identifiable name for the Media Realm. The valid value is a string of up to 40 characters.</p> <p>Notes:</p> <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/or 'IP Groups' table.

Parameter	Description
IPv4 Interface Name [CpMediaRealm_IPv4IF]	<p>Associates the IPv4 interface to the Media Realm.</p> <p>Note: The name of this interface must be exactly (i.e., case-sensitive etc.) as configured in the 'Multiple Interface' table (InterfaceTable parameter). For the VoIP WAN IP address, you must enter the string "WAN" (case-sensitive).</p>
IPv6 Interface Name [CpMediaRealm_IPv6IF]	<p>Associates the IPv6 interface with the media realm.</p> <p>Note: The name of this interface must be exactly as configured in the 'Multiple Interface' table (InterfaceTable parameter).</p>
Port Range Start [CpMediaRealm_PortRangeStart]	<p>Defines the starting port for the range of Media interface UDP ports.</p> <p>Notes:</p> <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 as follows, using the BaseUDPport parameter: <ul style="list-style-type: none"> ✓ BaseUDPport to BaseUDPport + 255*10 Port ranges over 60000 must not be used. Ranges of Media Realm ports must not overlap.
Number of Media Session Legs [CpMediaRealm_MediaSessionLeg]	<p>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.</p>
Port Range End [CpMediaRealm_PortRangeEnd]	<p>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.</p>
Default Media Realm Name [cpDefaultMediaRealmName]	<p>Defines any one of the Media Realms listed in this table as the default Media Realm. This default Media Realm is used when no Media Realm is configured for an IP Group or SRD for a specific call.</p> <p>The valid range is a string of up to 39 characters.</p> <p>Notes:</p> <ul style="list-style-type: none"> If this parameter is not configured, then the first Media Realm configured in the SIP Media Realm table (cpMediaRealm) is used as the default Media Realm. If the SIP Media Realm table is not configured, then the default Media Realm includes all the device's media interfaces.

3.3.2.5.8 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 653.

➤ **To configure media security:**

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

Figure 3-59: Media Security Page

▼ 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	
◆ 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.6 Services

The **Services** submenu contains the following page item:

- LDAP Settings (see "Configuring LDAP Settings" on page 112)

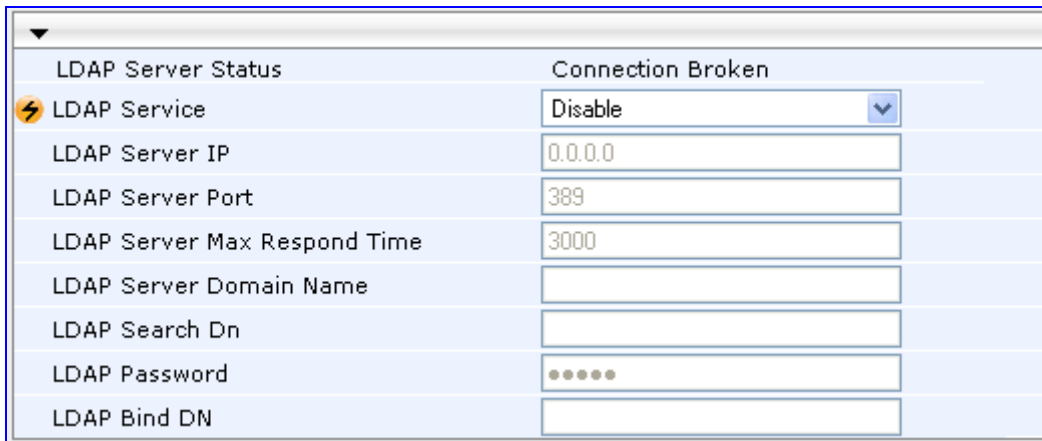
3.3.2.6.1 Configuring LDAP Settings

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 653. For an overview of LDAP, see "Routing Based on LDAP Active Directory Queries" on page 605.

➤ To configure the LDAP parameters:

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

Figure 3-60: LDAP Settings Page



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

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

- "Not Applicable"
 - "Connection Broken"
 - "Connecting"
 - "Connected"
2. Configure the parameters as required.
 3. Click the **Submit** button to save your changes.
 4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.7 Applications Enabling

3.3.2.7.1 Enabling Applications

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

- Stand-Alone Survivability (SAS) application
- Session Border Control (SBC) 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 339).
- The IP2IP application will only be supported in the next applicable release.
- For enabling an application, a device reset is required.

➤ **To enable an application:**

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

Figure 3-61: Applications Enabling Page

⚡ Enable SAS	Disable	▼
⚡ Enable SBC Application	Enable	▼
⚡ Enable IP2IP Application	Enable	▼

2. Save the changes to the device's flash memory and then reset the device (see "Saving Configuration" on page 336).

3.3.2.8 Control Network

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

- SRD Table (see Configuring SRD Table on page 114)
- SIP Interface Table (see Configuring SIP Interface Table on page 117)
- IP Group Table (see Configuring IP Groups on page 119)
- Proxy Sets Table (see Configuring Proxy Sets Table on page 126)

3.3.2.8.1 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 'SIP Media Realm' table - see "Configuring Media Realms" on page 109). In addition, other attributes such as media anchoring and user registration can also be configured.

Once configured, you can use the SRDs as follows:

- Associate it with a SIP Interface (see "Configuring SIP Interface Table" on page 117)
- Associate it with an IP Group (see Configuring IP Groups on page 119)
- Associate it with a Proxy Set (see Configuring Proxy Sets Table on page 126)
- Apply an Admission Control rule to it (see Configuring Admission Control Table on page 195)
- Define it as a Classification rule for the incoming SIP request (see Configuring Classification Table on page 198)
- Define it as a destination IP-to-IP routing rule (see "Configuring IP-to-IP Routing Table" on page 201)

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. Due to the B2BUA nature of the SBC application, different interfaces can be assigned to each leg of the call, and between the LAN and WAN side.
- Can operate with multiple gateway customers that may reside either in the same or in different Layer-3 networks as the device. This allows separation of signaling traffic between different customers. In such a scenario, the device is configured with multiple SRD's.

Typically, one SRD is defined for each group of SIP User Agents (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). One SRD is generally configured for the LAN and one for the WAN. Routing from one SRD to another is possible, whereby each routing destination (IP Group or destination address) indicates the SRD to which it belongs.

The 'SRD Settings' page 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 405.
- 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**).

Figure 3-62: SRD Settings Page

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 the **Submit** button to apply your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.



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 117.

Table 3-16: 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.

Parameter	Description
Media Realm [SRD_MediaRealm]	<p>Determines the media ports associated with the specific SRD. This is the name as defined in the 'SIP Media Realm' table (CpMediaRealm). The valid value is a string of up to 40 characters.</p> <p>Notes:</p> <ul style="list-style-type: none"> The string must be identical to that configured in the 'SIP Media Realm' table (i.e., case-sensitive etc.). If the Media Realm is later deleted from the 'SIP Media Realm' table, then this name becomes invalid in the SRD table.
Internal SRD Media Anchoring [SRD_IntraSRDMediaAnchoring]	<p>Determines whether the device performs media anchoring or not on media.</p> <ul style="list-style-type: none"> [0] Anchor Media (default) = RTP traverses the device and each leg uses a different coder or coder parameters. [1] Don't Anchor Media = The RTP packet flow does not traverse the device; instead, the two SIP UA's establish a direct RTP/SRTP (media) flow between one another. <p>Notes:</p> <ul style="list-style-type: none"> When No Media Anchoring is enabled: <ul style="list-style-type: none"> ✓ The device does not perform manipulation on SDP data (offer/answer transactions) such as ports, IP address, and coders. ✓ Opening voice channels and allocation of IP media ports are not required. When two UA's pertain to the same SRD and this parameter is set to [1], and one of the UA's is defined as a foreign user (example, "follow me service") located on the WAN while the other UA is located on the LAN, then calls between these two UA's can't be established until this parameter is set to 0, as the device doesn't interfere in the SIP signaling. In other words, parameters such as IP addresses are not manipulated for calls between LAN and WAN (although required). When the global parameter SBCDirectMedia is disabled, you cannot enable No Media Anchoring for two UA's pertaining to separate SRDs; No Media Anchoring can only be enable for two UA's pertaining to the same SRD. For a detailed description on media handling, see SBC Media Handling on page 493.
Block Unregistered Users [SRD_BlockUnRegUsers]	<p>Determines whether the device blocks incoming calls (INVITE requests) from unregistered users (pertaining to USER-type IP Groups).</p> <ul style="list-style-type: none"> [0] No = Calls from unregistered users are not blocked (default) [1] Yes = blocks unregistered users <p>Note: When the call is rejected, the device sends a SIP 500 "Server Internal Error" response to the remote end.</p>
Max Number of Registered Users [SRD_MaxNumOfRegUsers]	<p>Maximum number of users belonging to this SRD that can register with the device. By default, no limitation exists for registered users</p>

Parameter	Description
Enable Un-Authenticated Registrations [SRD_EnableUnAuthenticatedRegistrations]	<p>Determines whether the device blocks REGISTER requests from new users (i.e., users not registered in the device's registration database) when the destination IP Group is of type USER.</p> <ul style="list-style-type: none"> ▪ [0] No = The device sends REGISTER requests to the SIP proxy server and only if authenticated by the server does the device add the user registration to its database. ▪ [1] Yes = The device adds REGISTER requests to its database even if the requests are not authenticated by a SIP proxy (default).

3.3.2.8.2 Configuring SIP Interface Table

The 'SIP Interface Table' page allows you to configure up to 32 SIP Interfaces. A SIP Interface represents a SIP signaling interface (IPv4/IPv6), which is a combination of ports (UDP, TCP, and TLS) associated with a specific IP address (LAN or WAN) for a specific application (i.e., SAS, Gateway/IP2IP, and SBC) and associated with an SRD. SIP Interfaces allow you to use different SIP signaling interfaces for each call leg (i.e., each SIP user agent communicates with a specific SRD).

SIP Interfaces can be used for the following:

- Creating different SIP signaling ports (listening UDP, TCP, and TLS, and the UDP source ports) for a single interface or for multiple interfaces
- Differentiating between different device applications (i.e., SAS, Gateway\IP2IP, and SBC), 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:

- 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 only one SIP Interface per application for an SRD. In other words, each SRD may be associated with up to three SIP Interfaces (one per application type - SAS, Gateway\IP-to-IP, and SBC).
- The IP-to-IP application will only be supported in the next applicable release.
- The SIP Interface table also appears in the 'SRD Settings' page (see "Configuring SRD Table" on page 114), allowing you to add SIP interfaces there as well.
- For a detailed description of SIP interfaces, see "Multiple SIP Signaling/Media Interfaces Environment" on page 405.
- 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**).

Figure 3-63: SIP Interface Table Page

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	<input type="radio"/> Voice	SBC	5060	5060	5061	1
2	<input type="radio"/> Voice	GW/IP2IP	5070	5070	5071	1
3	<input type="radio"/> WAN	SBC	5080	5080	5081	2
4	<input type="radio"/> WAN	GW/IP2IP	5090	5090	5091	2

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 336.

Table 3-17: SIP Interface Table Parameters

Parameter	Description
Network Interface [SIPInterface_NetworkInterface]	Corresponding IP network interface name, as configured in the 'Multiple Interface' table (InterfaceTable). The default is "Not Configured". Notes: <ul style="list-style-type: none"> ▪ The value of this parameter must be identical (including case-sensitive) to that configured for the 'Interface Name' in the 'Multiple Interface' table (see "Configuring IP Interface Settings" on page 83). ▪ To create a SIP interface on the WAN interface, enter the string "WAN". This WAN interface is selected in the 'Multiple Interface' table (see Configuring IP Interface Settings on page 83 or use the WANInterfaceName parameter), which is the WAN interface address as defined in WAN Access Settings on page 224. If VLANs are defined for the WAN interface and one of the VLANs is selected as the VoIP WAN interface, then the defined SIP Interface uses this interface.
Application Type [SIPInterface_ApplicationType]	Determines 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 ▪ [2] SBC = SBC application Note: The IP-to-IP application will be supported in the next applicable release.
UDP Port [SIPInterface_UDPPort]	Determines the listening and source UDP port. The valid range is 1 to 65534. The default is 5060. Note: This port must be outside of the RTP port range.

Parameter	Description
TCP Port [SIPInterface_TCPort]	Determines the listening TCP port. The valid range is 1 to 65534. The default is 5060. Note: This port must be outside of the RTP port range.
TLS Port [SIPInterface_TLSPort]	Determines the listening TLS port. The valid range is 1 to 65534. The default is 5061. Note: This port must be outside of the RTP port range.
SRD [SIPInterface_SRD]	The SRD ID (configured in the SRD table as described in "Configuring SRD Table" on page 114) associated with the SIP Interface. The default SRD is 0. Note: Each SRD can be associated with up to three SIP Interfaces, where each SIP Interface pertains to a different Application Type (GW/IP2IP, SAS, and SBC).

3.3.2.8.3 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 126), which represents the IP address of the IP Group.

IP Groups provide the following uses:

- SIP dialog registration and authentication (digest user/password) of a specific IP Group (*Served IP Group*, e.g., corporate IP-PBX) with another IP Group (*Serving IP Group*, e.g., ITSP). This is configured in the 'Account' (see "Configuring Account Table" on page 133).
- 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 Hunt Group Settings" on page 148).
 - 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
- For the SBC application, IP Groups are used to classify incoming SIP dialog-initiating requests (e.g., INVITE messages) to a source IP Group, based on Proxy Set ID (defined in Configuring Classification Table on page 198). This occurs if the database search for a registered user is unsuccessful. The classification process locates a Proxy Set ID (associated with the SIP dialog request's IP address) in the Proxy Set table, and then locates a match with an IP Group that is associated with this Proxy Set in the IP Group table. This classification is enabled using the parameter Classify By Proxy Set.


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 SIP Configuration Parameters).

➤ **To configure IP Groups:**

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

Figure 3-64: IP Group Table

▼	
Index	1 ▼
▼ Common Parameters	
Type	SERVER ▼
Description	ITSP[
Proxy Set ID	1 ▼
SIP Group Name	
Contact User	
⚡ SRD	1
⚡ Media Realm	lan ▼
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	
▼ SBC Parameters	
Classify By Proxy Set	Enable ▼
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1

2. Configure the IP group parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

Table 3-18: 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. Typically, this IP Group is configured with a Serving IP Group that represents an IP-PBX, Application or Proxy server that serves this USER-type IP Group. Each SIP request sent by a user of this IP Group is proxied to the Serving IP Group. For registrations, the device updates its internal database with the AOR and contacts of the users. Digest authentication using SIP 401/407 responses (if needed) is performed by the Serving IP Group. The device forwards these responses directly to the SIP users. To route a call to a registered user, a rule must be configured in the 'Outbound IP Routing Table' table (see Configuring the Outbound IP Routing Table). The device searches the dynamic database (by using the request URI) for an entry that matches a registered AOR or Contact. Once an entry is found, the IP destination is obtained from this entry, and a SIP request is sent to the destination. The device also supports NAT traversal for the SIP clients that are behind NAT. In this case, the device must be defined with a global IP address. ▪ [2] GATEWAY = This is applicable only to the SBC application in scenarios where the device receives requests to and from a gateway representing multiple users. This IP Group type is necessary as the other IP Group types are not suitable: <ul style="list-style-type: none"> ✓ The IP Group cannot be defined as a SERVER since its destination address is unknown during configuration. ✓ The IP Group cannot be defined as a USER since the SIP Contact header of the incoming REGISTER does not represent a specific user. The Request-URI user part can change and therefore, the device is unable to identify an already registered user and therefore, adds an additional record to the database. <p>The IP address of the "GATEWAY" IP Group is obtained dynamically from the host part of the Contact header in the REGISTER request received from the IP Group. Therefore, routing to this IP Group is possible only once a REGISTER request is received. If a REGISTER refresh request arrives, the device updates the new location (i.e., IP address) of the IP Group. If the REGISTER fails, no update is performed. If an UN-REGISTER request arrives, the IP address associated with the IP Group is deleted and therefore, no</p>

Parameter	Description
	<p>routing to the IP Group is done.</p> <p>Notes:</p> <ul style="list-style-type: none"> This field is available only if the SBC or IP-to-IP application is enabled. (The IP-to-IP application will be supported in the next applicable release.) Currently, the GATEWAY IP Group type can only be configured using the IPGroup ini file parameter.
Description [IPGroup_Description]	<p>Brief string description of the IP Group.</p> <p>The value range is a string of up to 29 characters. The default is an empty field.</p>
Proxy Set ID [IPGroup_ProxySetId]	<p>The Proxy Set ID (defined in "Configuring Proxy Sets Table" on page 126) 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> <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]	<p>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 136) is used instead.</p> <p>The value range is a string of up to 100 characters. The default is an empty field.</p> <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]	<p>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> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only to USER-type IP Groups. This parameter is overridden by the 'Contact User' parameter in the 'Account' table (see "Configuring Account Table" on page 133).
SRD [IPGroup_SRD]	<p>The SRD (defined in Configuring SRD Table on page 114) associated with the IP Group.</p> <p>The default is 0.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>

Parameter	Description
Media Realm [IPGroup_MediaRealm]	The Media Realm name (defined in Configuring Media Realms on page 109) associated with this IP Group. This value must be identical (including case-sensitive) to that defined in the Media Realm table Note: For this parameter to take effect, a device reset is required.
IP Profile ID [IPGroup_ProfileId]	The IP Profile (defined in to "Configuring IP Profile Settings" on page 143) 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 165) 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 the Outbound IP Routing Table). (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 136).▪ [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 SBC or IP-to-IP application is enabled. (The IP-to-IP application will be supported in the next applicable release.)▪ 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).

Parameter	Description
	<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 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 redirected calls. ▪ This parameter is ignored if the parameter AlwaysSendToProxy is set to 1.
Enable Survivability [IPGroup_EnableSurvivability]	<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 SBC or IP-to-IP application is enabled. (The IP-to-IP application will be supported in the next applicable release.) ▪ This parameter is applicable only to USER-type IP Groups.

Parameter	Description
Serving IP Group ID [IPGroup_ServingIPGroup]	<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 SBC or IP-to-IP application is enabled. (The IP-to-IP application will be supported in the next applicable release.) 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'.
SBC Parameters	
Classify By Proxy Set [IPGroup_ClassifyByProxySet]	<p>Determines whether the incoming INVITE is classified to an IP Group according to the Proxy Set.</p> <ul style="list-style-type: none"> [0] Disable [1] Enable (default) <p>This classification occurs only if classification according to the device's database fails for locating whether the INVITE arrived from a registered user. The classification proceeds with checking whether the INVITE's IP address (if host names, then according to the dynamically resolved IP address list) is defined in the IP Group's Proxy Set ID (in the Proxy Set table). If the IP address is listed, then the INVITE is assigned to this IP Group.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only to SERVER-type IP Groups. This classification is not relevant in cases where multiple IP Groups use the same Proxy Set.
Max Number Of Registered Users	<p>Maximum number of users belonging to this IP Group that can register with the device. By default, no limitation exists for registered users.</p> <p>Note: This field is applicable only to USER-type IP Groups.</p>
Inbound Message Manipulation Set	<p>Message Manipulation Set (rule) that you want to assign to this IP Group for SIP message manipulation rule on the inbound message. The Message Manipulation rules are configured using the MessageManipulations parameter (see Configuring Message Manipulations on page 206).</p>
Outbound Message Manipulation Set	<p>Message Manipulation Set (rule) that you want to assign to this IP Group for SIP message manipulation on the outbound message. The Message Manipulation rules are configured using the MessageManipulations parameter (see Configuring Message Manipulations on page 206).</p>

3.3.2.8.4 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 119). 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.



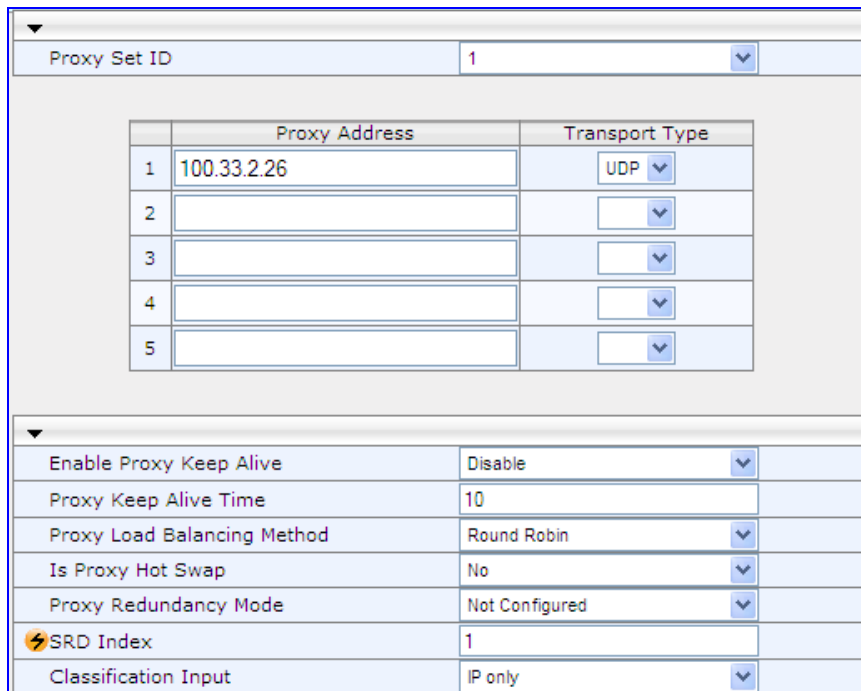
Notes:

- You can also configure the Proxy Sets table using two complementary *ini* file table parameters (see SIP Configuration Parameters):
 - ProxyIP: used for creating a Proxy Set ID defined with IP addresses.
 - ProxySet: used for defining various attributes for the Proxy Set ID.
- Proxy Sets can be assigned only to SERVER-type IP Groups.
- Each IP Group can be classified according to its Proxy Set ID, if in the IP Group table the parameter ClassifyByProxySet is enabled.

➤ To add Proxy servers:

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

Figure 3-65: Proxy Sets Table Page



The screenshot shows the 'Proxy Sets Table' configuration page. At the top, there is a dropdown menu for 'Proxy Set ID' with the value '1' selected. Below this is a table with 5 rows for adding proxy servers. The first row is populated with '100.33.2.26' and 'UDP'. The other four rows are empty. Below the table is a section for proxy settings with the following fields:

Proxy Address	Transport Type
100.33.2.26	UDP

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 the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

Table 3-19: 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, on the 'Hunt Group Settings' page (see "Configuring Hunt Group Settings" on page 148) you can configure a Serving IP Group to where you want to route specific Hunt Group's channels, while all other device channels use the default Proxy Set. At the same, you can also use IP Groups in the 'Outbound IP Routing Table' (see "Configuring the Outbound IP Routing Table" on page 165) to configure the default Proxy Set if the parameter PreferRouteTable is set to 1.</p> <p>To summarize, if the default Proxy Set is used, the INVITE message is sent according to the following preferences:</p> <ul style="list-style-type: none"> ▪ To the Hunt Group's Serving IP Group ID, as defined in the 'Hunt 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 133).</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</p>

Parameter	Description
	<p>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 130).</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 REGISTER messages. <p>If set to 'Using Options', the SIP OPTIONS message is sent every user-defined interval (configured by the parameter ProxyKeepAliveTime). If set to 'Using Register', the SIP REGISTER message is sent every user-defined interval (configured by the RegistrationTime parameter for the GW/IP2IP application or by the SBCProxyRegistrationTime parameter for SBC application). Any response from the Proxy, either success (200 OK) or failure (4xx response) is considered as if the Proxy is communicating correctly.</p> <p>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,

Parameter	Description
	using the UsePingPongKeepAlive parameter.
Web: Proxy Keep Alive Time EMS: Keep Alive Time [ProxySet_ProxyKeepAliveTime]	<p>Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages. This parameter is configured per Proxy Set.</p> <p>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 for the GW/IP2IP application or by the SBCProxyRegistrationTime parameter for SBC application.</p>
Web: Proxy Load Balancing Method EMS: Load Balancing Method [ProxySet_ProxyLoadBalancingMethod]	<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'. All outgoing messages are equally distributed across the list of IP addresses. REGISTER messages are also distributed unless a RegistrarIP is configured. The IP addresses list is refreshed according to ProxyIPListRefreshTime. If a change in the order of the entries in the list occurs, all load statistics are erased and balancing starts over again.</p> <p>When the Random Weights algorithm is used, the outgoing requests are not distributed equally among the Proxies. The weights are received from the DNS server by using SRV records. The device sends the requests in such a fashion that each Proxy receives a percentage of the requests according to its assigned weight. A single FQDN should be configured as a Proxy IP address. The Random Weights Load Balancing is not used in the following scenarios:</p> <ul style="list-style-type: none"> ▪ 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</p>

Parameter	Description
	HotSwapRtx), the message is resent to the next redundant Proxy/Registrar server.
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 114) 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.
Web/EMS: Classification Input [ClassificationInput]	<p>Classifies an IP call to a Proxy Set, based on either its IP address, or based on its IP address, port, and transport type:</p> <ul style="list-style-type: none"> ▪ [0] Compare only IP = IP call classified to Proxy Set according to IP address only (default). ▪ [1] Compare IP, port and transport type = IP call classified to Proxy Set according to IP address, port, and transport type.

3.3.2.9 SIP Definitions

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

- General Parameters (see "Configuring SIP General Parameters" on page 130)
- Advanced Parameters (see "Configuring Advanced Parameters" on page 132)
- Account Table (see Configuring Account Table on page 133)
- Proxy & Registration (see "Configuring Proxy and Registration Parameters" on page 136)

3.3.2.9.1 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 653.

➤ **To configure general SIP parameters:**

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

Figure 3-66: SIP General Parameters Page

SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Disable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	No Fax
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	UDP
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5060
Use user=phone in SIP URL	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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.9.2 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 653.

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

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

Figure 3-67: SIP General Parameters Page

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
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
Debug Level	0
Misc. Parameters	
Progress Indicator to IP	Not Configured
Enable X-Channel Header	Disable
Enable Busy Out	Disable
Graceful Busy Out Timeout [sec]	0
Default Release Cause	3
Max Number of Active Calls	400
Max Call Duration [min]	0
Enable LAN Watchdog	Disable
Enable Calls Cut Through	Disable
Enable User-Information Usage	Disable
Out-Of-Service Behavior	! Reorder Tone
Delay After Reset [sec]	7
T38 Fax Max Buffer	1024
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
IP2IP Registration Time	20
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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.9.3 Configuring Account Table

The 'Account Table' page allows you to define up to 32 *Accounts* per Hunt Group (*Served Hunt Group*) or source IP Group (*Served IP Group*) for registration and/or digest authentication (user name and password) to a destination IP address (*Serving IP Group*). The Account table can be used, for example, to register to an Internet Telephony Service Provider (ITSP) on behalf of an IP-PBX to which the device is connected. The registrations are sent to the Proxy Set ID (see "Configuring Proxy Sets Table" on page 126) associated with these Serving IP Groups.

A Hunt 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 Hunt 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 354.
- You can also configure the Account table using the *ini* file table parameter Account (see SIP Configuration Parameters).

➤ To configure Accounts:

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

Figure 3-68: Account Table Page

<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Compact"/> <input type="button" value="Delete"/> <input type="button" value="Apply"/>								
Index	Served Trunk Group	Served IP Group	Serving IP Group	Username	Password	Host Name	Register	ContactUser
1	1	3	1	itp-a	*	regiona	Yes	ITSPA-A
2	1	3	2	itp-b	*	regionb	Yes	ITSP-B

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 336.



Note: For a description of the Web interface's table command buttons (e.g., **Duplicate** and **Delete**), see "Working with Tables" on page 53.

Table 3-20: Account Table Parameters Description

Parameter	Description
Served Trunk Group [Account_ServedTrunkGroup]	<p>The Hunt Group ID for which you want to register and/or authenticate to a destination IP Group (i.e., Serving IP Group). For Tel-to-IP calls, the Served Hunt Group is the source Hunt Group from where the call originated. For IP-to-Tel calls, the Served Hunt Group is the 'Trunk Group ID' defined in the 'Inbound IP Routing Table' (see "Configuring the Inbound IP Routing Table" on page 172). For defining Hunt Groups, see Configuring the Hunt Group Table on page 146.</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 119) 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 126) 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 'Hunt Group Settings' table (see "Configuring Hunt Group Settings" on page 148). ▪ The parameter 'Register' in this table is set to 1. <p>In addition, for a SIP call that is identified by both the Served Hunt 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 'Hunt Group Settings' table or 'Outbound IP Routing Table' (see "Configuring the Outbound IP Routing Table" on page 165). 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 172).</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 183) or the global parameters (UserName and Password) defined on the 'Proxy & Registration' page.</p>

Parameter	Description
Username [Account_Username]	Digest MD5 Authentication user name (up to 50 characters).
Password [Account_Password]	Digest MD5 Authentication password (up to 50 characters). Note: After you click the Apply button, this password is displayed as an asterisk (*).
Host Name [Account_HostName]	Defines the Address of Record (AOR) host name. It appears in REGISTER From/To headers as ContactUser@HostName. For successful registrations, this HostName is also included in the INVITE request's From header URI. If not configured or if registration fails, the 'SIP Group Name' parameter from the 'IP Group' table is used instead. This parameter can be up to 49 characters.
Register [Account_Register]	<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 'Hunt Group Settings' table for the specific Hunt Group. The Host Name (i.e., host name in SIP From/To headers) and Contact User (user in From/To and Contact headers) are taken from this table upon a successful registration. See the example below:</p> <pre>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 Hunt 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 Hunt Group, and if this Hunt Group includes all the channels in the Hunt Group, the Hunt Group is set to Out-Of-Service if the parameter OOSOnRegistrationFail is set to 1 (see "Proxy & Registration Parameters" on page 136).

Parameter	Description
Contact User [Account_ContactUser]	<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 from 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>
Application Type [Account_ApplicationType]	<p>Defines the application type:</p> <ul style="list-style-type: none"> ▪ [0] GW/IP2IP = Gateway and IP-to-IP application (default) (The IP-to-IP application will be supported in the next applicable release.) ▪ [2] SBC = SBC application

3.3.2.9.4 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 [653](#).



Note: To view whether the device or its endpoints have registered to a SIP Registrar/Proxy server, see "Viewing Registration Status" on page [354](#).

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


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

Figure 3-69: Proxy & Registration Page

Use Default Proxy	Yes
Proxy Set Table	
Proxy Name	<input type="text"/>
Redundancy Mode	Homing
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Disable
Redundant Routing Mode	Disable
SIP ReRouting Mode	Standard Mode
Enable Registration	Disable
Registration Time	180
Re-registration Timing [%]	50
Registration Retry Time	30
Registration Time Threshold	0
Re-register On INVITE Failure	Disable
ReRegister On Connection Failure	Disable
Gateway Name	ipcs20.callbox.kt.com
Gateway Registration Name	<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	<input type="text"/>
Password	Default_Passwd
Cnonce	Default_Cnonce
Registration Mode	Per FXS
Set Out-Of-Service On Registration Failure	Disable
Challenge Caching Mode	None
Mutual Authentication Mode	Optional

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.

4. Click the **Register** or **Un-Register** buttons to save your changes and register/unregister to a Proxy/Registrar.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

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 126 for a description of this page).

3.3.2.10 Coders and Profiles

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

- Coders (see "Configuring Coders" on page 139)
- Coders Group Settings (see "Configuring Coder Groups" on page 140)
- Tel Profile Settings (see Configuring Tel Profiles on page 141)
- IP Profile Settings (see Configuring IP Profiles on page 143)

Implementing the device's Profile features provides the device with high-level adaptation when connected to a variety of equipment (at both Tel and IP sides) and protocols, each of which requires different system behavior. Each Profile contains a set of parameters such as coders, T.38 Relay, Voice and DTMF Gain, Silence Suppression, Echo Canceler, RTP DiffServ, Current Disconnect and more. The Profiles feature allows you to customize these parameters or turn them on or off, per source or destination routing and/or per the device's trunks (channels). For example, specific E1/T1 spans can be assigned a Profile that always uses G.711.

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

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

- 'Outbound IP Routing Table' page (see Configuring the Outbound IP Routing Table on page 165)
- 'Inbound IP Routing Table' page (see Configuring the Inbound IP Routing Table on page 172)

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



Notes:

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

3.3.2.10.1 Configuring Coders

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



Notes:

- For a list of supported coders and for configuring coders using the *ini* file, refer to the *ini* file parameter table CodersGroup, described in SIP Configuration Parameters.
- A coder (i.e., 'Coder Name') can appear only once in the table.
- If packetization time and/or rate are not specified, the default value is applied.
- Only the packetization time of the first coder in the coder list is declared in INVITE/200 OK SDP, even if multiple coders are defined.
- The device always uses the packetization time requested by the remote side for sending RTP packets.
- For G.729, it's also possible to select silence suppression without adaptations.
- If the coder G.729 is selected with silence suppression is disabled, the device includes 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is enabled or set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception to this logic is when the remote gateway is a Cisco device (IsCiscoSCMode).
- For defining groups of coders (which can be assigned to Tel and IP Profiles), see "Configuring Coder Groups" on page 140.
- For an explanation on V.152 support (and implementation of T.38 and VBD coders), see "Supporting V.152 Implementation" on page 452.

➤ To configure the device's coders:

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

Figure 3-70: Coders Page

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

2. From the 'Coder Name' drop-down list, select the required coder.

3. From the 'Packetization Time' drop-down list, select the packetization time (in msec) for the selected coder. The packetization time determines how many coder payloads are combined into a single RTP packet.
4. From the 'Rate' drop-down list, select the bit rate (in kbps) for the selected coder.
5. In the 'Payload Type' field, if the payload type (i.e., format of the RTP payload) for the selected coder is dynamic, enter a value from 0 to 120 (payload types of 'well-known' coders cannot be modified).
6. From the 'Silence Suppression' drop-down list, enable or disable the silence suppression option for the selected coder.
7. Repeat steps 2 through 6 for the next optional coders.
8. Click the **Submit** button to save your changes.
9. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.10.2 Configuring Coder Groups

The 'Coder Group Settings' page allows you to define up to four different Coder Groups. These Coder Groups can be assigned to Tel Profiles (see Configuring Tel Profiles on page 141) and/or IP Profiles (see Configuring IP Profiles on page 143). For each Coder Group, you can define up to ten coders, where the first coder in the table takes precedence over the second coder, and so on. The first coder is the highest priority coder and is used by the device whenever possible. If the far end device cannot use the first coder, the device attempts to use the next coder, and so on.



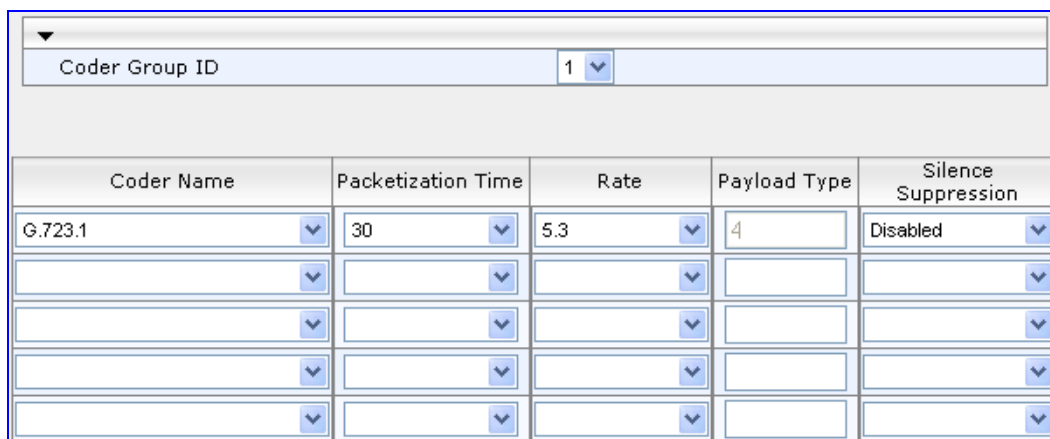
Notes:

- A coder type can appear only once per Coder Group.
- For a list of supported coders and for configuring coders using the *ini* file, refer to the *ini* file parameter table CodersGroup, described in SIP Configuration Parameters.
- For information on coders, refer to the notes in "Configuring Coders" on page 139.

➤ To configure Coder Groups:

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

Figure 3-71: Coder Group Settings Page



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

2. From the 'Coder Group ID' drop-down list, select a Coder Group ID.
3. From the 'Coder Name' drop-down list, select the first coder for the Coder Group.
4. From the 'Packetization Time' drop-down list, select the packetization time (in msec) for the coder. The packetization time determines how many coder payloads are combined into a single RTP packet.
5. From the 'Rate' drop-down list, select the bit rate (in kbps) for the coder you selected.
6. In the 'Payload Type' field, if the payload type (i.e., format of the RTP payload) for the coder you selected is dynamic, enter a value from 0 to 120 (payload types of 'well-known' coders cannot be modified).
7. From the 'Silence Suppression' drop-down list, enable or disable the silence suppression option for the coder you selected.
8. Repeat steps 3 through 7 for the next coders (optional).
9. Repeat steps 2 through 8 for the next coder group (optional).
10. Click the **Submit** button to save your changes.
11. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.10.3 Configuring Tel Profile

The 'Tel Profile Settings' page allows you to define up to nine Tel Profiles. You can assign these Tel Profiles to the device's channels in the Hunt Group Table (see Configuring the Hunt Group Table on page 146)), and thereby, apply different behaviors to different channels.



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

➤ **To configure Tel Profiles:**

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

Figure 3-72: Tel Profile Settings Page

▼	
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 identification number you want to configure.
3. In the 'Profile Name' field, enter an arbitrary name that enables you to easily identify the Tel Profile.

4. From the 'Profile Preference' drop-down list, select the priority of the Tel Profile, where '1' is the lowest priority and '20' is the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk in the description of the parameter TelProfile) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
Note: If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the preference.
5. Configure the Profile's parameters according to your requirements. For detailed information on each parameter, refer to the description of the "global" parameter.
6. From the 'Coder Group' drop-down list, select the Coder Group (see "Configuring Coder Groups" on page 140) or the device's default coder (see "Configuring Coders" on page 139) to which you want to assign the Profile.
7. Repeat steps 2 through 6 to configure additional Tel Profiles (optional).
8. Click the **Submit** button to save your changes.
9. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.10.4 Configuring IP Profiles

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

- Outbound IP Routing Table (see "Configuring Outbound IP Routing Table" on page 165)
- Inbound IP Routing Table (see "Configuring Inbound IP Routing Table" on page 172)
- IP Group (see "Configuring IP Groups" on page 119)

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

- Common Parameters: parameters common to all application types
- Gateway Parameters: parameters applicable to gateway functionality
- SBC Parameters: parameters that are applicable only to the SBC application



Notes:

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

➤ **To configure IP Profiles:**

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

Figure 3-73: IP Profile Settings Page

▼	
Profile ID	1 ▼
Profile Name	
▼ Common Parameters	
RTP IP DiffServ	46
Signaling DiffServ	40
Disconnect on Broken Connection	Yes ▼
Media IP Version Preference	Only IPv4 ▼
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	Fax Fallback ▼
Play Ringback Tone to IP	Don't Play ▼
Enable Early Media	Enable ▼
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 ▼
Enable Hold	Enable ▼
▼ SBC	
Transcoding Mode	Only if Required ▼
Extension Coders Group ID	None ▼
Allowed Coders Group ID	None ▼
Allowed Coders Mode	Restriction ▼
Diversion Mode	Not Configured ▼
History Info Mode	Not Configured ▼

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

4. From the 'Profile Preference' drop-down list, select the priority of the IP Profile, where '1' is the lowest priority and '20' is the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
Note: If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the preference.
5. Configure the IP Profile's parameters according to your requirements.
6. From the 'Coder Group' drop-down list, select the coder group that you want to assign to the IP Profile. You can select the device's default coders (see "Configuring Coders" on page 139), or one of the coder groups you defined in the 'Coder Group Settings' page (see "Configuring Coder Groups" on page 140).
7. Repeat steps 2 through 6 for the next IP Profiles (optional).
8. Click the **Submit** button to save your changes.
9. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11 GW and IP to IP

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

- Trunk Group (see Hunt Group on page 145)
- Manipulations (see Manipulation on page 151)
- Routing (see Routing on page 164)
- DTMF and Supplementary (see "DTMF and Supplementary" on page 177)
- Analog Gateway (see Analog Gateway on page 179)
- Digital Gateway (see Digital Gateway on page 190)
- Advanced Applications (see Advanced Applications on page 193)



Note: The IP-to-IP application will be supported in the next applicable release.

3.3.2.11.1 Hunt Group

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

- Hunt Group Table (see Configuring Hunt Group Table on page 146)
- Hunt Group Settings (see "Configuring Hunt Group Settings" on page 148)

3.3.2.11.1.1 Configuring Hunt Group Table

The 'Hunt Group Table' page allows you to define up to 120 Hunt Groups. This table enables the device's channels by assigning them telephone numbers, Hunt Group IDs and Tel Profiles. Channels that are not defined in this table are disabled. Hunt Groups are used for routing calls (Tel-to-IP and IP-to-Tel) on the channels associated with the Hunt Group.



Note: You can also configure Hunt Groups using the *ini* file table parameter `TrunkGroup_x` to (see "Number Manipulation and Routing Parameters" on page 836).

➤ **To configure the Hunt Group Table:**

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

Figure 3-74: Hunt Group Table Page

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 Hunt Group according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to the flash memory, see "Saving Configuration" on page 336.

Table 3-21: Hunt Group Table Parameters

Parameter	Description
Module [TrunkGroup_Module]	The module (i.e., FXS, FXO, PRI, or BRI) for which you want to define the Hunt Group.
From Trunk [TrunkGroup_FirstTrunkId]	Starting physical Trunk number in the Hunt 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 Hunt 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],	The device's channels/ports (analog module) or Trunk B-channels (digital module). To enable channels, enter the

Parameter	Description
[TrunkGroup_LastBChannel]	<p>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.</p> <p>Notes:</p> <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]	<p>The telephone number that is assigned to the channel.</p> <p>This value can include up to 50 characters.</p> <p>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.</p> <p>These numbers are also used for channel allocation for IP-to-Tel calls if the Hunt Group's 'Channel Select Mode' is set to 'By Dest Phone Number'.</p> <p>Notes:</p> <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]	<p>The Hunt Group ID (0-119) assigned to the corresponding channels. The same Hunt Group ID can be assigned to more than one group of channels. The Hunt Group ID is used to define a group of common channel behavior that are used for routing IP-to-Tel calls. If an IP-to-Tel call is assigned to a Hunt Group, the IP call is routed to the channel(s) pertaining to that Hunt Group ID.</p> <p>Notes:</p> <ul style="list-style-type: none"> Once you have defined a Hunt Group, you must configure the parameter PSTNPrefix (Inbound IP Routing Table) to assign incoming IP calls to the appropriate Hunt Group. If you do not configure this, calls cannot be established. You can define the method for which calls are assigned to channels within Hunt Groups, using the parameter TrunkGroupSettings.
Tel Profile ID [TrunkGroup_ProfileId]	<p>The Tel Profile ID assigned to the channels pertaining to the Hunt Group.</p> <p>Note: For configuring Tel Profiles, refer to the parameter TelProfile.</p>

3.3.2.11.1.2 Configuring Hunt Group Settings

The 'Hunt Group Settings' page allows you to configure the settings of up to 24 Hunt Groups. These Hunt Groups are configured in the 'Hunt Group Table' page (see Configuring Hunt Group Table on page 146).

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

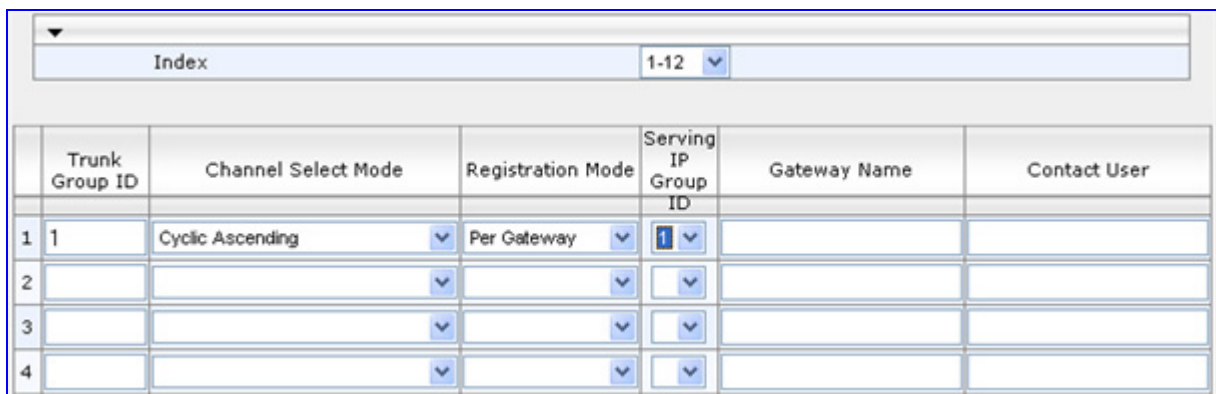


Note: You can also configure the 'Hunt Group Settings' table using the *ini* file table parameter TrunkGroupSettings (see "Number Manipulation and Routing Parameters" on page 836).

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

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

Figure 3-75: Hunt Group Settings Page



	Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	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 Hunt Group according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

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 119).

```
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 3-22: Hunt Group Settings Parameters

Parameter	Description
Trunk Group ID [TrunkGroupSettings_TrunkGroupId]	The Hunt 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 Hunt 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) <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 Hunt 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 Hunt Group registers individually. The registrations are sent to the ServingIPGroupID if defined in the table, otherwise to the default Proxy, and if no default Proxy, then to the Registrar IP. ▪ [4] Don't Register = No registrations are sent by endpoints pertaining to the Hunt Group. For example, if the device is configured globally to register all its endpoints (using the parameter ChannelSelectMode), you can exclude some endpoints from being registered by assigning them to a Hunt Group and configuring the Hunt Group registration mode to 'Don't Register'. ▪ [5] Per Account = Registrations are sent (or not) to an IP Group, according to the settings in the Account table (see "Configuring Account Table" on page 133).

Parameter	Description
	<p>Notes:</p> <ul style="list-style-type: none"> To enable Hunt Group registrations, configure the global parameter <code>IsRegisterNeeded</code> to 1. This is unnecessary for 'Per Account' registration mode. If no mode is selected, the registration is performed according to the global registration parameter <code>ChannelSelectMode</code>. If the device is configured globally (<code>ChannelSelectMode</code>) 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.
Serving IP Group ID [<code>TrunkGroupSettings_ServingIPGroup</code>]	<p>The Serving IP Group ID to where INVITE messages initiated by this Hunt Group's endpoints are sent. The actual destination to where these INVITE messages are sent is according to the Proxy Set ID (see "Configuring Proxy Sets Table" on page 126) 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 119). 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 165).</p> <p>Note: If the parameter <code>PreferRouteTable</code> is set to 1 (see "Configuring Proxy and Registration Parameters" on page 136), the routing rules in the 'Outbound IP Routing Table' prevail over the selected Serving IP Group ID.</p>
Gateway Name [<code>TrunkGroupSettings_GatewayName</code>]	<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 <code>SIPGatewayName</code> is used instead.</p>
Contact User [<code>TrunkGroupSettings_ContactUser</code>]	<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.

3.3.2.11.2 Manipulation

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

- General Settings (see "Configuring General Settings" on page 151)
- Manipulation tables (see "Configuring Number Manipulation Tables" on page 152):
 - Dest Number IP->Tel
 - Dest Number Tel->IP
 - Source Number IP->Tel
 - Source Number Tel->IP
- Redirect Number IP->Tel (see Configuring Redirect Number IP to Tel on page 156)
- Redirect Number Tel->IP (see "Configuring Redirect Number Tel to IP" on page 158)
- Phone Context (see "Mapping NPI/TON to SIP Phone-Context" on page 160)
- Release Cause Mapping (see Configuring Release Cause Mapping on page 162)

3.3.2.11.2.1 Configuring General Settings

The 'General Settings' page allows you to configure general manipulation parameters. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 653.

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

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

Figure 3-76: 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.2.2 Configuring Number Manipulation Tables

The device provides number manipulation tables for incoming (IP-to-Tel) and outgoing (Tel-to-IP) calls. These tables are used to modify the destination and/or source telephone numbers so that the calls can be routed correctly. For example, telephone number manipulation can be implemented by the following:

- Stripping or adding dialing plan digits from or to the number, respectively. For example, a user may need to first dial 9 before dialing the phone number to indicate an external line. This number 9 can then be removed by number manipulation before the call is setup.
- Allowing or blocking Caller ID information according to destination or source prefixes. For detailed information on Caller ID, see [Configuring Caller Display Information](#) on page 185.
- 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.

Number manipulation is configured in the following tables:

- **Tel-to-IP calls:**
 - Destination Phone Number Manipulation Table for Tel-to-IP Calls (NumberMapTel2IP *ini* file parameter) - up to 120 entries
 - Source Phone Number Manipulation Table for Tel-to-IP Calls (SourceNumberMapTel2IP *ini* file parameter) - up to 120 entries
- **IP-to-Tel calls:**
 - Destination Phone Number Manipulation Table for IP-to-Tel Calls (NumberMapIP2Tel *ini* file parameter) - up to 100 entries
 - Source Phone Number Manipulation Table for IP-to-Tel Calls (SourceNumberMapIP2Tel *ini* file parameter) - up to 120 entries

The device searches a matching manipulation rule starting from the first entry (i.e., top of the table). In other words, a rule at the top of the table takes precedence over a rule defined lower down in the table. Therefore, define more specific rules above more generic rules. For example, if you enter 551 in Index 1 and 55 in Index 2, the device applies rule 1 to numbers that start with 551 and applies rule 2 to numbers that start with 550, 552, 553, and so on until 559. However, if you enter 55 in Index 1 and 551 in Index 2, the device applies rule 1 to all numbers that start with 55, including numbers that start with 551.

You can perform a second "round" (additional) of destination (NumberMapIP2Tel parameter) and source (SourceNumberMapIP2Tel parameter) number manipulations for IP-to-Tel calls on an already manipulated number. The initial and additional number manipulation rules are both configured in these tables. The additional manipulation is performed on the initially manipulated number. Therefore, for complex number manipulation schemes, you only need to configure relatively few manipulation rules in these tables (that would otherwise require many rules). This feature is enabled using the following parameters:

- PerformAdditionalIP2TELSrcManipulation for source number manipulation
- PerformAdditionalIP2TELDestinationManipulation for destination number manipulation

**Notes:**

- Number manipulation can occur before or after a routing decision is made. For example, you can route a call to a specific Hunt Group according to its original number, and then you can remove or add a prefix to that number before it is routed. To determine when number manipulation is performed, configure the 'IP to Tel Routing Mode' parameter (RouteModelIP2Tel) described in "Configuring Inbound IP Routing Table" on page 172, and 'Tel to IP Routing Mode' parameter (RouteModeTel2IP) described in "Configuring Outbound IP Routing Table" on page 165.
- Manipulation rules are done in the following order: 1) Stripped digits from left, 2) Stripped digits from right, 3) Number of digits to leave, 4) Prefix to add, and then 5) Suffix to add.
- The manipulation rules can be applied to any incoming call whose source IP address, source Hunt Group, source IP Group, destination number prefix, and/or source number prefix match the values defined in the 'Source IP Address', 'Source Trunk Group', 'Source IP Group', 'Destination Prefix', and 'Source Prefix' fields respectively. The number manipulation can be performed using a combination of each of the above criteria or using each criterion independently.
- For available notations representing multiple numbers/digits for destination and source prefixes, see "Dialing Plan Notation for Routing and Manipulation" on page 413.
- For configuring number manipulation using *ini* file table parameters NumberMapIP2Tel, NumberMapTel2IP, SourceNumberMapIP2Tel, and SourceNumberMapTel2IP, see "Number Manipulation and Routing Parameters" on page 836.

➤ **To configure number manipulation rules:**

1. Open the required 'Number Manipulation' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** submenu > **Dest Number IP->Tel**, **Dest Number Tel->IP**, **Source Number IP->Tel**, or **Source Number Tel->IP**); the relevant Manipulation table page is displayed (e.g., 'Source Phone Number Manipulation Table for Tel->IP Calls' page).

Figure 3-77: 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 the **Submit** button to save your changes.
 4. To save the changes to flash memory, see "Saving Configuration" on page 336.

Table 3-23: Number Manipulation Parameters Description

Parameter	Description
Source Trunk Group	<p>The source Hunt Group ID for Tel-to-IP calls. To denote all Hunt Groups, leave this 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. ▪ For IP-to-IP call routing, this parameter is not required (i.e., leave the field empty).
Source IP Group	<p>The IP Group from where the IP-to-IP call originated. Typically, this 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 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. An asterisk (*) represents any number.
Web/EMS: Source Prefix	Source (calling) telephone number prefix. An asterisk (*) represents any number.

Parameter	Description
Web/EMS: Source IP Address	<p>Source IP address of the caller (obtained from the Contact header in the INVITE message).</p> <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.
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>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only to Number Manipulation tables for IP-to-Tel calls. For a detailed list of the available NPI/TON values, see Numbering Plans and Type of Number on page 162

Parameter	Description
Web: TON EMS: Number Type	<p>The Type of Number (TON) assigned to this entry.</p> <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]. <p>Notes:</p> <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	<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 185). [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"> 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.

3.3.2.11.2.3 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 and Routing Parameters" on page 836).
- 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 3-78: 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

Table 3-24: 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.
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 185). [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	Description
	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 a detailed list of the available NPI/TON values, see "Numbering Plans and Type of Number" on page 162</p>

3.3.2.11.2.4 Configuring Redirect Number Tel to IP

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



Notes:

- Redirect Tel-to-IP manipulation is not done if the device copies the received destination number to the outgoing SIP redirect number, as enabled by the CopyDest2RedirectNumber parameter.
- You can also configure the Redirect Number Tel to IP table using the *ini* file parameter RedirectNumberMapTel2Ip (see "Number Manipulation and Routing Parameters" on page 836).
- If the characteristics Destination Prefix, Redirect Prefix, and/or Source Address match the incoming SIP message, manipulation is performed according to the configured manipulation rule.
- The manipulation rules are executed in the following order: Stripped Digits From Left, Stripped Digits From Right, Number of Digits to Leave, Prefix to Add, and then Suffix to Add.
- The Destination Number and Redirect Prefix parameters are used before any manipulation has been done on them.

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

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

Figure 3-79: 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

Table 3-25: Redirect Number Tel to IP Parameters Description

Parameter	Description
Source Trunk Group	The Hunt Group from where the Tel call is received. To denote any Hunt Group, leave this field empty. 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 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. (The IP-to-IP application will be supported in the next applicable release.)
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.

Parameter	Description
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	<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 185). [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>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.</p>

3.3.2.11.2.5 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 3-80: Phone Context Table Page

Add Phone Context As Prefix			Enable
Phone Context Index			1-10
	NPI	TON	Phone Context
1	Unknown	Unknown	unknown.com
2	Private	Level 2 Regional	host.com
3	E.164 Public	National	na.e164.host.com
4			

2. Configure the Phone Context table according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

**Notes:**

- Several rows with the same NPI-TON or Phone-Context are allowed. In such a scenario, a Tel-to-IP call uses the first match.
- You can also configure the Phone Context table using the *ini* file table parameter PhoneContext (see "Number Manipulation and Routing Parameters" on page 836).

Table 3-26: Phone-Context Parameters Description

Parameter	Description
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 (digital interfaces) with Called and Calling numbers.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
NPI	<p>Select the Number Plan assigned to this entry.</p> <ul style="list-style-type: none"> ▪ [0] Unknown (default) ▪ [1] E.164 Public ▪ [9] Private <p>For a detailed list of the available NPI/TON values, see Numbering Plans and Type of Number on page 162.</p>
TON	<p>Select the Type of Number assigned to this entry.</p> <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 ✓ [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.

3.3.2.11.2.6 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 ISDN ETSI NPI/TON values is shown in the following table:

Table 3-27: NPI/TON Values for ISDN ETSI

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.
	Subscriber [4]	A public number in complete E.164 format representing a local subscriber, e.g., 5551234.
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

3.3.2.11.2.7 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 638).



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 799).

➤ **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 3-81: 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 the **Submit** button to save your changes.
5. To save the changes so they are available after a power fail, see "Saving Configuration" on page [336](#).

3.3.2.11.3 Routing

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

- General Parameters (see "Configuring General Routing Parameters" on page 164)
- Tel to IP Routing (see "Configuring Outbound IP Routing Table" on page 165)
- IP to Trunk Group Routing (see "Configuring Inbound IP Routing Table" on page 172)
- Alternative Routing Reasons (see "Configuring Alternative Routing Reasons" on page 174)
- Forward on Busy Trunk (see "Configuring Call Forward upon Busy Trunk" on page 176)

3.3.2.11.3.1 Configuring General Routing Parameters

The 'Routing General Parameters' page allows you to configure general routing parameters. For a description of these parameters, see "Configuration Parameters Reference" on page 653.

➤ To configure general routing parameters:

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

Figure 3-82: Routing General Parameters Page

General Parameters	
Add Hunt Group ID as Prefix	No
Add Trunk ID as Prefix	No
Replace Empty Destination with B-channel Phone Number	No
Add NPI and TON to Called Number	No
Add NPI and TON to Calling Number	No
IP to Tel Remove Routing Table Prefix	No
Source IP Address Input	SIP Contact Header
Enable Alt Routing Tel to IP	Disable
Alt Routing Tel to IP Mode	Both
Alt Routing Tel to IP Connectivity Method	ICMP Ping
Alt Routing Tel to IP Keep Alive Time	60
Alternative Routing Tone Duration [ms]	0
Source Manipulation Mode	FROM & PAI (after manipulation)
Max Allowed Packet Loss for Alt Routing [%]	20
Max Allowed Delay for Alt Routing [msec]	250

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.3.2 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 IP destinations.

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

- **Matching Characteristics:** User-defined characteristics of the incoming call. If the call characteristics match a table entry, the routing rule is used to route the call to the specified destination. One or more characteristics can be defined for the rule such as source IP Group (to which the call belongs), Hunt Group (from where the call is received), source (calling)/destination (called) telephone number prefix, source/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 605
 - 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 119)

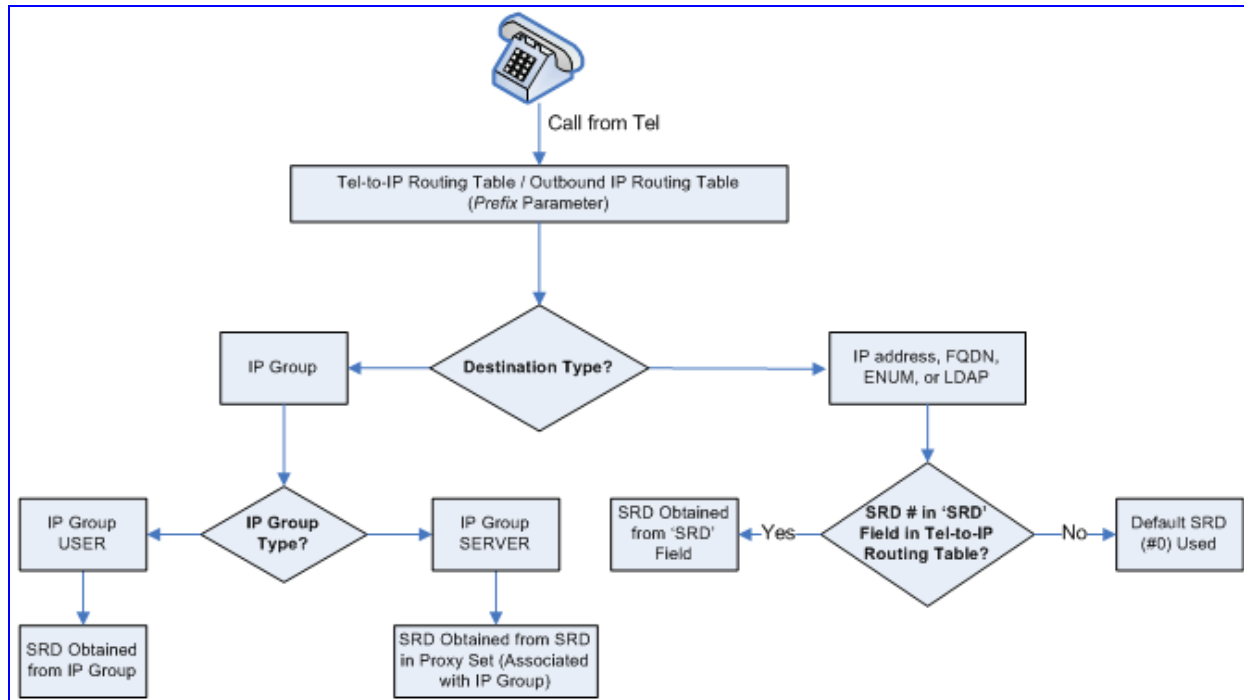
If the device is configured with multiple SRDs, you can also indicate (in the table's 'Dest. SRD' field) the destination SRD for routing to one of the following destination types - IP address, FQDN, ENUM, or LDAP. If the SRD is not selected, then the default SRD-0 is used. In scenarios where routing 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 when 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 3-83: Locating SRD



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

- Fallback routing if communication is lost with the proxy server.
- IP Security feature (enabled using the SecureCallFromIP parameter): the device routes only received calls whose source IP address is defined in this table.
- Filter Calls to IP feature: the device checks this table before a call is routed to the proxy server. However, if the number is not allowed, i.e., the number does not exist in the table or a Call Restriction (see below) routing rule is applied, the call is released.
- Obtain different SIP URI host names (per called number).
- Assign IP Profiles to calls.



Note: For this table to take precedence over a proxy for routing calls, you need to set the parameter PreferRouteTable to 1. The device checks the 'Destination IP Address' field in this table for a match with the outgoing call; a proxy is used only if a match is not found.

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

- **Call Restriction:** Rejects calls whose routing rule is associated with the destination IP address 0.0.0.0.
- **Always Use Routing Table feature:** Even if a proxy server is used, the SIP Request-URI host name in the sent INVITE message is obtained from this table. Using this feature, you can assign a different SIP URI host name for different called and/or calling numbers. This feature is enabled using the AlwaysUseRouteTable parameter.

- **Assign IP Profiles:** IP Profiles can be assigned to destination addresses (also when a proxy is used).
- **Alternative Routing (when a proxy isn't used):** An alternative IP destination can be configured for specific 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 detailed information on Alternative Routing, see "Configuring Alternative Routing (Based on Connectivity and QoS)" on page 442).
 - A defined Release Reason code (see "Configuring Alternative Routing Reasons" on page 174) is received.

Alternative routing is typically implemented when there is no response to an INVITE message (after INVITE re-transmissions). The device then issues an internal 408 'No Response' implicit Release Reason. If this reason is defined (see "Configuring Alternative Routing Reasons" on page 174), the device immediately initiates a call to the alternative destination using the next matching entry in this routing table. Note that if a domain name in this table is resolved into two IP addresses, the timeout for INVITE re-transmissions can be reduced by using the HotSwapRtx parameter.

**Notes:**

- If the alternative routing destination is the device itself, the call can be configured to be routed to the PSTN. This feature is referred to as *PSTN Fallback*. For example, if poor voice quality occurs over the IP network, the call is rerouted through the legacy telephony system (PSTN).
- Outbound IP routing can be performed before or after number manipulation. This is configured using the RouteModeTel2IP parameter, as described below.
- You can also configure this table using the *ini* file table parameter Prefix (see "Number Manipulation and Routing Parameters" on page 836).

➤ 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 3-84: Outbound IP Routing Table Page

	Src. IPGroupID	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix
1	<input type="text" value="1"/>			*	10	100
2	<input type="text" value="1"/>			*	20	*
3	<input type="text" value="1"/>			1	[5,7-9]	*
4	<input type="text" value="1"/>			*	00	*
5	<input type="text" value="1"/>					
6	<input type="text" value="2"/>	domain.com		*	*	*

↓

-	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID	Dest. SRD	IP Profile ID	Status	Charge Code
>	10.33.45.63		Not Configured	<input type="text" value="1"/>	-1	1	n/a	
			Not Configured	<input type="text" value="1"/>	-1	0	n/a	
	domain.com		Not Configured	<input type="text" value="1"/>	-1	0	n/a	
	0.0.0.0		Not Configured	<input type="text" value="1"/>	-1	0	n/a	
			Not Configured	<input type="text" value="1"/>				
	10.33.45.65		Not Configured	<input type="text" value="1"/>	-1	0	n/a	

The figure above displays the following outbound IP routing rules:

- **Rule 1:** If the called phone number prefix is 10 and the caller's phone number prefix is 100, the call is assigned settings configured for IP Profile ID 1 and then sent to IP address 10.33.45.63.
 - **Rule 2:** For all callers (*), if the called phone number prefix is 20, the call is sent to the destination according to IP Group 1 (which in turn is associated with a Proxy Set ID providing the IP address).
 - **Rule 3:** If the called phone number prefix is 5, 7, 8, or 9 and the caller belongs to Hunt Group ID 1, the call is sent to domain.com.
 - **Rule 4:** For all callers (*), if the called phone number prefix is 00, the call is rejected (discarded).
 - **Rule 5:** For all callers (*), if the called phone number prefix is 6, the call is sent to SRD 2 (i.e., Proxy Set associated with this SRD).
 - **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.
2. From the 'Routing Index' drop-down list, select the range of entries that you want to add.
 3. Configure the routing rules according to the table below.
 4. Click the **Submit** button to apply your changes.
 5. To save the changes to flash memory, see "Saving Configuration" on page 336.

Table 3-28: 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 152.
Web: Src. IPGroupID EMS: Source IP Group ID	<p>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. (The IP-to-IP application will be supported in the next applicable release.) 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>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. (The IP-to-IP application will be supported in the next applicable release.)
Web: Dest. Host Prefix EMS: Destination Host Prefix	<p>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. (The IP-to-IP application will be supported in the next applicable release.)
Web: Src. Trunk Group ID EMS: Source Trunk Group ID	<p>The Hunt Group from where call is received.</p> <p>Notes:</p> <ul style="list-style-type: none"> To denote any Hunt Group, use the asterisk (*) symbol. For IP-to-IP calls, this parameter is not required.
Web: Dest. Phone Prefix EMS: Destination Phone Prefix	<p>Prefix of the called telephone number. The prefix can include up to 50 digits.</p> <p>Note: To denote any prefix, enter an asterisk (*) symbol. The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 413.</p>

Parameter	Description
Web/EMS: Source Phone Prefix	<p>Prefix of the calling telephone number. The prefix can include up to 50 digits.</p> <p>Note: To denote any prefix, enter an asterisk (*) symbol. The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 413.</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>Destination IP address (in dotted-decimal notation or FQDN) to where the call must be sent. If an FQDN is used (e.g., domain.com), DNS resolution is done according to the DNSQueryType parameter.</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 91). ▪ 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	The destination port to where you want to route the call.
Web/EMS: Transport Type	<p>The transport layer type used 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>

Parameter	Description
Web: Dest IP Group ID EMS: Destination IP Group ID	<p>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 address. However, if both parameters are configured in this table, the INVITE message is sent only to the IP Group (and not the defined IP address). ▪ If the 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 119), 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 133). ▪ For defining Proxy Set ID's, see "Configuring Proxy Sets Table" on page 126.
Dest SRD	<p>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 114.</p>
IP Profile ID	IP Profile ID (see "Configuring IP Profiles" on page 143) assigned to this IP destination call. This allows you to assign numerous configuration attributes (e.g., voice codes) per routing rule.
Status	<p>Read-only field displaying 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>Optional Charge Code assigned to the routing rule. For configuring Charge Codes, see Configuring Charge Codes Table on page 181.</p> <p>Note: This parameter is applicable only to FXS interfaces.</p>

3.3.2.11.3.3 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 the Outbound IP Routing Table).
- For IP-to-Tel routing: routing incoming IP calls to Hunt Groups. The specific channel pertaining to the Hunt Group to which the call is routed is determined according to the Hunt Group's channel selection mode. The channel selection mode can be defined per Hunt Group (see "Configuring Hunt Group Settings" on page 148), or for all Hunt Groups using the global parameter ChannelSelectMode.

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

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



Notes:

- When a call release reason (defined in "Configuring Reasons for Alternative Routing" on page 174) is received for a specific IP-to-Tel call, an alternative Hunt Group for that call can be configured. This is done by configuring an additional routing rule for the same call characteristics, but with a different Hunt Group ID.
- The IP-to-IP application will be supported in the next applicable release.
- You can also configure the 'Inbound IP Routing Table' using the *ini* file table parameter PSTNPrefix (see "Number Manipulation and Routing Parameters" on page 836).

➤ 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 3-85: Inbound IP Routing Table

<div> <div>Routing Index</div> <div>1-12</div> <div>IP To Tel Routing Mode</div> <div>Route calls before manipulation</div> </div>								
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IPGroup ID
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 Hunt Group ID 1.
 - **Rule 2:** If the incoming IP call destination phone prefix is between 501 and 502, and source phone prefix is 101, the call is assigned settings configured for IP Profile ID 1 and routed to Hunt Group ID 2.
 - **Rule 3:** If the incoming IP call has a From URI host prefix as domain.com, the call is routed to Hunt Group ID 3.
 - **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 the **Submit** button to save your changes.
 5. To save the changes so they are available after a power failure, see "Saving Configuration" on page 336.

Table 3-29: 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 152). <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	The called telephone number prefix. The prefix can include up to 49 digits. Note: The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 413.
Source Phone Prefix	The calling telephone number prefix. The prefix can include up to 49 digits.

Parameter	Description
	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 413.
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 Hunt 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 Hunt 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	<p>The IP Profile (configured in "Configuring IP Profiles" on page 143) to assign to the call.</p>
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 133).</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 133).</p>

3.3.2.11.3.4 Configuring Alternative Routing Reasons

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

The release reasons depend on the call direction:

- **Release reason for IP-to-Tel calls:** Reason for call release on the Tel side, provided in Q.931 notation. As a result of a release reason, an alternative Hunt Group is provided. For defining an alternative Hunt Group, see "Configuring Inbound IP Routing Table" on page 172. 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 165. This call release reason type can be configured, for example, when there is no response to an INVITE message (after INVITE re-transmissions), the device issues an internal 408 'No Response' implicit release reason.

The device plays a tone to the endpoint whenever an alternative route is used. This tone is played for a user-defined time, configured by the `AltRoutingToneDuration` parameter.



Notes:

- To enable alternative routing using the IP-to-Tel routing table, set the parameter `RedundantRoutingMode` to 1 (default).
- The reasons for alternative routing for Tel-to-IP calls also apply for Proxies (if the parameter `RedundantRoutingMode` is set to 2).
- You can also configure alternative routing using the *ini* file table parameters `AltRouteCauseTel2IP` and `AltRouteCauseIP2Tel` (see "Number Manipulation and Routing Parameters" on page 836).

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

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

Figure 3-86: 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 the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.3.5 Configuring Call Forward upon Busy Trunk

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

This alternative destination is configured per Hunt Group.

The alternative destination can be defined as a host name (IP address with optional port and transport type), or as a SIP Request-URI user name and host part (i.e., user@host). For example, the below configuration forwards IP-to-Tel calls to destination user “112” at host IP address 10.13.4.12, port 5060, using transport protocol TCP, if Trunk Group ID 2 is unavailable:

```
ForwardOnBusyTrunkDest 1 = 2, 112@10.13.4.12:5060;transport=tcp;
```

When configured with user@host, the original destination number is replaced by the user part.

The device forwards calls using this table only if no alternative IP-to-Tel routing rule has been configured or alternative routing fails, and 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 Hunt Group are busy or unavailable



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

➤ To configure the Forward on Busy Trunk Destination rules:

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

Figure 3-87: Forward on Busy Trunk Destination Page

Index	Trunk Group ID	Forward Destination
0 <input type="radio"/>	<input type="text" value="1"/>	<input type="text" value="10.13.5.67"/>

The figure above displays a configuration that forwards IP-to-Tel calls destined for Hunt Group ID 1 to destination IP address 10.13.5.67 if the conditions mentioned earlier exist.

2. Configure the table as required, and then click the **Submit** button to save your changes.
3. To save the changes so they are available after a power fail, see "Saving Configuration" on page 336.

3.3.2.11.4 DTMF and Supplementary

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

- DTMF & Dialing (see "Configuring DTMF and Dialing" on page 177)
- Supplementary Services (see "Configuring Supplementary Services" on page 177)


3.3.2.11.4.1 Configuring DTMF and Dialing

The 'DTMF & Dialing' page is used to configure parameters associated with dual-tone multi-frequency (DTMF) and dialing. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 653.

➤ **To configure the DTMF and dialing parameters:**

1. Open the 'DTMF & Dialing' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **DTMF & Supplementary** submenu > **DTMF & Dialing**).

Figure 3-88: DTMF & Dialing Page

Max Digits In Phone Num	30
Inter Digit Timeout [sec]	4
Declare RFC 2833 in SDP	Yes
1st Tx DTMF Option	RFC 2833
2nd Tx DTMF Option	
RFC 2833 Payload Type	101
Hook-Flash Option	Not Supported
 Digit Mapping Rules	
Dial Plan Index	-1
Dial Tone Duration [sec]	16
Hotline Dial Tone Duration [sec]	16
Enable Special Digits	Disable
Default Destination Number	1000
Special Digit Representation	Special

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.4.2 Configuring Supplementary Services

The 'Supplementary Services' page is used to configure parameters associated with supplementary services. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 653. For an overview on supplementary services, see "Working with Supplementary Services" on page 453.

➤ To configure supplementary services parameters:

1. Open the 'Supplementary Services' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **DTMF & Supplementary** submenu > **Supplementary Services**).

Figure 3-89: Supplementary Services Page

Enable Hold	Enable
Enable Hold to ISDN	Disable
Hold Format	0.0.0.0
Held Timeout	-1
Call Hold Reminder Ring Timeout	30
Enable Transfer	Enable
Transfer Prefix	
Enable Call Forward	Enable
Enable Call Waiting	Enable
Number of Call Waiting Indications	2
Time Between Call Waiting Indications	10
Time Before Waiting Indications	0
Waiting Beep Duration	300
Enable Caller ID	Disable
Caller ID Type	Standard Bellcore
Hook-Flash Code	
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 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	

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes, or click the **Subscribe to MWI** or **Unsubscribe to MWI** buttons to save your changes and to subscribe / unsubscribe to the MWI server.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.5 Analog Gateway

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

- Keypad Features (see "Configuring Keypad Features" on page 179)
- Metering Tones (see "Configuring Metering Tones" on page 180)
- Charge Codes (see "Configuring Charge Codes" on page 181)
- FXO Settings (see "Configuring FXO Settings" on page 182)
- Authentication (see "Configuring Authentication" on page 183)
- Automatic Dialing (see "Configuring Automatic Dialing" on page 184)
- Caller Display Information (see "Configuring Caller Display Information" on page 185)
- Call Forward (see "Configuring Call Forward" on page 186)
- Caller ID Permissions (see "Configuring Caller ID Permissions" on page 188)
- Call Waiting (see "Configuring Call Waiting" on page 189)



Note: The Analog Gateway submenu appears only if the device is installed with an FXS or FXO module.

3.3.2.11.5.1 Configuring Keypad Features

The 'Keypad Features' page enables you to activate and deactivate the following features directly from the connected telephone's keypad:

- Call Forward (see "Configuring Call Forward" on page 186)
- Caller ID Restriction (see "Configuring Caller Display Information" on page 185)
- Hotline (see "Configuring Automatic Dialing" on page 184)
- Call Transfer
- Call Waiting (see "Configuring Call Waiting" on page 189)
- Rejection of Anonymous Calls



Notes:

- The 'Keypad Features' page is available only for FXS interfaces.
- The method used by the device to collect dialed numbers is identical to the method used during a regular call (i.e., max digits, interdigit timeout, digit map, etc.).
- The activation of each feature remains in effect until it is deactivated (i.e., not deactivated after a call).

➤ **To configure the keypad features**

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

Figure 3-90: 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 653.
3. Click the **Submit** button to save your changes.
4. To save the changes to the flash memory, see "Saving Configuration" on page 336.

3.3.2.11.5.2 Configuring Metering Tones

The FXS interfaces can generate 12/16 KHz metering pulses toward the Tel side (e.g., for connection to a pay phone or private meter). Tariff pulse rate is determined according to the device's Charge Codes table. This capability enables users to define different tariffs according to the source/destination numbers and the time-of-day. The tariff rate includes the time interval between the generated pulses and the number of pulses generated on answer.


**Notes:**

- The 'Metering Tones' page is available only for FXS interfaces.
- Charge Code rules can be assigned to routing rules in the 'Outbound IP Routing Table' (see "Configuring Outbound IP Routing Table" on page 165). 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 3-91: 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 653.
3. Click the **Submit** button to save your changes.
4. To save the changes to the flash memory, see "Saving Configuration" on page 336.

If you set the 'Generate Metering Tones' parameter to 'Internal Table', access the 'Charge Codes Table' page by clicking the **Charge Codes Table**  button. For a detailed description on configuring the Charge Codes table, see "Configuring Charge Codes Table" on page 181.

3.3.2.11.5.3 Configuring Charge Codes

The 'Charge Codes Table' page is used to configure the metering tones (and their time interval) that the FXS interfaces generate to the Tel side. To associate a charge code to an outgoing Tel-to-IP call, use the '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.

➤ To configure the Charge Codes:

1. Access the 'Charge Codes Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Charge Codes**). Alternatively, you can access this page from the 'Metering Tones' page (see "Configuring Metering Tones" on page 180).

Figure 3-92: 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 the **Submit** button to save your changes.
4. To save the changes to the flash memory, see "Saving Configuration" on page 336.

3.3.2.11.5.4 Configuring FXO Settings

The 'FXO Settings' page allows you to configure the device's specific FXO parameters. For a description of these parameters, see "Configuration Parameters Reference" on page 653.



Note: The 'FXO Settings' page is available only for FXO interfaces.

➤ **To configure the FXO parameters:**

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

Figure 3-93: 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.5.5 Configuring Authentication

The 'Authentication' page defines a user name and password for authenticating each device port. Authentication is typically used for FXS interfaces, but can also be used for FXO interfaces.



Notes:

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

➤ **To configure the Authentication Table:**

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

Figure 3-94: Authentication Page

Gateway Port	User Name	Password
Module 1 Port 1 FXS	<input type="text" value="user1"/>	<input type="password" value="sksksksk"/>
Module 1 Port 2 FXS	<input type="text" value="user2"/>	<input type="password" value="sksksksk"/>
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 the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.5.6 Configuring Automatic Dialing

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



Notes:

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

➤ **To configure Automatic Dialing:**

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

Figure 3-95: Automatic Dialing Page

Gateway Port	Destination Phone Number	Auto Dial Status
Module 1 Port 1 FXS	101	Enable ▼
Module 1 Port 2 FXS	911	Hotline ▼
Module 2 Port 1 FXO	302	Enable ▼
Module 2 Port 2 FXO		Enable ▼
Module 2 Port 3 FXO		Enable ▼
Module 2 Port 4 FXO		Enable ▼

2. In the 'Destination Phone Number' field corresponding to a port, enter the telephone number that you want automatically dialed.
3. From the 'Auto Dial Status' drop-down list, select one of the following:
 - **Disable [0]:** The automatic dialing feature for the specific port is disabled (i.e., the number in the 'Destination Phone Number' field is ignored).
 - **Enable [1]:** The number in the 'Destination Phone Number' field is automatically dialed if the phone is off-hooked (for FXS interfaces) or a ring signal (from PBX/PSTN switch) is detected (FXO interfaces). The FXO line is seized only after the SIP call is answered.
 - **Hotline [2]:**
 - ♦ **FXS interfaces:** When a phone is off-hooked and no digit is dialed for a user-defined time (configured using the parameter HotLineToneDuration), the number in the 'Destination Phone Number' field is automatically dialed.
 - ♦ **FXO interfaces:** If a ring signal is detected, the device seizes the FXO line, plays a dial tone, and then waits for DTMF digits. If no digits are detected for a user-defined time (configured using the parameter HotLineToneDuration), the number in the 'Destination Phone Number' field is automatically dialed by sending a SIP INVITE message with this number.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.5.7 Configuring Caller Display Information

The 'Caller Display Information' page allows you to enable the device to send Caller ID information to IP when a call is made. The called party can use this information for caller identification. The information configured on this page is sent in an INVITE message in the From header. For information on Caller ID restriction according to destination/source prefixes, see "Configuring Number Manipulation Tables" on page 152.

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

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

Figure 3-96: Caller Display Information Page

Gateway Port	Caller ID/Name	Presentation
Module 1 Port 1 FXS	Private	Restricted ▼
Module 1 Port 2 FXS	Susan C.	Restricted ▼
Module 2 Port 1 FXO	Lee P.	Allowed ▼
Module 2 Port 2 FXO	Ronaldo	Allowed ▼
Module 2 Port 3 FXO		Allowed ▼
Module 2 Port 4 FXO		Allowed ▼

2. In the 'Caller ID/Name' field corresponding to the desired port, enter the Caller ID string (up to 18 characters).
3. From the 'Presentation' drop-down list, select one of the following:
 - 'Allowed' **[0]** - sends the string defined in the 'Caller ID/Name' field when a Tel-to-IP call is made using the corresponding device port.
 - 'Restricted' **[1]** - the string defined in the 'Caller ID/Name' field is not sent.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

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 152).
- You can also configure the Caller Display Information table using the *ini* file table parameter CallerDisplayInfo.



3.3.2.11.5.8 Configuring Call Forward

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

**Notes:**

- Ensure that the Call Forward feature is enabled (default) for the settings on this page to take effect. To enable Call Forward, use the parameter EnableForward ("Configuring Supplementary Services" on page 177).
- You can also configure the Call Forward table using the *ini* file table parameter FwdInfo.

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

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

Figure 3-97: Call Forward Table Page

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

2. Configure the Call Forward parameters for each port according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

Table 3-30: 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 used, the 'forward to' phone number must be specified in the 'Outbound IP Routing Table' (see "Configuring Outbound IP Routing Table" on page 165).</p>

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

3.3.2.11.5.9 Configuring Caller ID Permissions

The 'Caller ID Permissions' page allows you to enable or disable (per port) the Caller ID generation (for FXS interfaces) and detection (for FXO interfaces). If a port isn't configured, its Caller ID generation / detection is determined according to the global parameter EnableCallerID described in "Configuring Supplementary Services" on page 177.



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

➤ To configure Caller ID Permissions per port:

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

Figure 3-98: Caller ID Permissions Page

Gateway Port	Caller ID
Module 1 Port 1 FXS	Enable ▼
Module 1 Port 2 FXS	Disable ▼
Module 2 Port 1 FXO	▼
Module 2 Port 2 FXO	▼
Module 2 Port 3 FXO	▼
Module 2 Port 4 FXO	▼

2. 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 177).
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.5.10 Configuring Call Waiting

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



Notes:

- This page is applicable only to FXS interfaces.
- Instead of using this page, you can enable or disable call waiting for all the device's ports, using the global call waiting parameter 'Enable Call Waiting' (see "Configuring Supplementary Services" on page 177).
- You can also configure the Call Waiting table using the *ini* file table parameter CallWaitingPerPort (see SIP Configuration Parameters).
- For additional call waiting configuration, see the following parameters: FirstCallWaitingToneID (in the CPT file), TimeBeforeWaitingIndication, WaitingBeepDuration, TimeBetweenWaitingIndications, and NumberOfWaitingIndications.

➤ **To configure Call Waiting:**

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

Figure 3-99: Caller Waiting Page

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 177).
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.6 Digital Gateway

The **Digital Gateway** submenu allows you to configure digital PSTN settings. This submenu includes the following page items:

- Digital Gateway Parameters (see "Configuring Digital Gateway Parameters" on page 190)
- ISDN Supp Services (see "Configuring ISDN Supplementary Services" on page 191)

3.3.2.11.6.1 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 653.

➤ 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 3-100: 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
TdmOverIP Minimum Calls For Trunk Activation	0
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
Digital Out-Of-Service Behavior	Default
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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.11.6.2 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 354.
- Caller ID name - for displaying the BRI endpoint's caller ID to a dialed destination, if enabled (i.e., "Presentation" is not restricted)
- Caller ID presentation or restriction
- Enable/disable sending caller ID to BRI endpoints



Notes:

- To use this table for routing of IP-to-Tel calls to specific BRI channels, the Channel Select Mode in the Hunt Group Settings must be set to 'Select Trunk by ISDN Supplementary Services Table' (see "Configuring Hunt Group Settings" on page 148).
- You can also configure this table using the ISDNSuppServ *ini* file table parameter (see "Configuration Parameters Reference" on page 653).
- 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 3-101: 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 the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

Table 3-31: 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

3.3.2.11.7 Advanced Applications

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

- Voice Mail Settings (see Configuring Voice Mail Parameters on page 193)

3.3.2.11.7.1 Configuring Voice Mail Parameters

The 'Voice Mail Settings' page allows you to configure the voice mail parameters. For a description of these parameters, see "Configuration Parameters Reference" on page 653.



Notes:

- The 'Voice Mail Settings' page is available only for FXO and CAS interfaces.
- For detailed information on configuring the voice mail application, refer to the *CPE Configuration Guide for Voice Mail User's Manual*.

➤ To configure the Voice Mail parameters:

1. Open the 'Voice Mail Settings' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Advanced Applications** submenu > **Voice Mail Settings**).

Figure 3-102: ISDN Supp Services Table Page

Line Transfer Mode	None
Voice Mail Interface	NONE
Digit Patterns	
Forward on Busy Digit Pattern (Internal)	
Forward on No Answer Digit Pattern (Internal)	
Forward on Do Not Disturb Digit Pattern (Internal)	
Forward on No Reason Digit Pattern (Internal)	
Forward on Busy Digit Pattern (External)	
Forward on No Answer Digit Pattern (External)	
Forward on Do Not Disturb Digit Pattern (External)	
Forward on No Reason Digit Pattern (External)	
Internal Call Digit Pattern	
External Call Digit Pattern	
Disconnect Call Digit Pattern	
Digit To Ignore Digit Pattern	
Message Waiting Indication (MWI)	
MWI Off Digit Pattern	
MWI On Digit Pattern	
MWI Suffix Pattern	
MWI Source Number	
SMDI	
Enable SMDI	Disable
SMDI Timeout [msec]	2000

2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.12 SBC

The **SBC** submenu allows you to configure the SBC application. This submenu includes the following items:

- General Settings (see "Configuring General Settings" on page 194)
- Admission Control (see "Configuring Admission Control" on page 195)
- Allowed Coders Group (see "Configuring Allowed Coder Groups" on page 197)
- Routing SBC:
 - Classification Table (see "Configuring the Classification Table" on page 198)
 - IP to IP Routing Table (see "Configuring the IP-to-IP Routing" on page 201)
 - Alternative Routing Reasons (see "Configuring Alternative Routing Reasons" on page 206)
- Manipulations SBC:
 - Message (see "Configuring Message Manipulations" on page 206)
 - IP to IP Inbound (see "Configuring IP-to-IP Inbound Manipulations" on page 210)
 - IP to IP Outbound (see "Configuring IP-to-IP Outbound Manipulations" on page 212)



Notes: The SBC submenu appears only if you have enabled the SBC application (see "Enabling Applications" on page 113) and the SBC Software Upgrade Key is installed on the device (see "Loading Software Upgrade Key" on page 339).

3.3.2.12.1 Configuring General Settings

The 'General Settings' page allows you to configure general SBC parameters. For a description of these parameters, see "SBC Parameters" on page 858.

➤ **To configure general parameters:**

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

Figure 3-103: General Settings Page

WAN IP Address	0.0.0.0
Transcoding Mode	Only If Required
SBC Registration Time	20
SBC No Answer Timeout	600
SBC GRUU Mode	AsProxy
Minimum Session-Expires	0
Allow Unclassified Calls	Allow

2. Configure the parameters as required.

3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.12.2 Configuring Admission Control

The 'Admission Control' page allows you to define up to 100 rules for limiting the number of concurrent calls (SIP dialogs). These call limits can be applied per SRD, IP Group, SIP request type (e.g., INVITEs), SIP dialog direction (e.g., inbound), and/or per user (identified by its registered contact). This is especially important for MSBG applications where VoIP and Data traffic contend on the WAN throughput, which may be limited by itself. For example, DSL WAN access interface is very limited in the uplink. Therefore, by controlling the number of calls allowed, bandwidth can be reserved for Data applications. In addition, this feature can be useful for implementing Service Level Agreements (SLA) policies.

The SIP dialog limits can be defined per SIP request type and direction. These relate to requests that initiate SIP dialogs and not the subsequent requests that can be of different type and direction. The SIP dialog-initiating request types can include SIP INVITEs, REGISTER, and/or SUBSCRIBE, or it can be configured to include the total number of all dialogs. Requests that supersede the defined limit are rejected with SIP 486 "Busy Here" responses.

This feature also provides support for SIP-dialog rate control, using the "token bucket" mechanism. The token bucket is a control mechanism that dictates the rate of SIP-dialog setups based on the presence of tokens in the bucket – a logical container that holds aggregate SIP dialogs to be accepted or transmitted. Tokens in the bucket are removed ("cached in") for the ability to setup a dialog. Therefore, a flow can setup dialogs up to its peak burst rate if there are adequate tokens in the bucket and if the burst threshold is configured appropriately.



Notes:

- The enforcement of a configured limitation for the incoming leg is performed immediately after the Classification process. If the call/request is rejected at this stage, no routing is performed. The enforcement for the outgoing leg is performed within each alternative route iteration. This is accessed from two places: one during initial classification/routing, and another during alternative routing process.
- For configuring Admission Control using the *ini* file, refer to the parameter SBCAdmissionControl.

➤ To configure Admission Control rules:

1. Open the 'Admission Control' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Admission Control**).

Figure 3-104: Admission Control Page

Index	Limit Type	IP Group ID	SRD ID	Request Type	Request Direction	Limit	Limit Per User	Rate	MaxBurst
1	IP Group	-1	-1	INVITE	Inbound	-1	50	0	0

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 336.

Table 3-32: Admission Control Parameters

Parameter	Description
Limit Type	<p>Limitation rule defined per IP group or SRD.</p> <ul style="list-style-type: none"> ▪ [0] IP Group (default) ▪ [1] SRD
IP Group ID	<p>IP Group to which you want to apply the SIP dialog limit. To apply the rule to all IP Groups, set this parameter to -1 (default).</p> <p>Note: This parameter is applicable only if Limit Type is set to IP Group.</p>
SRD ID	<p>SRD to which you want to apply the SIP dialog limit. To apply the rule to all SRD's, set this parameter to -1 (default).</p> <p>Note: This parameter is applicable only if Limit Type is set to SRD.</p>
Request Type	<p>SIP dialog-initiating request type that initiates the SIP dialog to which you want to apply the SIP dialog limit (not the subsequent requests that can be of different type and direction). The SIP dialog-initiating request types can include:</p> <ul style="list-style-type: none"> ▪ [0] All = include the total number of all dialogs (default) ▪ [1] INVITE ▪ [2] SUBSCRIBE ▪ [3] Other
Request Direction	<p>The direction of the SIP request to which the limitation is applied.</p> <ul style="list-style-type: none"> ▪ [0] Both = Applied to inbound and outbound SIP dialogs (default) ▪ [1] Inbound = Applies only to inbound SIP dialogs ▪ [2] Outbound = Applies only to outbound SIP dialogs
Limit	<p>Maximum number of concurrent SIP dialogs per IP Group or SRD. You can also use the following special values:</p> <ul style="list-style-type: none"> ▪ [0] 0 = Disallow/block all these dialogs ▪ [-1] -1 = No limit (default)
Limit Per User	<p>Maximum number of concurrent SIP dialogs per user belonging to the configured IP Group or SRD. You can also use the following special values:</p> <ul style="list-style-type: none"> ▪ [0] 0 = Disallow/block all these dialogs ▪ [-1] -1 = No limit (default)
Rate	<p>Rate at which tokens are added to the bucket per second (i.e., token rate) or unlimited if set to 0 (default). One token is added to the bucket every 1000 divided by the value of this parameter (in milliseconds).</p> <p>Note: The token bucket feature is per IP Group, SRD, SIP request type, and SIP request direction.</p>

Parameter	Description
MaxBurst	<p>The maximum number of tokens (SIP dialogs) that the bucket can hold, where 0 is unlimited (default). The device only accepts a SIP dialog if a token exists in the bucket. Once the SIP dialog is accepted, a token is removed from the bucket. If a SIP dialog is received by the device and the token bucket is empty, then the device rejects the SIP dialog. Alternatively, if the bucket is full, for example, 100 tokens, and 101 SIP dialogs arrive (before another token is added to the bucket, i.e., faster than that defined in the Rate field), then the device accepts the first 100 SIP dialogs and rejects the last one.</p> <p>Dropped requests are replied with the 486 "Busy Here" SIP response. Dropped requests are not counted in the bucket.</p> <p>Note: The token bucket feature is per IP Group, SRD, SIP request type, and SIP request direction.</p>

3.3.2.12.3 Configuring Allowed Coder Groups

The 'Allowed Coders Group' page allows you to define up to 5 Allowed Coder Groups, each with up to 10 coders. Allowed Coder Groups determine the coders that can be used for a specific SBC leg. In other words, the device's SBC application can enforce the use of specific coders while preventing the use of "restricted" coders. Coders excluded from the Allowed Coders Group are removed from the SDP offer; only common coders between SDP offered coders and coders configured in the Allowed Coder Groups are used. In addition, the order of appearance of coders in the Allowed Coder Group determines the coder priority (preference), whereby the first coder is given the highest priority. Coders preference is done on both legs on the original SDP offer without the extended coders, and the offered side selects its chosen coders from the suggested coders list.



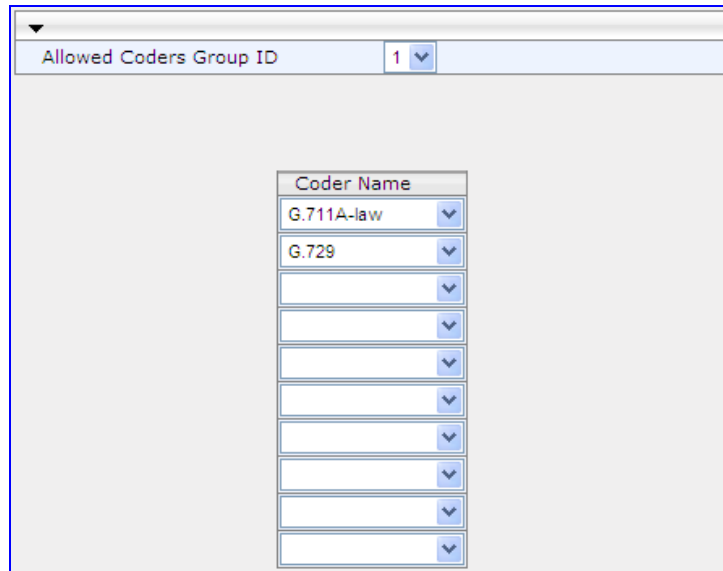
Notes:

- For a list of supported coders, refer to the *ini* file parameter table CodersGroup.
- Each coder can appear only once per Allowed Coder Group.
- If Allowed Coder Groups are configured, coders not included are blocked by the device.
- Allowed Coder Groups are applicable only to audio media.
- Allowed Coder Groups can be assigned to IP Profiles (see "Configuring IP Profiles" on page 143).
- You can also configure Allowed Coder Groups using the *ini* file parameter table AllowedCodersGroup.

➤ **To configure Allowed Coder Groups:**

1. Open the 'Allowed Coders Group' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Allowed Coders Group**).

Figure 3-105: Allowed Coders Group Page



Allowed Coders Group ID	
Allowed Coders Group ID	1

Coder Name	
G.711A-law	▼
G.729	▼
	▼
	▼
	▼
	▼
	▼
	▼
	▼
	▼

2. From the 'Allowed Coders Group ID' drop-down list, select an ID for the Allowed Coder Group.
3. In the Coder Name table, select coders for the Allowed Coder Group.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.12.4 Routing SBC

The **Routing SBC** submenu includes the following page items:

- Classification Table (see "Configuring the Classification Table" on page 198)
- IP to IP Routing Table (see "Configuring the IP-to-IP Routing" on page 201)
- Alternative Routing Reasons (see "Configuring Alternative Routing Reasons" on page 206)

3.3.2.12.4.1 Configuring Classification Table

The 'Classification Table' page allows you to configure rules for classifying incoming SIP dialog initiating requests (e.g. SIP INVITE messages). The classification identifies the incoming SIP dialog request as belonging to a specific IP Group (from where the SIP dialog request originated). The 'Classification' table is used to classify the SIP dialog request only if the other classification methods (based on Registration database and Proxy Set) have failed.

Classification begins with the device's Registration database, where it searches for a match by checking if the request arrived from a registered user in the database:

- Compares Contact header of the received SIP dialog to the Contact of the registered user

- Compares P-Asserted/From URL to the registered AOR

If the database search is unsuccessful, then the classification process proceeds with locating a Proxy Set (associated with the SIP dialog request's IP address) and then finding a match with a corresponding IP Group in the 'IP Group' table. Each IP Group can be classified according to its Proxy Set if in the 'IP Group' table the parameter `ClassifyByProxySet` is enabled (see "Configuring IP Groups" on page 119). If enabled, the device classifies requests arriving from the IP Group's Proxy Set as coming from this IP Group. The classification is done according to the Proxy IP list (in case of host names, then according to the dynamically resolved IP address list). Note that this classification is not relevant in cases where multiple IP Groups use the same Proxy Set.

If classification based on Proxy Set is unsuccessful, the device proceeds to the 'Classification' table, which searches for a source IP Group based on the following matching rules: source SRD, source IP address, source username/host prefix, and destination username/host prefix.

If the above classification process fails to determine the source IP Group to which the incoming packet belongs, the call can either be rejected, or allowed and processed (by assigning it to the default IP Group of the default SRD) if the parameter `AllowUnclassifiedCalls` is enabled.

This IP Group is afterwards used for the following purposes:

- Input for the manipulation and routing processes
- Defining SIP behavior and IP Profile, Media Realm and matching account



Notes:

- For a specific classification rule to be effective, the incoming SIP dialog message must match the characteristics configured for that rule.
- Incoming REGISTER messages are recorded in the device's database and sent to a destination only if they are associated with a source IP Group that is of USER type.
- The 'Classification' table can also be configured using the *ini* file table parameter `Classification` (see "SBC Parameters" on page 858).

➤ To configure classification rules:

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

Figure 3-106: Classification Table Page

Note: Select row index to modify the relevant row.

1

Index	Source SRD ID	Source IP Address	Source Username Prefix	Source Host Prefix	Destination Username Prefix	Destination Host Prefix	Source IP Group ID
1 <input type="radio"/>	0	10.13.2.4	*	*	*	*	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 336.

Table 3-33: Classification Table Parameters

Parameter	Description
Matching Characteristics	
Source SRD ID [Classification_SrcSRDID]	<p>The SRD ID (configured in the SRD table) from where the SIP dialog request is received. The default is -1.</p> <p>Note: The source SRD is defined according to the UDP/TCP/TLS port at which the incoming SIP dialog request is received. The 'SIP Interface' table (SIPInterface) defines the UDP/TCP/TLS ports per SRD (see "Configuring SIP Interface Table" on page 117).</p>
Source IP Address [Classification_SrcAddress]	<p>The source IP address from where the SIP dialog request is received.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ If this parameter is not configured or is configured as an "*" (asterisk), then any source IP address is accepted. ▪ The IP address can include the "x" wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. ▪ The IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255.
Source Username Prefix [Classification_SrcUsernamePrefix]	<p>The prefix of the user part of the incoming SIP dialog request's source URI (usually the From URI).</p> <p>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 413.</p>
Source Host Prefix [Classification_SrcHost]	<p>The From header URI host name prefix of the incoming SIP dialog request. If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any source host prefix.</p>
Destination Username Prefix [Classification_DestUsernamePrefix]	<p>The prefix of the incoming SIP dialog request's destination URI (usually the Request-URI) user part.</p> <p>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 413.</p>
Destination Host Prefix [Classification_DestHost]	<p>The Request-URI host name prefix of the incoming SIP dialog request. If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any destination host prefix.</p>
Operation Rule	
Source IP Group ID [Classification_SrcIPGroupID]	<p>The IP Group to which the incoming SIP dialog request is assigned. The default is -1.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This IP Group must be one of the IP Groups associated with the SRD.

Parameter	Description
	<ul style="list-style-type: none"> ▪ This IP Group is used for SBC routing and manipulations ▪ To define IP Groups, see "Configuring IP Groups" on page 119.

3.3.2.12.4.2 Configuring SBC IP-to-IP Routing

The 'IP2IP Routing Table' page configures up to 120 SBC IP-to-IP routing rules. This table provides enhanced IP-to-IP call routing capabilities for routing received SIP dialog messages (e.g., INVITE) to a destination IP address. The SIP message is routed according to a routing rule whose configured input characteristics (e.g., Source IP Group) match the incoming SIP message. If the characteristics of an incoming call does not match the first rule, the call characteristics is then compared to those of the second rule, and so on until a matching rule is located. If no rule is matched, the call is rejected.

The IP-to-IP call destination can be one of the following:

- Registered user Contact listed in the device's database (only for USER-type IP Groups).
- Proxy Set associated with the destination IP Group (allows redundancy/load balancing).
- Specific destination address (can be based on IP address, host name, port, transport type, and/or SRD). Routing to a host name can be resolved using NAPTR/SRV/A-Record.
- Incoming Request-URI.
- ENUM query.

For all destination types listed above except destination IP Group, the IP Group can optionally be itself, configured to provide the destination SRD and/or IP Profile. If neither destination SRD nor destination IP Group are defined, the destination SRD is the source SRD and the destination IP Group is its default IP Group.

In addition to the alternative routing/load balancing provided by the Proxy Set associated with the destination IP Group, the table allows the configuration of alternative routes whereby if a route fails, the next adjacent (below) rule in the table that is configured as 'Alt Route Ignore/Consider Inputs' are used. The alternative routes rules can be set to enforce the input matching criteria or to ignore any matching criteria.

Alternative routing occurs upon one of the following conditions:

- A request sent by the device is responded with the following:
 - SIP response code (i.e., 4xx, 5xx, and 6xx SIP responses) configured in the SBC Alternative Routing Reasons table (see "Configuring Alternative Routing Reasons" on page 206).
 - SIP 408 Timeout or no response (after timeout).
- The DNS resolution includes IP addresses that the device has yet to try (for the current call).

Messages are re-routed with the same SIP Call-ID and CSeq header fields (increased by 1).


Notes:

- For a specific IP-to-IP routing rule to be effective, the incoming SIP dialog message must match the characteristics configured for that rule.
- The 'IP2IP Routing' table can also be configured using the *ini* file table parameter IP2IPRouting (see "SBC Parameters" on page 858).

➤ **To configure SBC IP-to-IP routing rules:**

- Open the 'IP2IP Routing Table' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Routing SBC** submenu > **IP to IP Routing Table**).

Figure 3-107: IP2IP Routing Table Page

Index	Source IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host
1	<input type="text"/>	*	*	1	*
2	<input type="text"/>	*	*	2	*
3	<input type="text"/>	*	*	3	*

- Add an entry and then configure it according to the table below.
- Click the **Apply** button to save your changes.
- To save the changes to flash memory, see "Saving Configuration" on page 336.

Table 3-34: IP2IP Routing Table Parameters

Parameter	Description
Matching Characteristics	
Source IP Group ID [IP2IPRouting_SrcIPGroupID]	The IP Group from where the IP-to-IP call originated. Typically, the IP Group of an incoming SIP dialog is determined (or classified) using the 'Classification' table (see "Configuring Classification Table" on page 198). If not used (i.e., any IP Group), simply leave the field empty. The default is -1.
Source Username Prefix [IP2IPRouting_SrcUsernamePrefix]	The prefix of the user part of the incoming SIP dialog'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 413.
Source Host [IP2IPRouting_SrcHost]	The host part of the incoming SIP SIP dialog's source URI (usually the From URI). If this rule is not required, leave the field empty. To denote any host name, use the asterisk (*) symbol. The default is "".
Destination Username Prefix [IP2IPRouting_DestUsernamePrefix]	The prefix of the incoming SIP SIP dialog'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 "". Note: The prefix can be a single digit or a range of digits.

Parameter	Description
	For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 413.
Destination Host [IP2IPRouting_DestHost]	The host part of the incoming SIP dialog's destination URI (usually the Request-URI). If this rule is not required, leave the field empty. The asterisk (*) symbol 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 (when match occurs in characteristics)	
Destination Type [IP2IPRouting_DestType]	Determines the destination type to which the outgoing SIP dialog is sent. <ul style="list-style-type: none"> ▪ [0] IP Group (default) = The SIP dialog is sent to the IP Group's Proxy Set (SERVER-type IP Group) or registered contact from the database (if USER-type IP Group). ▪ [1] Dest Address = The SIP dialog is sent to the address configured in the following fields: 'Destination SRD ID', 'Destination Address', 'Destination Port', and 'Destination Transport Type'. ▪ [2] Request URI = The SIP dialog is sent to the address indicated in the incoming Request-URI. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence. ▪ [3] ENUM = An ENUM query is sent to include the destination address. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence.
Destination IP Group ID [IP2IPRouting_DestIPGroupID]	The IP Group ID to where you want to route the call. The SIP dialog messages are sent to the IP address defined for the Proxy Set associated with this IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Destination Address' field). However, if both parameters are configured, then the IP Group takes precedence. If the destination IP Group is of USER type, the device searches for a match between the Request-URI (of the received SIP dialog) to an AOR registration record in the device's database. The SIP dialog is then sent to the IP address of the registered contact. The default is -1.

Parameter	Description
	<p>Notes:</p> <ul style="list-style-type: none"> This parameter is only relevant if the parameter 'Destination Type' is set to 'IP Group'. However, regardless of the settings of the parameter 'Destination Type', the IP Group is still used - only for determining the IP Profile or outgoing SRD. If neither IP Group nor SRD are defined in this table, the destination SRD is determined according to the source SRD associated with the Source IP Group (configured in the 'IP Group' table, see "Configuring IP Groups" on page 119). If this table does not define an IP Group but only an SRD, then the first IP Group associated with this SRD (in the 'IP Group' table) is used. If the selected destination IP Group ID is type SERVER, the request is routed according to the IP Group addresses. If the selected destination IP Group ID is type USER, the request is routed according to the IP Group specific database (i.e., only to registered users of the selected database). If the selected destination IP Group ID is ANY USER ([-2]), the request is routed according to the general database (i.e., any matching registered user).
Destination SRD ID [IP2IPRouting_DestSRDID]	<p>The SRD ID. The default is -1.</p> <p>Note: The destination IP Group must belong to the destination SRD, if both are configured in this table.</p>
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 92).
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>

Parameter	Description
Alternative Route Options [IP2IPRouting_AltRouteOptions]	<p>Determines whether this routing rule is the main routing rule or an alternative routing rule (to the rule defined directly above it in the table).</p> <ul style="list-style-type: none"> ▪ [0] Route Row (default) = Main routing rule - the device first attempts to route the call to this route if the incoming SIP dialog's input characteristics matches this rule. ▪ [1] Alt Route Ignore Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route regardless of the incoming SIP dialog's input characteristics. ▪ [2] Alt Route Consider Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route only if the incoming SIP dialog matches this routing rule's input characteristics. <p>Notes:</p> <ul style="list-style-type: none"> ▪ The alternative routing entry ([1] or [2]) must be defined in the next consecutive table entry index to the Route Row entry (i.e., directly below it). For example, if Index 4 is configured as a Route Row, Index 5 must be configured as the alternative route. ▪ For IP-to-IP alternative routing, configure SBC alternative routing reasons upon receipt of 4xx, 5xx, and 6xx SIP responses (see "Configuring Alternative Routing Reasons" on page 206). However, if no response, ICMP, or a SIP 408 response is received, the device attempts to use the alternative route even if no entries are configured in the 'SBC Alternative Routing Reasons' table. ▪ Multiple alternative route entries can be configured (e.g., Index 1 is the main route - Route Row - and indices 2 through 4 are configured as alternative routes).

3.3.2.12.4.3 Configuring Alternative Routing Reasons

The 'SBC Alternative Routing Reasons' page allows you to define up to five different call release (termination) reasons for call releases. If a call is released as a result of one of these reasons provided in SIP 4xx, 5xx, and 6xx response codes, the device tries to find an alternative route for the call. This call release reason type can be configured, for example, when there is no response to an INVITE message (after INVITE re-transmissions), where the device issues an internal 408 'No Response' implicit release reason.

Alternative routes are configured in the IP2IP Routing table (see "Configuring SBC IP-to-IP Routing Table" on page 201).



Notes:

- Alternative routing occurs even if this table is not configured, upon scenarios where no response, ICMP, or a SIP 408 response is received.
- You can also configure alternative routing reasons using the *ini* file table parameter SBCAlternativeRoutingReasons.

➤ **To configure SIP reason codes for alternative IP routing:**

1. Open the 'SBC Alternative Routing Reasons' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Routing SBC** submenu > **Alternative Routing Reasons**).

Figure 3-108: Alternative Routing Reasons Page

SBC Alternative Routing Reasons	
Reason 1	401
Reason 2	
Reason 3	
Reason 4	
Reason 5	

2. Configure different call failure reasons that invoke alternative routing.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 336.

3.3.2.12.5 Manipulations SBC

The **Manipulations SBC** submenu includes the following page items:

- Message (see "Configuring Message Manipulations" on page 206)
- IP to IP Inbound (see "Configuring IP-to-IP Inbound Manipulations" on page 210)
- IP to IP Outbound (see "Configuring IP-to-IP Outbound Manipulations" on page 212)

3.3.2.12.5.1 Configuring Message Manipulations

The 'Message Manipulations' page allows you to define up to 200 SIP message manipulation rules. This manipulation includes insertion, removal, and/or modification of SIP headers. Multiple manipulation rules can be configured for the same SIP message.

**Notes:**

- For a detailed description on the syntax for configuring SIP message manipulation rules in the Message Manipulation table, see "SIP Message Manipulation Description" on page 506.
- SIP message manipulation is done on the inbound and outbound legs (i.e., only after classification, inbound/outbound manipulations, and routing).
- Each message can be manipulated twice, once for the source leg manipulation rules and once in the destination leg (source and destination IP Groups).
- SIP message manipulation rules configured on this page can be assigned to an IP Group and determined whether they must be applied to inbound or outbound messages (see "Configuring IP Groups" on page 119).
- 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.
- The values entered in the table are not case-sensitive.
- For configuring Message Manipulation using the *ini* file, see the parameter MessageManipulations.

➤ **To configure SIP message manipulation rules:**

1. Open the 'Message Manipulations' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Manipulations SBC** submenu > **Message**).

Figure 3-109: Message Manipulations Page

Index	Manipulation Set ID	Message Type	Condition	Action Subject
1 <input type="radio"/>	0	Invite.Response.200		Header.To.Url.User
2 <input type="radio"/>	1	Invite.Request		Header.From.Url.User
3 <input type="radio"/>	2	Invite.Response.200		Header.From.Url.User
4 <input type="radio"/>	3	Invite.Request	Header.From.Url.User=="Unko	Header.From.Url.Host.Port
5 <input type="radio"/>	4	Invite.Request		Header.Priority

↓

Action Type	Action Value	Row Role
Add Suffix	'com'	Use Current Condition
Modify	200	Use Current Condition
Modify	Header.P-Asserted-Id.Url.User	Use Current Condition
Modify	param.jpq.src.user	Use Current Condition
Remove		Use Current Condition

The previous figure shows the following message manipulation rules:

- Index 1: adds the suffix ".com" to the host part of the To header.
 - Index 2: changes the user part of the SIP From header to 200.
 - Index 3: changes the user part of the From header to the user part of the P-Asserted-ID.
 - Index 4: if the user part of the From header equals "unknown", then it is changed according to the srcIPGroup call's parameter.
 - Index 5: removes the Priority header from an incoming INVITE message.
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 336.



Note: For a detailed description on the syntax for configuring SIP message manipulation rules, see "SIP Message Manipulation Description" on page 506.

Table 3-35: Message Manipulations Parameters

Parameter	Description
Manipulation Set ID [ManSetID]	Unique manipulation set ID that you can later assign to an IP Group (see "Configuring IP Groups" on page 119). In the IP Group, this manipulation rule can be applied on the inbound and/or outbound message.
Matching Characteristics	
Message Type [MessageType]	<p>SIP message type that you want to manipulate. The valid value is a string depicting the SIP message. For example:</p> <ul style="list-style-type: none"> ▪ Empty = rule applies to all messages ▪ Invite = rule applies to all INVITE requests and responses ▪ Invite.Request = rule applies to INVITE requests ▪ Invite.Response = rule applies to INVITE responses ▪ subscribe.response.2xx = rule applies to SUBSCRIBE confirmation responses <p>Note: Currently, SIP 100 Trying messages cannot be manipulated.</p>
Condition [Condition]	<p>Condition that must exist for the rule to apply. The valid value is a string. For example:</p> <ul style="list-style-type: none"> ▪ header.from.url.user== 100 (indicates that the user part of the From header must have the value "100") ▪ header.contact.param.expires > 3600 ▪ header.to.url.host contains 'domain' ▪ param.call.dst.user != 100 <p>Note: Currently, SDP body message types are not supported.</p>

Parameter	Description
Operation	
Action Subject [ActionSubject]	SIP header upon which the manipulation is performed.
Action Type [ActionType]	<p>The type of manipulation to perform.</p> <ul style="list-style-type: none"> ▪ [0] Add (default) = adds new header/param/body (header or parameter elements). ▪ [1] Remove = removes header/param/body (header or parameter elements). ▪ [2] Modify = sets element to the new value (all element types). ▪ [3] Add Prefix = adds value at the beginning of the string (string element only). ▪ [4] Add Suffix = adds value at the end of the string (string element only). ▪ [5] Remove Suffix = removes value from the end of the string (string element only). ▪ [6] Remove Prefix = removes value from the beginning of the string (string element only).
Action Value [ActionValue]	<p>Value (string) that you want to use in the manipulation. The syntax is as follows: string/<message-element>/<call-param> "+" string/<message-element>/<call-param> For example:</p> <ul style="list-style-type: none"> ▪ 'itsp.com' ▪ header.from.url.user ▪ param.call.dst.user ▪ param.call.dst.host + '.com' ▪ param.call.src.user + "<" + header.from.url.user + '@' + header.p-asserted-id.url.host + '>' <p>Note: Only single quotation marks must be used.</p>
Row Role [RowRole]	<p>Determines which condition must be used for the rule of this table row.</p> <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 table row must be used in order to perform the defined action. This option allows you to configure multiple actions for the same condition. <p>Note: When multiple manipulations rules apply to the same header, the next rule applies to the result string of the previous rule.</p>

3.3.2.12.5.2 Configuring IP-to-IP Inbound Manipulations

The 'IP to IP Inbound Manipulation' page allows you to configure up to 100 manipulation rules for manipulating the SIP URI user part (source and destination) of inbound SIP dialog requests. You can apply these manipulations to different SIP dialog message types (e.g., INVITE or REGISTER).

- Manipulated destination URI user part are done on the following SIP headers: Request-URI, To, and Remote-Party-ID (if exists)
- Manipulated source URI user part are done on the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists)



Notes:

- For a specific manipulation rule to be effective, the incoming SIP dialog must match the configured characteristics.
- SIP URI host name (source and destination) manipulations are configured in the 'IP Group' table (see "Configuring IP Groups" on page 119). These manipulations are simply host name substitutions with the names defined for the source and destination IP Groups respectively.
- The 'IP to IP Inbound Manipulation' table can also be configured using the *ini* file table parameter IPInboundManipulation (see "SBC Parameters" on page 858).

➤ To configure IP-to-IP inbound manipulation rules:

1. Open the 'IP to IP Inbound Manipulation' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Manipulations SBC** submenu > **IP to IP Inbound**).

Figure 3-110: IP to IP Inbound Manipulation Page

Index	Is Additional Manipulation	Manipulated URI	Manipulation Purpose	Source IP Group	Source Username Prefix
1	<input type="radio"/>	Source	Normal	-1	*
		Source Host	Destination Username Prefix	Destination Host	Request Type
		*	*	*	All
		Remove From Left	Remove From Right	Leave From Right	Prefix to Add
		0	0	255	

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 336.

Table 3-36: IP to IP Inbound Manipulation Parameters

Parameter	Description
Matching Characteristics	
Is Additional Manipulation [IsAdditionalManipulation]	<p>Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it.</p> <ul style="list-style-type: none"> [0] 0 = Regular manipulation rule (not done in addition to the rule above it). [1] 1 = If the previous table row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule. <p>Note: Additional manipulation can only be performed on a different SIP URI (either source or destination) to the rule configured in the row above (defined by the parameter ManipulatedURI).</p>
Manipulated URI [ManipulatedURI]	<p>Determines whether the source or destination SIP URI user part is manipulated.</p> <ul style="list-style-type: none"> [0] Source = Manipulation is done on the source SIP URI user part. [1] Destination = Manipulation is done on the destination SIP URI user part.
Manipulation Purpose [ManipulationPurpose]	<p>Purpose of manipulation:</p> <ul style="list-style-type: none"> [0] Normal = Inbound manipulations affect the routing input and the source and/or destination number (default). [1] Routing input only = Inbound manipulations affect the routing input only, retaining the original source and destination number.
Source IP Group [SrcIpGroup]	The Source IP Group to which the incoming INVITE belongs. For any Source IP Group, enter the value -1.
Source Username Prefix [SrcUsernamePrefix]	<p>The prefix of the source SIP URI user name (usually in the From header). For any prefix, enter an asterisk (*), which is the default.</p> <p>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 413.</p>
Source Host [SrcHost]	The source SIP URI host name - full name (usually in the From header). For any host name, enter an asterisk (*), which is the default.
Destination Username Prefix [DestUsernamePrefix]	<p>The prefix of the destination SIP URI user name (usually in the Request-URI). For any prefix, enter an asterisk (*), which is the default.</p> <p>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 413.</p>
Destination Host [DestHost]	The destination SIP URI host name - full name (usually in the Request URI). For any host name, enter an asterisk (*), which is the default.
Request Type [RequestType]	<p>SIP request type to which the manipulation rule is applied.</p> <ul style="list-style-type: none"> [0] All = all SIP messages (default) [1] INVITE = all SIP messages except REGISTER and SUBSCRIBE [2] REGISTER = only SIP REGISTER messages

Parameter	Description
	<ul style="list-style-type: none"> [3] SUBSCRIBE = only SIP SUBSCRIBE messages [4] INVITE and REGISTER = all SIP messages except SUBSCRIBE [5] INVITE and SUBSCRIBE = all SIP messages except REGISTER
Operation Manipulation Rule (when match occurs in characteristics)	
Remove From Left [RemoveFromLeft]	The number of digits to remove from the left of the user name prefix. For example, if you enter 3 and the user name is "bobby", the new user name is "by".
Remove From Right [RemoveFromRight]	The number of digits to remove from the right of the user name prefix. For example, if you enter 3 and the user name is "bobby", the new user name is "bo".
Leave From Right [LeaveFromRight]	The number of characters that you want retained from the right of the user name.
Prefix to Add [Prefix2Add]	The number or string that you want added to the front of the user name. For example, if you enter 'sir' and the user name is "bobby", the new user name is "sirbobby".
Suffix to Add [Suffix2Add]	The number or string that you want added to the end of the user name. For example, if you enter '01' and the user name is "bobby", the new user name is "bobby01".

3.3.2.12.5.3 Configuring IP-to-IP Outbound Manipulations

The 'IP to IP Outbound Manipulation' page allows you to configure up to 100 manipulation rules for manipulating SIP URI user part (source and destination) of outbound SIP dialog requests. Manipulation rules in the table are located according to the source IP Group, and source and destination host and user prefixes and can be applied to a user-defined SIP request type (e.g., INVITE, OPTIONS, SUBSCRIBE, and /or REGISTER). However, since outbound manipulations are done only after routing, the outbound manipulation rule matching can also be done by destination IP Group.

Manipulated destination URI user part are performed on the following SIP headers: Request URI, To, and Remote-Party-ID (if exists). Manipulated source URI user part are performed on the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists).



Notes:

- For a specific manipulation rule to be effective, the incoming SIP dialog must match the characteristics configured for that rule.
- SIP URI host name (source and destination) manipulations are configured in the 'IP Group' table. These manipulations are simply host name substitutions with the names defined for the source and destination IP Groups respectively.
- The 'IP to IP Outbound Manipulation' table can also be configured using the *ini* file table parameter IPOutboundManipulation (see "SBC Parameters" on page 858).

➤ **To configure IP-to-IP outbound manipulation rules:**

1. Open the 'IP to IP Outbound Manipulation' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Manipulations SBC** submenu > **IP to IP Outbound**).

Figure 3-111: IP to IP Outbound Manipulation Page

Index	Is Additional Manipulation	Manipulated URI	Source IP Group ID	Destination IP Group ID	Source Username Prefix
1	<input type="radio"/>	Source	-1	-1	*
Source Host		Destination Username Prefix		Destination Host	
*		*		*	
				Request Type	
				All	
Remove From Left	Remove From Right	Leave From Right	Prefix to Add	Suffix to Add	Privacy Restriction Mode
0	0	255			Transparent

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 336.

Table 3-37: IP to IP Outbound Manipulation Table Parameters

Parameter	Description
Matching Characteristics	
Is Additional Manipulation [IsAdditionalManipulation]	<p>Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it.</p> <ul style="list-style-type: none"> ▪ [0] 0 = Regular manipulation rule - not done in addition to the rule above it (default). ▪ [1] 1 = If the previous table row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule. <p>Note: Additional manipulation can only be performed on a different SIP URI (either source or destination) to the rule configured in the row above (defined by the parameter ManipulatedURI).</p>
Manipulated URI [IsAdditionalManipulation]	<p>Determines whether the source or destination SIP URI user part is manipulated.</p> <ul style="list-style-type: none"> ▪ [0] Source = Manipulation is done on the source SIP URI user part (default). ▪ [1] Destination = Manipulation is done on the destination SIP URI user part.
Source IP Group ID [SrcIPGroupID]	The Source IP Group to which the INVITE belongs. For any Source IP Group, enter the value -1.
Destination IP Group ID [DestIPGroupID]	The Destination IP Group to where the INVITE is sent. For any Destination IP Group, enter the value -1.

Parameter	Description
Source Username Prefix [SrcUsernamePrefix]	The prefix of the source SIP URI user name (usually in the From header). For any prefix, enter an asterisk (*), which is the default. 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 413.
Source Host [SrcHost]	The source SIP URI host name - full name (usually in the From header). For any host name, enter an asterisk (*), which is the default.
Destination Username Prefix [DestUsernamePrefix]	The prefix of the destination SIP URI user name (usually in the Request-URI). For any prefix, enter an asterisk (*), which is the default. 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 413.
Destination Host [DestHost]	The destination SIP URI host name - full name (usually in the Request URI). For any host name, enter an asterisk (*), which is the default.
Request Type [RequestType]	SIP request type to which the manipulation rule is applied. <ul style="list-style-type: none"> ▪ [0] All = all SIP messages (default) ▪ [1] INVITE = all SIP messages except REGISTER and SUBSCRIBE ▪ [2] REGISTER = only SIP REGISTER messages ▪ [3] SUBSCRIBE = only SIP SUBSCRIBE messages ▪ [4] INVITE and REGISTER = all SIP messages except SUBSCRIBE ▪ [5] INVITE and SUBSCRIBE = all SIP messages except REGISTER
Operation Manipulation Rule (when match occurs in characteristics)	
Remove From Left [RemoveFromLeft]	The number of digits to remove from the left of the user name prefix. For example, if you enter 3 and the user name is "bobby", the new user name is "by".
Remove From Right [RemoveFromRight]	The number of digits to remove from the right of the user name prefix. For example, if you enter 3 and the user name is "bobby", the new user name is "bo".
Leave From Right [LeaveFromRight]	The number of characters that you want retained from the right of the user name.
Prefix to Add [Prefix2Add]	The number or string that you want added to the front of the user name. For example, if you enter 'sir' and the user name is "bobby", the new user name is "sirbobby".

Parameter	Description
Suffix to Add [Suffix2Add]	The number or string that you want added to the end of the user name. For example, if you enter '01' and the user name is "bobby", the new user name is "bobby01".
Privacy Restriction Mode [PrivacyRestrictionMode]	<p>Determines user privacy handling (i.e., restricting source user identity in outgoing SIP dialogs).</p> <ul style="list-style-type: none"> ▪ [0] Transparent = No intervention in SIP privacy (default). ▪ [1] Don't change privacy = The user identity remains the same as in the incoming SIP dialog. If a restricted number exists, the restricted presentation is normalized as follows: <ul style="list-style-type: none"> ✓ From URL header: anonymous@anonymous.invalid. ✓ If a P-Asserted-Identity header exists (either in the incoming SIP dialog or added by the device), a Privacy header is added with the value "id". ▪ [2] Restrict = The user identity is restricted (the restricted presentation is as mentioned above). ▪ [3] Remove Restriction = The device attempts to reveal the user identity by setting user values in the From header and removing the privacy "id" value if the Privacy header exists. <p>If the From header user is anonymous, the value is taken from the P-Preferred-Identity, P-Asserted-Identity, or Remote-Party-ID header (if exists).</p> <p>The device identifies an incoming user as restricted if one of the following exists:</p> <ul style="list-style-type: none"> ▪ From header user is anonymous. ▪ P-Asserted-Identity and Privacy headers contain the value "id". <p>Note: All restriction logic is performed after the user number has been manipulated.</p>

3.3.2.13 SAS

The **SAS** submenu allows you to configure the SAS application. This submenu includes the **Stand Alone Survivability** item page (see "Configuring Stand-Alone Survivability" on page 216), from which you can also access the 'IP2IP Routing Table' page for configuring SAS routing rules (see "Configuring IP2IP Routing Table (SAS)" on page 218).



Notes:

- The SAS menu and its page items appear only if you have enabled the SAS application (see "Enabling Applications" on page 113) and the SAS application is included in the device's Software Upgrade Key (see "Loading Software Upgrade Key" on page 339).
- For a detailed explanation on SAS, see "Stand-Alone Survivability (SAS) Application" on page 582.

3.3.2.13.1 Configuring Stand-Alone Survivability

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

➤ **To configure SAS:**

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

Figure 3-112: SAS Configuration Page

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	Un-Block
Redundant SAS Proxy Set	-1

SAS Registration Manipulation	
Remove From Right	Leave From Right
0	0

SAS Routing


SAS Routing Table

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



Notes:

- Once manipulated, the SAS application searches for the user in the registration database.
- The SAS Registration Manipulation feature does not modify the Request-URI of the outgoing INVITE message.
- The SAS Registration Manipulation can also be configured using the SASRegistrationManipulation *ini* file parameter (see "SAS Parameters" on page 216).

4. Click the **Submit** button to apply your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 336.
6. To configure the SAS Routing table, under the **SAS Routing** group, click the **SAS Routing Table**  button to open the 'IP2IP Routing Table' page. For a description of this table, see "Configuring the IP2IP Routing Table (SAS)" on page 218.

3.3.2.13.2 Configuring IP2IP Routing Table (SAS)

The 'IP2IP Routing Table' page allows you to configure up to 120 SAS routing rules (for Normal and Emergency modes). The device routes the SAS call (received SIP INVITE message) once a rule in this table is matched. If the characteristics of an incoming call do not match the first rule, the call characteristics is then compared to the settings of the second rule, and so on until a matching rule is located. If no rule is matched, the call is rejected.

When SAS receives a SIP INVITE request from a proxy server, the following routing logic is performed:

- a. Sends the request according to rules configured in the IP2IP Routing table.
- b. If no matching routing rule exists, the device sends the request according to its SAS registration database.
- c. If no routing rule is located in the database, the device sends the request according to the Request-URI header.



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

➤ To configure the IP2IP Routing table for SAS:



1. In the 'SAS Configuration' page (see "Configuring Stand-Alone Survivability" on page 216), click the **SAS Routing Table**  button; the 'IP2IP Routing Table' page appears.

Figure 3-113: IP2IP Routing Page

Index	Source IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host																				
1		*	*	*	*																				
<table border="1"> <thead> <tr> <th>RequestType</th> <th>Destination Type</th> <th>Destination IP Group ID</th> <th>Destination SRD ID</th> <th>Destination Address</th> </tr> </thead> <tbody> <tr> <td>All</td> <td>IP Group</td> <td></td> <td></td> <td></td> </tr> <tr> <td colspan="2"></td> <th>Destination Port</th> <th>Destination Transport Type</th> <th>Alternative Route Options</th> </tr> <tr> <td colspan="2"></td> <td>0</td> <td></td> <td>Route Row</td> </tr> </tbody> </table>						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
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 336.

Table 3-38: SAS IP2IP Routing Table Parameters

Parameter	Description
Matching Characteristics	
Source IP Group ID [IP2IPRouting_SrcIPGroupID]	This parameter is not applicable.
Source Username Prefix [IP2IPRouting_SrcUsernamePrefix]	<p>The prefix of the user part of the incoming INVITE's source URI (usually the From URI). The default is "".</p> <p>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 413.</p>
Source Host [IP2IPRouting_SrcHost]	<p>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 "".</p>
Destination Username Prefix [IP2IPRouting_DestUsernamePrefix]	<p>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 "".</p>
Destination Host [IP2IPRouting_DestHost]	<p>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 "".</p>
Request Type [IP2IPRouting_RequestType]	<p>The type of incoming SIP request:</p> <ul style="list-style-type: none"> ▪ [0] All (default) ▪ [1] INVITE ▪ [2] REGISTER ▪ [3] SUBSCRIBE ▪ [4] INVITE & REGISTER ▪ [5] INVITE & SUBSCRIBE
Operation Routing Rule (performed when match found in above characteristics)	
Destination Type [IP2IPRouting_DestType]	<p>Determines the destination type to which the outgoing INVITE is sent.</p> <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 SRD ID', '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 IP Group ID [IP2IPRouting_DestIPGroupID]	<p>The IP Group ID to where you want to route the call. The INVITE messages are sent to the IP address(es) defined for the Proxy Set associated with this IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Destination Address' field). However, if both parameters are configured, the IP Group takes precedence.</p> <p>If the destination IP Group is of USER type, the device searches for a match between the Request-URI (of the received INVITE) to an AOR registration record in the device's database. The INVITE is then sent to the IP address of the registered contact.</p> <p>The default is -1.</p> <p>Note: This parameter is only relevant if the parameter 'Destination Type' is set to 'IP Group'. However, regardless of the settings of the parameter 'Destination Type', the IP Group is still used - only for determining the IP Profile or outgoing SRD. If neither IP Group nor SRD are defined in this table, the destination SRD is determined according to the source SRD associated with the Source IP Group (configured in the 'IP Group' table). If this table does not define an IP Group but only an SRD, then the first IP Group associated with this SRD (in the 'IP Group' table) is used.</p>
Destination SRD ID [IP2IPRouting_DestSRDID]	<p>Determines the SRD ID.</p> <p>The default is -1.</p> <p>Note: The destination IP Group must belong to the destination SRD, if both are configured in this table.</p>
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 92).
Destination Port [IP2IPRouting_DestPort]	<p>The destination port to where the call is sent.</p>

Parameter	Description
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>
Alternative Route Options [IP2IPRouting_AltRouteOptions]	<p>This parameter is not applicable to SAS.</p>

3.3.3 Data Settings

The **Data** menu allows you to configure the device's data routing functionality. This menu contains the following submenus:

- WAN Access (see "WAN Access" on page 224)
- Firewall and ACL (see "Firewall and ACL" on page 238)
- QoS (see "QoS" on page 252)
- VPN (see "VPN" on page 262)
- Data Services (see "Data Services" on page 270)
- Data Routing (see "Data Routing" on page 276)
- Objects and Rules (see "Objects and Rules" on page 283)
- Data System (see "Configuring Network Connections" on page 287)

Before you begin configuring the data functionality, you should familiarize yourself with working with the data-related configuration pages, as described in "Getting Acquainted with Data Configuration Pages" on page 223.



Notes:

- Virtual Routing and Forwarding (VRF) can only be configured using the device's CLI. This allows multiple instances of a routing table to co-exist within the same router at the same time. The device's VRF feature allows interfaces to be clustered into a VRF to provide segregated routing domains. The VRF feature uses the device's single physical router as multiple logical routers (up to 32). Each VRF is associated with its own routing table. When creating fully separated logical routers on the same physical router, every interface can be mapped to a specified VRF and static routes can be added to it. The main CLI command for configuring VRF is **ip vrf**. Note: Some features are available only on the default, unnamed, VRF. These include, amongst others, BGP, OSPF, RIP, Management interfaces (Web, CLI and SNMP), and SIP (when using the device's VoIP component). For a complete list of features supported only on the default VRF, please contact AudioCodes. For a detailed description of CLI configuration, refer to the *MSBG Series CLI Reference Guide*.
- IPSec tunneling can only be configured using the device's CLI. This is configured using the **crypto** CLI commands. For a detailed description of CLI configuration, refer to the *MSBG Series CLI Reference Guide*.
- Power over Ethernet (PoE) status indication when an IP Phone is connected to one of the device's LAN ports. This status is provided by the CLI **GetPOEPortStatusCmd** command, which when run, displays the status.
- The device supports the monitoring of traffic traversing its LAN ports (i.e., Port Mirroring). This includes monitoring of egress and/or ingress traffic. This feature is useful for analyzing traffic or debugging network problems. The CLI commands, **port monitor** and **show data port-monitoring** are used for displaying this information.

3.3.3.1 Getting Acquainted with Data Configuration Pages

This section provides you with an overview on working with the data-routing configuration pages.

3.3.3.1.1 Working with Tables








Throughout the data section of the Web interface, various configuration icons are provided in the configuration tables. The figure below displays a typical example of such a table, where each row defines an entry in the table:

Figure 3-114: Working with Tables

Local Host	Local Address	Restricted Website	Restricted IP Address	Status	Action
<input checked="" type="checkbox"/> Any	Any	www.pokerabc.com	www.pokerabc.com (Unresolved)	Resolving...	 
<input checked="" type="checkbox"/> Any	Any	www.adultx.com	www.adultx.com	Active	 
New Entry					




The 'Action' column provides icons for performing various configuration actions, as described in the table below:


Table 3-39: Description of Table Action Icons

Icon	Name	Description
	New	Adds an entry (row) in the table.
	Edit	Edits an entry in the table.
	Remove	Deletes an entry from the table.
	Download	Downloads a file.
	Copy	Copies an item to the clipboard.
	Move Up	Moves an entry one place up in the table.
	Move Down	Moves an entry one place down in the table.

Once you have added an entry in a table, you can later disable the entry by clearing the check box corresponding to the entry. For example, you can temporarily disable an access rule, by clearing the check box, as shown below.

Figure 3-115: Checkbox for Temporarily Disabling Entry





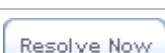


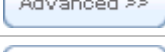
Local Host	Local Address	Protocols	Status	Action
<input checked="" type="checkbox"/> Any	Any	DirectX Games - TCP Any -> 47624-47625 TCP Any -> 2300-2400 TCP Any -> 28800-28912 UDP Any -> 47624-47625 UDP Any -> 2300-2400	Active	 
New Entry				

 Check Box for Disabling Entry

3.3.3.1.2 Using the Configuration Buttons

Throughout the Data section of the Web interface, various buttons appear in the configuration pages, as described in the table below:

Table 3-40: Description of the Main Configuration Buttons

Button	Name	Description
	OK	Applies and saves the settings.
	Apply	Applies the settings.
	Cancel	Disregards your settings.
	Refresh	Refreshes the page, updating the configuration values or status.
	Resolve Now	Verifies or validates a setting, for example, that a valid Web site exists at a specified URL.
	Close	Closes the page and returns you to the previously opened page.
	Advanced	Shows additional (advanced) fields on the page.
	Basic	Hides the advanced fields (if previously shown by clicking the Advanced button).

The above table describes the main configuration buttons. Buttons specific to a certain configuration is explained later in the relevant section.

3.3.3.2 WAN Access

The **WAN Access** menu allows you to configure your WAN (Internet) connection. When subscribing to a broadband service, your Internet Service Provider (ISP) should provide you information regarding the method by which you are connecting to the Internet.

The device can connect to the broadband service (WAN), using one of the following methods:

- Ethernet interface (copper or fiber cable), using connection methods such as automatic IP address allocation or Point-to-Point Protocol over Ethernet (PPPoE). For more information, refer to "Configuring Ethernet WAN Interface" on page 225.
- T1 WAN connection through a dual T1 line interface (according to ANSI T1.403-1999). The device uses its dual T1 WAN Data Service Unit/Channel Service Unit (DSU/CSU) port interface to transmit and receive data using IP over Point-to-Point Protocol (PPP), IP over High-Level Data Link Control (HDLC), or IP over Multilink Point-to-Point Protocol (MLPPP) framing. For more information, refer to "Configuring T1 WAN Interface" on page 227.
- Symmetric High-Speed Digital Subscriber Line (SHDSL) connection using copper wire pairs. The SHDSL WAN connection supports up to four copper wire pairs according to G.991.2, acting as a remote-terminal CPE device. Both ATM and EFM modes are supported. In the ATM mode, a variety of protocols are supported, including PPPoE, PPPoA, and RFC 2684 in both bridged (Ethernet-over-ATM) and routed (IP-over-ATM) variants. In the EFM mode, the SHDSL port functions as a logical Ethernet

device. For more information, refer to "Configuring SHDSL WAN Interface" on page 234.



Note: The supported WAN connection methods depend on the installed Software Upgrade Key. For installing a Software Upgrade Key, refer to "Loading Software Upgrade Key" on page 339.


3.3.3.2.1 Configuring Ethernet WAN Interface

For Ethernet WAN interface, you can configure the device to use one of the following methods for connecting to the Internet:

- Manual IP address Ethernet connection
- Automatic IP address Ethernet connection
- Point-to-Point Protocol over Ethernet (PPPoE)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

The type of connection should be as instructed by your ISP. If you do not have an Internet connection or if you want to disable all existing connections, select 'No Internet Connection' from the 'Connection Type' drop-down list.

Once you have defined the basic WAN connection type (listed above and described in the procedure below), you can configure advanced settings such as the WAN port's physical attributes (link speed and duplex mode) and routing. The advanced configuration parameters can be accessed using one of the following methods:

- Clicking the **Click here for Advanced Settings** link as described in Step 3 below
- Clicking the **Edit**  icon in the Connections list, as described in "Editing Existing Connections" on page 328

➤ To configure the Internet (WAN) connection:

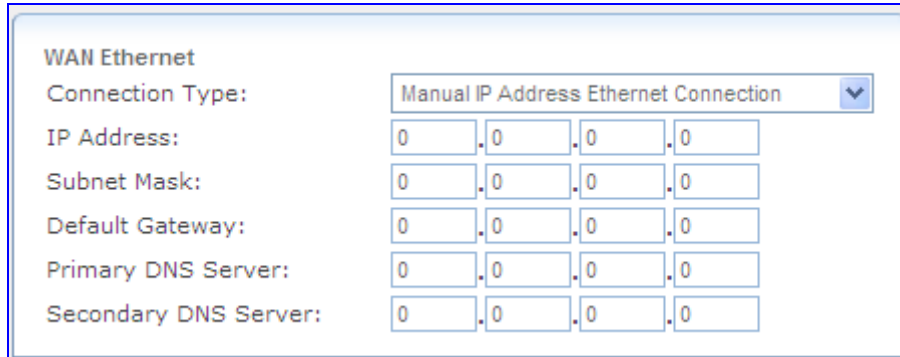
1. Open the 'Settings' page (**Configuration** tab > **Data** menu > **WAN Access** submenu > **Settings**); the following page appears:

Figure 3-116: WAN Access

WAN Ethernet	
Connection Type:	Automatic IP Address Ethernet Connection
Name:	WAN Ethernet
Status:	Connected
MAC Address:	00:90:8f:1b:33:7d
IP Address:	10.33.2.105
Subnet Mask:	255.255.0.0
Default Gateway:	10.33.0.1
DNS Server	10.1.1.11
Click here for Advanced Settings	

2. From the 'Connection Type' drop-down list, select the required WAN connection type:
 - 'Automatic IP Address Ethernet Connection' (see figure above)
 - 'Manual IP Address Ethernet Connection':

Figure 3-117: Manual WAN Connection

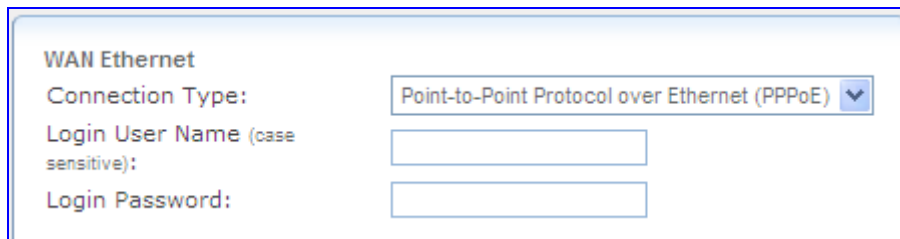


The screenshot shows a configuration window titled 'WAN Ethernet'. The 'Connection Type' dropdown is set to 'Manual IP Address Ethernet Connection'. Below this, there are six input fields, each with four sub-fields separated by dots, representing IP addresses: IP Address, Subnet Mask, Default Gateway, Primary DNS Server, and Secondary DNS Server. All sub-fields are currently set to '0'.

Specify the following:

- ◆ IP address
- ◆ Subnet mask
- ◆ Default gateway
- ◆ Primary DNS Server
- ◆ Secondary DNS Server
- 'Point-to-Point Protocol over Ethernet (PPPoE)':

Figure 3-118: PPPoE WAN Connection

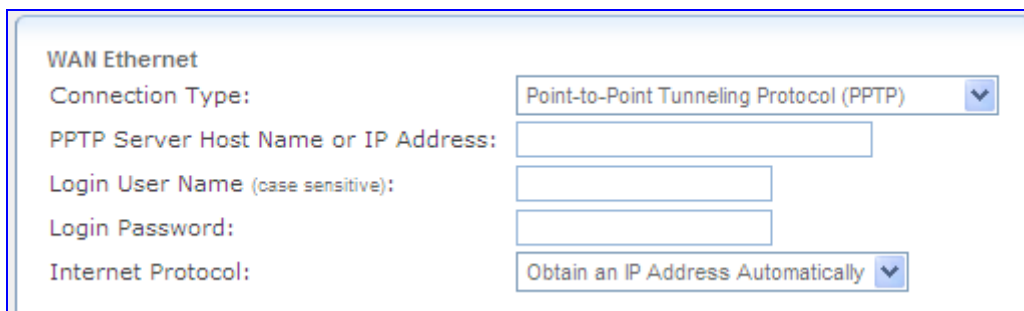


The screenshot shows a configuration window titled 'WAN Ethernet'. The 'Connection Type' dropdown is set to 'Point-to-Point Protocol over Ethernet (PPPoE)'. Below this, there are two input fields: 'Login User Name (case sensitive)' and 'Login Password'.

Specify the following:

- ◆ Login user name
- ◆ Login password
- 'Point-to-Point Tunneling Protocol (PPTP)':

Figure 3-119: PPTP WAN Connection Type



The screenshot shows a configuration window titled 'WAN Ethernet'. The 'Connection Type' dropdown is set to 'Point-to-Point Tunneling Protocol (PPTP)'. Below this, there are four input fields: 'PPTP Server Host Name or IP Address', 'Login User Name (case sensitive)', 'Login Password', and 'Internet Protocol'. The 'Internet Protocol' dropdown is set to 'Obtain an IP Address Automatically'.

Specify the following:

- ◆ PPTP Server Host Name or IP Address
 - ◆ Login User Name
 - ◆ Login Password
 - ◆ Internet Protocol - select the method used by your ISP for assigning an IP address.
- 'Layer 2 Tunneling Protocol (L2TP)':

Figure 3-120: L2TP WAN Connection Type

The screenshot shows a web-based configuration window titled "WAN Ethernet". It contains the following fields and options:

- Connection Type:** A dropdown menu with "Layer 2 Tunneling Protocol (L2TP)" selected.
- L2TP Server Host Name or IP Address:** A text input field.
- Login User Name (case sensitive):** A text input field.
- Login Password:** A text input field.
- Internet Protocol:** A dropdown menu with "Obtain an IP Address Automatically" selected.

Specify the following:

- ◆ L2TP Server Host Name or IP Address
 - ◆ Login User Name
 - ◆ Login Password
 - ◆ Internet Protocol - select the method used by your ISP for assigning an IP address
3. For advanced WAN settings, click the **Click here for Advanced Settings** link. For a detailed description of configuring advanced settings, see "Editing Existing Connections" on page 328.

3.3.3.2.2 Configuring T1 WAN Interface

The T1 WAN interface can be configured to transmit/receive data using IP over Point-to-Point Protocol (PPP), IP over High-Level Data Link Control (HDLC), or IP over Multilink Point-to-Point Protocol (also referred to as ML-PPP, MP, MPPP, MLP, or Multilink) framing. The WAN connection must contain a physical interface (T1) and a Layer-2 protocol (PPP, HDLC, or ML-PPP). The physical interface provides the actual bandwidth between the device and the network provider. The Layer 2 protocol defines how the data is packaged and presented on the physical interface. Layer 2 protocols must be configured to match the protocol provided on the circuit.


Notes:

- Each physical T1 link is configured separately.
- Local-line loopback on the T1 WAN interface can only be configured using the device's CLI. In this loopback, packets from the Tx line interface connect to the Rx line interface. The maximum time of this loopback is enabled and configured using the **loopback** CLI command. For a detailed description of CLI configuration, refer to the *MSBG Series CLI Reference Guide*.
- Bit error rate (BER) testing on the T1 WAN interface for the far-end transmission link can only be configured using the device's CLI. The BER Test is done by generating and detecting both pseudorandom and repeating bit patterns. The test is enabled using the **ber-test** CLI command. For a detailed description of CLI configuration, refer to the *MSBG Series CLI Reference Guide*.

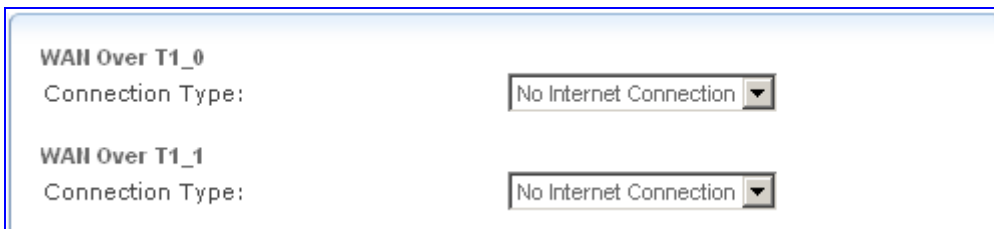
3.3.3.2.2.1 PPP over T1 WAN

The procedure below describes how to configure PPP over T1 WAN interface.

➤ **To configure PPP over T1 WAN interface:**

1. Open the 'WAN Access' page (**Configuration** tab > **Data** menu > **WAN Access** > **Settings**).

Figure 3-121: WAN Access Page for T1 WAN Interface



2. From the 'Connection Type' drop-down list, select "PPP Over T1"; the page refreshes, displaying the relevant parameters:

Figure 3-122: PPP Over T1



3. In the 'Login User Name' and 'Login Password' fields, enter the username and password provided by your Internet Service Provider (ISP), and then click **OK**.

4. Click the **Click here for Advanced Settings** link; the **General** tab page is displayed. The **General** tab allows you to define an arbitrary name for the connection (in the 'Name' field), view various statistical information of the connection, and disable the connection (by clicking **Disable**).
5. Click the **Settings** tab, and then from the 'Internet Protocol' drop-down list, select the IP address method used for the PPP link. This can be obtained automatically from the ISP or defined manually (by selecting 'Use the Following IP Address').

Figure 3-123: Settings Tab for PPP over T1

Status: **Connected**

Connection Type: PPP over T1

MTU: Automatic 1500

Internet Protocol Obtain an IP Address Automatically

☐ Override Subnet Mask: 0.0.0.0

DNS Server Obtain DNS Server Address Automatically

6. Click the **PPP** tab, and then select the supported PPP authentication and encryption methods. (You can also change the PPP login username and password.)

Figure 3-124: PPP Tab

PPP Authentication

Login User Name (case sensitive): aa

Login Password:

☒ Support Unencrypted Password (PAP)

☒ Support Challenge Handshake Authentication (CHAP)

☒ Support Microsoft CHAP (MS-CHAP)

☒ Support Microsoft CHAP Version 2 (MS-CHAP v2)

PPP Encryption

☐ Require Encryption (disconnect if server declines)

☐ Support Encryption (40 bit keys)

☐ Support Maximum Strength Encryption (128 bit keys)

7. Click the **T1** tab, and then define the following as instructed by your ISP:
 - Framing Method
 - Line Code
 - Channel Groups: define the active T1 data channels. This can be Full T1 (1.e., 1-24) or Fractional T1 (e.g., 1-3,5,8-12,24)
 - Clock Master

- Line Build Out - pulse shape of the T1 analog interface:
 - ◆ Line Loss (pulse shape of the T1 analog interface): the Line CI code, as defined by ANSI T1.403 Annex H.
 - ◆ Max Cable Loss: the maximum customer cable loss, as defined by ANSI T1.403 Annex H

Figure 3-125: T1 Tab

Framing Method:	Extended SuperFrame (F24) ▼
Line Code:	B8ZS Code Dual Rail Interface ▼
Channel Groups:	1-24
Clock Master:	Recover Data Clock From Line ▼
Remote Loopback:	Off ▼
Status:	LOS

Line Build Out	
Line Loss:	0 dB ▼
Max Cable Loss:	0.6 dB ▼

The 'Status' field displays the status of the T1 WAN interface:

- "Not available" (wait to sync)
- "Active" (sync)
- "LOS" (Red alarm – loss of signal)
- "LOF" (Red alarm – OOF)
- "AIS"
- "RAI" (Yellow alarm)

3.3.3.2.2.2 HDLC over T1 WAN

The procedure below describes how to configure HDLC over T1 WAN interface.

➤ **To configure HDLC over T1 WAN interface:**

1. Open the 'WAN Access' page (**Configuration** tab > **Data** menu > **WAN Access** > **Settings**).

Figure 3-126: WAN Access Page for T1 WAN Interface

WAN Over T1_0	
Connection Type:	No Internet Connection ▼
WAN Over T1_1	
Connection Type:	No Internet Connection ▼

- From the 'Connection Type' drop-down list, select "HDLC Over T1"; the page refreshes, displaying the relevant parameters:

Figure 3-127: HDLC Over T1

WAN Over T1	
Connection Type:	HDLC Over T1 ▼
IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0

- In the 'IP Address' and 'Subnet Mask' fields, enter the IP address supplied by your ISP for this connection, and then click **OK**.
- Click the **Click here for Advanced Settings** link; the **General** tab page is displayed. The **General** tab allows you to define an arbitrary name for the connection (in the 'Name' field), view various statistical information of the connection, and disable the connection (by clicking **Disable**).
- Click the **Settings** tab, and then from the 'Internet Protocol' drop-down list, select the IP address method used for the link. This can be obtained automatically from the ISP or defined manually (by selecting 'Use the Following IP Address').

Figure 3-128: Settings Tab HDLC over T1

Status:	Connected
Connection Type:	HDLC Over T1
Internet Protocol	
IP Address:	192 . 168 . 0 . 1
Subnet Mask:	255 . 255 . 0 . 0
DNS Server	
	Use the Following DNS Server Addresses ▼
Primary DNS Server:	192 . 168 . 5 . 1
Secondary DNS Server:	192 . 168 . 10 . 1

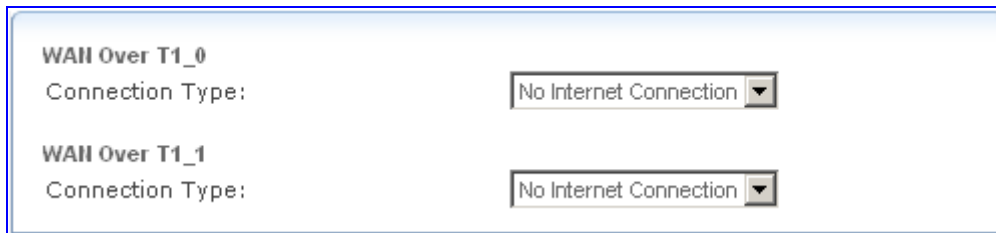
3.3.3.2.2.3 ML-PPP over T1 WAN

The procedure below describes how to configure ML-PPP over T1 WAN interface.

➤ **To configure ML-PPP over T1 WAN interface:**

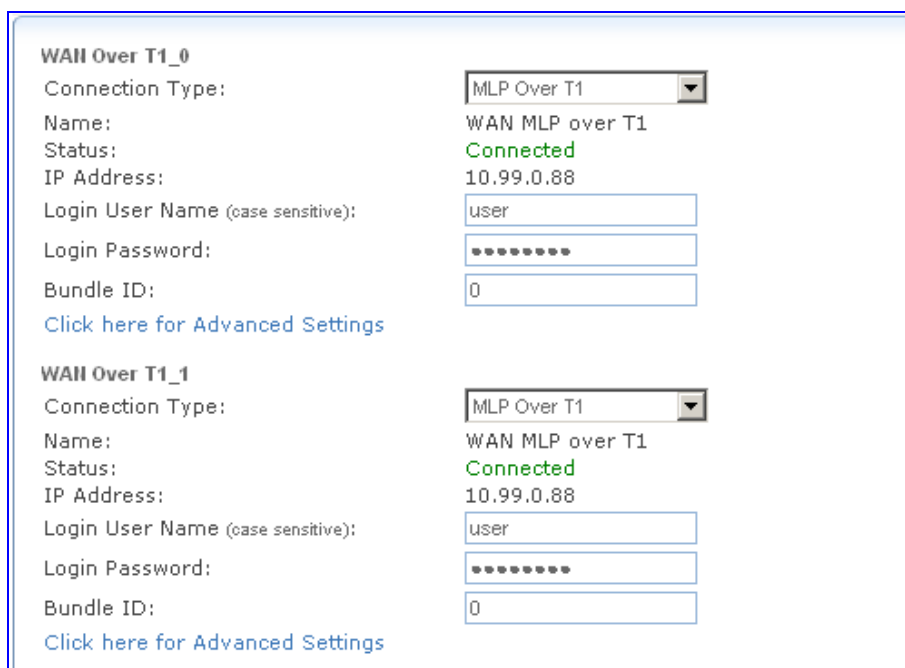
1. Open the 'WAN Access' page (**Configuration** tab > **Data** menu > **WAN Access** > **Settings**).

Figure 3-129: WAN Access Page for T1 WAN Interface



2. From the 'Connection Type' drop-down list, select "MLP Over T1"; the page refreshes, displaying the relevant parameters:

Figure 3-130: MLP over T1 WAN




Note: For each physical T1 link to which you want to add the logical bundle, perform the steps below.

- a. In the 'Login User Name' and 'Login Password' fields, enter the username and password respectively, provided by your ISP.
- b. In the 'Bundle ID' field, enter an arbitrary number that is common to all physical T1 links on the same bundle.
- c. Click **OK**.

3. Click the **Click here for Advanced Settings** link; the **General** tab page appears. The **General** tab allows you to define an arbitrary name for the connection (in the 'Name' field), view various statistical information of the connection, and disable the connection (by clicking **Disable**).
4. Click the **Settings** tab, and then from the 'Internet Protocol' drop-down list, select the IP address method used for the PPP link. This can be obtained automatically from the ISP or defined manually (by selecting 'Use the Following IP Address').

Figure 3-131: Settings Tab for MLP over T1

Status:	Connected
Connection Type:	MLP over T1
<hr/>	
Internet Protocol	Obtain an IP Address Automatically ▼
<input type="checkbox"/> Override Subnet Mask:	0 . 0 . 0 . 0
<hr/>	
DNS Server	Obtain DNS Server Address Automatically ▼

5. Click the **PPP** tab.

Figure 3-132: PPP Tab for MLP over T1 WAN

MLP Settings	
Bundle ID:	0
MRRU:	1500
Use Fragmented Mode:	No ▼
<hr/>	
PPP Authentication	
Login User Name (case sensitive):	user
Login Password:	*****
<input checked="" type="checkbox"/> Support Unencrypted Password (PAP) <input checked="" type="checkbox"/> Support Challenge Handshake Authentication (CHAP) <input checked="" type="checkbox"/> Support Microsoft CHAP (MS-CHAP) <input checked="" type="checkbox"/> Support Microsoft CHAP Version 2 (MS-CHAP v2)	
<hr/>	
PPP Encryption	
<input type="checkbox"/> Require Encryption (disconnect if server declines) <input type="checkbox"/> Support Encryption (40 bit keys) <input type="checkbox"/> Support Maximum Strength Encryption (128 bit keys)	

- a. Select the supported PPP authentication and encryption methods. (You can also change the PPP login username and password.)
- b. Configure the MLP parameters:
 - ◆ Bundle ID: the logical bundle identifier
 - ◆ MRRU: the Maximum Reconstructed Receive Unit value

- ◆ Use Fragmented Mode: whether to use a fragmented mode:
 - ✓ Yes: each packet is fragmented per the bandwidth ratio of the physical links in the bundle or non fragmented mode
 - ✓ No: each packet is sent as a whole on a single link while alternating between physical T1 links in the bundle
6. Click the **T1** tab, and then define the following as instructed by your ISP:
- Framing Method
 - Line Code
 - Channel Groups: define the active T1 data channels. This can be Full T1 (1.e., 1-24) or Fractional T1 (e.g., 1-3,5,8-12,24)
 - Clock Master
 - Line Build Out - pulse shape of the T1 analog interface:
 - ◆ Line Loss (pulse shape of the T1 analog interface): Line CI code, as defined by ANSI T1.403 Annex H
 - ◆ Max Cable Loss: maximum customer cable loss, as defined by ANSI T1.403 Annex H

Figure 3-133: T1 Tab

Framing Method:	Extended SuperFrame (F24) ▼
Line Code:	B8ZS Code Dual Rail Interface ▼
Channel Groups:	1-24
Clock Master:	Recover Data Clock From Line ▼
Remote Loopback:	Off ▼
Status:	LOS

Line Build Out	
Line Loss:	0 dB ▼
Max Cable Loss:	0.6 dB ▼

The Status field displays the status of the T1 WAN interface:

- “Not available” (wait to sync)
- “Active” (sync)
- “LOS” (Red alarm – loss of signal)
- “LOF” (Red alarm – OOF)
- “AIS”
- “RAI” (Yellow alarm)

3.3.3.2.3 Configuring SHDSL WAN Interface

The SHDSL WAN interface can be set up using a variety of protocol configurations. The WAN connection must contain a physical interface specification (SHDSL pairs and grouping information) and one or more Layer-2 protocols (PPPoE, PPPoA, RFC 2684 ETHoA, or IPoA). This configuration must match the network setup provided by your Internet Service Provider (ISP).

Multiple wire-pairs are bonded into a single broadband access link using G.991.2 multiple-pair (also known as "m-pair") technology when the transmission control is ATM, or by 802.3ah PMD Aggregation Function (PAF) when using Ethernet in the First Mile (EFM).

➤ **To configure the SHDSL WAN interface:**

1. Obtain the connection information from your ISP, including the following data:
 - Transmission control type (ATM or EFM)
 - Line rate (automatic or specific range)
 - Regional annex (A/F or B/G)
 - Number of copper wire-pairs used and the order (i.e., one pair is the master, the others are slaves)
 - VPI and VCI values
 - IP encapsulation (PPPoE, PPPoA, ETHoA, IPoA) and variant (LLC-SNAP or VC multiplexing)
 - ATM service class information (CBR/VBR/UBR and data rates)
2. Open the 'SHDSL Line Settings' page (**Configuration** tab > **Data** menu > **WAN Access** > **SHDSL Line Settings**).
3. Select ATM or EFM mode of operation. Note that any change to this setting erases all SHDSL configuration; after switching modes, save the configuration to flash and reset the device.

Figure 3-134: SHDSL Line Mode Page

SHDSL line mode: ATM

Shdsl Group Table

Group ID	Annex	DSL Line rate	Pairs	Termination	Status	Action
0	a	auto	0	cpe	RUNNING	
1	a	auto	1	co	RUNNING	

[New Group](#)

4. Click **New Group**  to add a new SHDSL wire.

Figure 3-135: Adding a New Group

dev name:	shdsl_atm0
Group ID:	0
Annex:	a
DSL Line rate:	auto
Pairs: Master:	0
Slave 1:	1
Slave 2:	none
Slave 3:	none
Termination:	cpe



Note: When using EFM, only one wire-pair group can be defined.

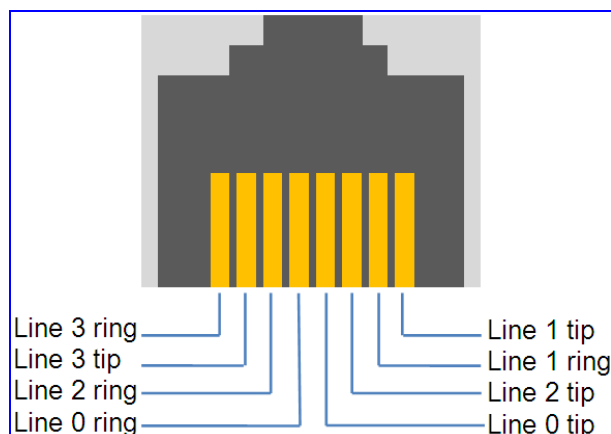
5. Configure the annex, line rate, and pair numbers as provided by your ISP, and then click **OK**.



Note: Central Office (CO) termination mode is available for diagnosis only; the device cannot be used as a full-featured DSLAM or LTU.

6. Connect the SHDSL cabling as required. SHDSL wire pairs are numbered 0 to 3, according to the following RJ-45 connector pinouts:








Figure 3-136: SHDSL RJ-45 Wire Pinouts



7. Click the **SHDSL Line Settings** link to refresh the status display and wait for the line to synchronize. Ensure that the group status displays "RUNNING" before proceeding to the next step.

8. If EFM mode was selected, skip the following steps and proceed to "Configuring Ethernet WAN Interface" on page 225.
9. Open the 'Protocol Interface Settings' page (**Configuration** tab > **Data** menu > **WAN Access** > **Protocol Interface Settings**); the current ATM interface list is displayed.

Figure 3-137: Protocol Interface Settings Page

Name	Status	Action
 PPPoE on SHDSL ATM 0/0  SHDSL ATM 1/0 New Connection	Reconnecting... Connected	    

10. Click **New Connection**, select the 'Internet Connection' option, and then click **Next**.

Figure 3-138: Choosing Internet Connection Type

☒ SHDSL PPPoE connection
SHDSL PPPoE connection (RFC2364)

☐ SHDSL RFC2684 connection
SHDSL ETHoA or IPoA connection (RFC2684 Bridged/Routed mode)

☐ SHDSL PPPoA connection
SHDSL PPPoA connection (RFC2364)

11. Select the required IP encapsulation method, and then click **Next**.

Figure 3-139: Configuring Internet Connection

SHDSL Group number:

Sub interface number:

ATM VPI:

ATM VCI:

ATM Traffic class:

Peak Cell Rate:

Sustained Cell Rate:

Burst size:

ATM Encapsulation:

Login User Name (case sensitive):

Login Password:

Internet Protocol:

DNS Server:

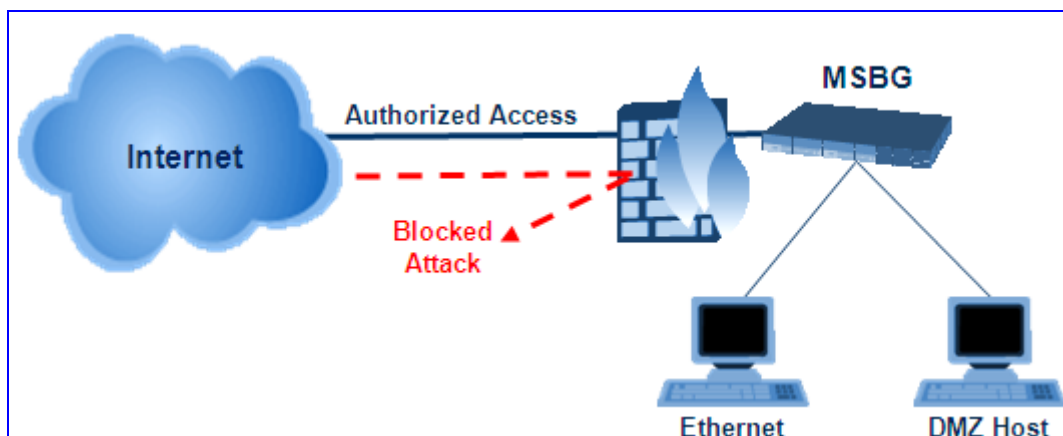
- a. Select a unique sub-interface number for the new connection.

- b. Configure the VPI, VCI, encapsulation variant and class-of-service parameters as provided by your ISP. Note that the VPI/VCI combination must be unique in an SHDSL group.
 - c. If required by your ISP, configure the IP addressing parameters (IP address, network mask, DNS server information); otherwise, use the default setting "Obtain an IP address automatically".
 - d. For PPPoE and PPPoA links, enter the user name and password for the connection.
 - e. Click **Next** and then **Finish** to complete creating the connection.
12. Repeat as necessary for any additional ATM interfaces.

3.3.3.3 Firewall and ACL

The **Firewall and ACL** menu allows you to configure various security applications. The device's security suite includes comprehensive and robust security services: Stateful Packet Inspection Firewall, user authentication protocols and password protection mechanisms. These features together allow users to connect their computers to the Internet and simultaneously be protected from the security threats of the Internet. The device's firewall has been pre-configured to provide optimum security (see the figure below).

Figure 3-140: Device's Firewall (Example)



The device's firewall provides both security and flexibility. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as Internet gaming and video-conferencing. Additional features, including surfing restrictions and access control, can also be easily configured locally by the user through a user-friendly Web-based interface, or remotely by a service provider. The firewall supports advanced filtering, designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN network devices.

The **Firewall and ACL** menu includes the following items:

- **General Security:** allows you to choose the security level for the firewall (see "Configuring General Security Settings" on page 239).
- **LAN Restrictions:** allows you to restrict access from the device's LAN network to the Internet (see "Configuring LAN Restrictions" on page 240).
- **Port Forwarding:** allows you to enable access from the Internet to specified services provided by computers in the network and special Internet applications (see "Configuring Port Forwarding" on page 242).

- **DMZ Host:** allows you to configure a LAN host to receive all traffic arriving at your device, which does not belong to a known session (see "Configuring DMZ Host" on page 244).
- **Port Triggering:** allows you to define port triggering entries to dynamically open the firewall for specific protocols or ports (see "Configuring Port Triggering" on page 244).
- **Web Restrictions:** allows you to block LAN access to specified hosts or Web sites on the Internet (see "Configuring Website Restrictions" on page 246).
- **NAT:** allows you to manually control the translation of network addresses and ports (see "Configuring NAT" on page 247).
- **Access Lists:** allows you to define firewall settings and rules (see "Configuring the Access List" on page 249).
- **Advanced Filtering:** allows you to assign Access List rules to the device's LAN/WAN interfaces (see "Configuring Advanced Filtering" on page 252).

3.3.3.3.1 Configuring General Security Settings

The **General Security** item allows you to easily configure the device's basic security settings. The firewall regulates the flow of data between the enterprise's network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through) or rejected (barred from passing through) according to the configurable set of rules.

The firewall rules specify what types of services available on the Internet may be accessed from the enterprise's network and what types of services available in the enterprise's network may be accessed from the Internet. Each request for a service that the firewall receives, whether originating in the Internet or from a computer in the enterprise's network is checked against the set of firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, then all subsequent data associated with this request (a "session") is also allowed to pass, regardless of its direction.

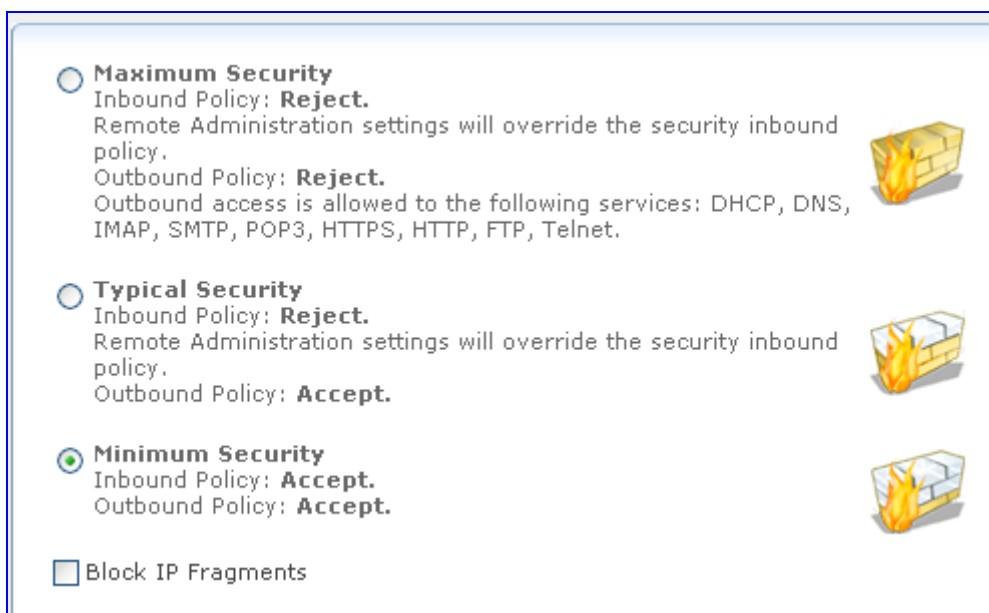
For example, when you point your Web browser to a Web page on the Internet, a request is sent out to the Internet for this page. The device's firewall identifies the request type and origin—HTTP and a specific PC in your enterprise's network, in this case. Unless you have configured access control to block requests of this type from this computer, the firewall allows this request to pass out onto the Internet. When the Web page is returned from the Web server the firewall associates it with this session and allows it to pass, regardless of whether HTTP access from the Internet to the enterprise's network is blocked or permitted. Therefore, it is the origin of the request, not subsequent responses to this request that determines whether a session can be established or not.

These services include Telnet, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP. The list of allowed services at 'Maximum Security' mode can be edited in the Access Control page. Note that some applications (such as some Internet messengers and Peer-To-Peer client applications) tend to use these ports if they cannot connect with their own default ports. When applying this behavior, these applications will not be blocked outbound, even at Maximum Security Level.

➤ **To configure basic security:**

1. Click the **General Security** item (**Configuration** tab > **Data** menu > **Firewall and ACL** submenu > **General Security**); the following page appears:

Figure 3-141: Configuring General Security



☐ **Maximum Security**
Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Reject.**
Outbound access is allowed to the following services: DHCP, DNS, IMAP, SMTP, POP3, HTTPS, HTTP, FTP, Telnet.

☐ **Typical Security**
Inbound Policy: **Reject.**
Remote Administration settings will override the security inbound policy.
Outbound Policy: **Accept.**

☒ **Minimum Security**
Inbound Policy: **Accept.**
Outbound Policy: **Accept.**

☐ Block IP Fragments

2. Select one of the pre-defined security levels.



Note: Selecting the 'Minimum Security' option may expose the enterprise's network to significant security risks, and therefore, should only be used if necessary.

3. Select the 'Block IP Fragments' check box to protect your network from a common type of hacker attack that could make use of fragmented data packets to sabotage your network. Note that VPN over IPsec and some UDP-based services make legitimate use of IP fragments. Therefore, you need to allow IP fragments to pass into the enterprise's network to make use of these select services.
4. Click **OK** to save your settings.

3.3.3.3.2 Configuring LAN Restrictions

The **LAN Restrictions** item allows you to define restriction rules on the types of requests that may pass from the LAN network to the Internet, and thus, may block traffic flowing in both directions. It can also be used for allowing specific services when maximum security is configured. You may want to block specific computers within the home network (or even the whole network) from accessing certain services on the Internet. For example, you may want to prohibit one computer from surfing the Web, and the whole network from receiving incoming e-mail (by blocking their outgoing requests to POP3 servers on the Internet). There are numerous services you should consider blocking, such as popular game and file sharing servers. For example, if you want to make sure that your employees do not put your business at risk from illegally traded copyright files, you may want to block several popular P2P and file sharing applications.



Note: When Web Filtering is enabled, HTTP services cannot be blocked by Access Control.

➤ **To configure LAN restrictions rule:**

1. Click the **LAN Restrictions** item (**Configuration** tab > **Data** menu > **Firewall and ACL** submenu > **LAN Restrictions**); the following page appears:

Figure 3-142: Configuring LAN Restriction Rules

Local Host	Local Address	Protocols	Status	Action
New Entry				+


2. Click the **New**  icon; the following page appears:

Figure 3-143: Adding an Access Control Rule

Address	Any
Protocol	Any
<input checked="" type="checkbox"/> Reply an HTML Page to the Blocked Client	
Schedule	Always




3. From the 'Address' drop-down list, specify the computer or group of computers on which you would like to apply the access control rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all the device's LAN hosts. If you want to add a new address, select the 'User Defined' option, and then follow the sequence to add a new Network Object, representing the new host (see "Configuring Network Objects" on page 284).
4. From the 'Protocol' drop-down list, select or specify the type of protocol. Selecting the 'Show All Services' option expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option, and then follow the sequence to add a new Service representing the protocol (see "Configuring Protocols" on page 283).
5. Select the 'Reply an HTML Page to the Blocked Client' check box to display the following message to the client: "Access Denied – this computer is not allowed to surf the WAN. Please contact your admin.". When this check box is cleared, the client's packets are simply ignored and no notification is issued.
6. From the 'Schedule' drop-down list, select the time during which the rule is active. By default, the rule is always active. However, you can configure scheduler rules by selecting 'User Defined', and then defining the day and time period during which the rule is active. Once a scheduler rule(s) is defined, the 'Schedule' drop-down list allows you to choose an available rule (for adding user-defined schedule rules, see "Configuring Scheduler Rules" on page 285).
7. Click **OK** to save your changes; the LAN restriction rule is displayed in the LAN Restriction list.

You can disable a LAN restriction rule to make a service available without having to delete the rule. This may be useful if you wish to make the service temporarily available and expect to reinstate the restriction in the future.

➤ **To disable a LAN restriction rule:**

- In the LAN Restriction list, clear the check box corresponding to the rule that you want to disable.

Figure 3-144: Disabled LAN Restrictions - Cleared Check Box

Local Host	Local Address	Protocols	Status	Action
<input type="checkbox"/> Any	Any	FTP - TCP Any -> 21	Active	 
New Entry				

3.3.3.3 Configuring Port Forwarding

By default, the device blocks all external users from connecting to or communicating with your network. Therefore, the system is safe from hackers who may try to intrude on the network and damage it. However, you may want to expose your network to the Internet in certain limited and controlled ways to enable some applications to work from the LAN (game, voice and chat applications, for example) and to enable Internet-access to servers in the home network. The Port Forwarding feature supports both of these functionalities.

The **Port Forwarding** item enables you to define the applications that require special handling by the device. This allows you to select the application's protocol (or add a new protocol) and the local IP address of the computer that will be using or providing the service.

Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that will provide it. This is useful, for example, if you want to host a Web server inside your home network. When an Internet user points a browser to the device's WAN IP address, the device forwards the incoming HTTP request to your Web server.

Note that as the device has one external (WAN) IP address, different applications can be assigned to your LAN computers, however each type of application is limited to one computer (IP address). Therefore, to overcome this, you can add additional public IP addresses to port forwarding rules, which you must first obtain from your ISP, and enter into the 'NAT IP Addresses Pool' (see "NAT" on page 247).

Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. For example, you have a Web server running on your PC on port 8080 and you want to grant access to this server to anyone who accesses the device via HTTP. To accomplish this, you have to define a port forwarding rule for the HTTP service, with the PC's IP or host name, as well as specify 8080 in the 'Forward to Port' field. All incoming HTTP traffic is now forwarded to the PC running the Web server on port 8080.

When setting a port forwarding service, you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP—the port used by the device's VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.

➤ **To configure a port forwarding service:**

1. Click the **Port Forwarding** item (**Configuration** tab > **Data** menu > **Firewall and ACL** submenu > **Port Forwarding**); the following page appears:

Figure 3-145: Configuring Port Forwarding

Local Host	Local Address	Public IP Address	Protocols	Status	Action
<input type="checkbox"/> 192.168.0.2	192.168.0.2	Any	Any	Disabled	 
New Entry 					

2. Click the **New Entry** link; the following page appears:

Figure 3-146: Adding Port Forwarding Rule

☐ Specify Public IP Address

Local Host:

Protocol: Any

Forward to Port: Same as Incoming Port

Schedule: Always

3. Select the 'Specify Public IP Address' check box if you want to apply this rule on the device's non-default IP address, defined in the 'NAT' page (see "Configuring NAT" on page 247) and then in the 'Public IP Address' field, enter the additional external IP address.
4. In the 'Local Host' field, enter the host name or IP address of the computer that will provide the service (the "server"). Note that unless an additional external IP address has been added, only one LAN computer can be assigned to provide a specific service or application.
5. From the 'Protocol' drop-down list, select or specify the type of protocol. Selecting the 'Show All Services' option expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option, and then add a new Service, representing the protocol (see "Configuring Protocols" on page 283).
6. From the 'Forward to Port' drop-down list, select the 'Specify' option and define a port to redirect traffic to a different port. By default, the device forwards traffic to the same port as the incoming port.
7. From the 'Schedule' drop-down list, select the time during which the rule is active. By default, the rule is always active. However, you can configure scheduler rules by selecting 'User Defined', and then defining the day and time period during which the rule is active. Once a scheduler rule(s) is defined, the 'Schedule' drop-down list allows you to choose an available rule (for adding user-defined schedule rules, see "Configuring Scheduler Rules" on page 285).
8. Click **OK** to save your changes; the main Port Forwarding page displays a summary of the rule that you added.

3.3.3.3.4 Configuring DMZ Host

The DMZ (Demilitarized) Host feature allows a single local computer to be exposed to the Internet. You can designate a DMZ host for the following scenario examples:

- You wish to use a special-purpose Internet service, such as an on-line game or video conferencing program that is not present in the Port Forwarding list and for which no port range information is available.
- You are not concerned with security and wish to expose one computer to all services without restriction.




Warning: A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

For an incoming request for access to a service in the home network, such as a Web server, the device forwards this request to the DMZ host (if one is designated) unless the service is being provided by another PC in the home network (assigned in Port Forwarding), in which case that PC receives the request instead.

➤ **To designate a local computer as a DMZ Host:**

1. Click the **DMZ Host** item (**Configuration** tab > **Data** menu > **Firewall and ACL** submenu > **DMZ Host**); the following page appears:

Figure 3-147: Defining a DMZ Host



2. Select the check box, and then enter the local IP address of the computer that you want to designate as a DMZ host. Note that only one LAN computer may be a DMZ host at any time.
3. Click **OK** to save the settings.

3.3.3.3.5 Configuring Port Triggering

Port triggering can be used for dynamic port forwarding configuration. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed. For example, consider a gaming server that is accessed using UDP protocol on port 2222. The gaming server responds by connecting the user using UDP on port 3333 when starting gaming sessions. In such a case, you must use port triggering, since this scenario conflicts with the following default firewall settings:


- The firewall blocks inbound traffic, by default.
- The server replies to the device's IP address, and the connection is not sent back to your host, since it is not part of a session.

To solve this you need to define a Port Triggering entry, which allows inbound traffic on UDP port 3333, only after a LAN host generated traffic to UDP port 2222. This will result in accepting the inbound traffic from the gaming server and sending it back to the LAN Host which originated the outgoing traffic to UDP port 2222.

➤ **To configure port triggering:**

1. Click the **Port Triggering** item (**Configuration** tab > **Data** menu > **Firewall and ACL** submenu > **Port Triggering**); the following page appears:

Figure 3-148: Configuring Port Triggering

Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
<input checked="" type="checkbox"/> L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating Ports	✗
<input checked="" type="checkbox"/> TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating Ports	✗
Add... 			


2. From the drop-down list, you can select a pre-configured service by selecting 'Show All Services', and then from the refreshed drop-down list, selecting a service.

If you want to define your own service, select 'User-Defined'; the following page appears:


Figure 3-149: Editing Port Triggering Rule

Service Name:

Outgoing Trigger Ports

Protocol	Server Ports	Action
New Trigger Ports		

Incoming Ports to Open

Protocol	Opened Ports	Action
New Opened Ports		

3. In the 'Service Name', enter a name for the service (e.g. "game_server"), and then under the 'Outgoing Trigger Ports' group, click the **New Trigger Ports** link; the following page appears:

Figure 3-150: Defining Trigger Ports

Protocol

Protocol Number:

4. From the 'Protocol' drop-down lists, select the protocol (e.g., 'UDP'); the 'Source Ports' and 'Destination Ports' fields appear.
5. Leave the 'Source Ports' value at its default 'Any'.
6. In the 'Destination Ports' drop-down list, select 'Single'; a field for entering the destination port appears (enter the destination port, e.g., "2222").
7. Click **OK** to save the settings.
8. Under the 'Incoming Ports to Open' group, click the **New Opened Ports** link, and then configure the incoming ports by repeating steps 4 through 7, but entering values for incoming ports.

3.3.3.3.6 Configuring Website Restrictions

You can configure the device to block specific Internet Web sites so that they cannot be accessed from computers in the home network. Moreover, restrictions can be applied to a comprehensive and automatically-updated table of sites to which access is not recommended.

➤ **To block access to a web site:**

1. Click the **Web Restrictions** item (**Configuration** tab > **Data** menu > **Firewall and ACL** submenu > **Web Restrictions**); the following page appears:

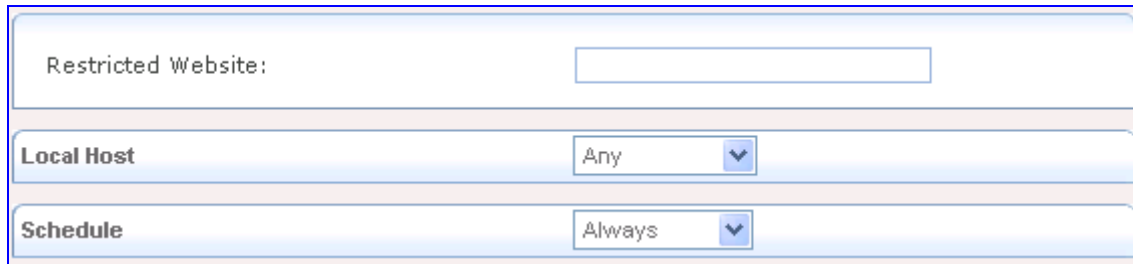
Figure 3-151: Configuring Website Restrictions



Local Host	Local Address	Restricted Website	Restricted IP Address	Status	Action
New Entry					

2. Click the **New Entry** link; the following page appears:

Figure 3-152: Adding a Restricted Website



Restricted Website:

Local Host: Any ▼

Schedule: Always ▼

3. In the 'Restricted Website' field, enter the URL (or part of the URL) that you want to make inaccessible from your home network (all Web pages within this URL are also be blocked). If the URL has multiple IP addresses, the device resolves all additional addresses and automatically adds them to the restrictions table.
4. From the 'Local Host' drop-down list, specify the computer or group of computers to which you want to apply the Web site restriction. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all the device's LAN hosts. If you want to add a new address, select the 'User Defined' option and add a new Network Object representing the new host (see "Configuring Network Objects" on page 284).
5. From the 'Schedule' drop-down list, select the time during which the rule is active. By default, the rule is always active. However, you can configure scheduler rules by selecting 'User Defined', and then defining the day and time period during which the rule is active. Once a scheduler rule(s) is defined, the 'Schedule' drop-down list allows you to choose an available rule (for defining user-defined schedule rules, see "Configuring Scheduler Rules" on page 285).
6. Click **OK** to save the settings; you are returned to the previous page while the device attempts to find the site. 'Resolving...' appears in the Status column while the site is being located (the URL is 'resolved' into one or more IP addresses).
7. Click **Refresh** to update the status if necessary. If the site is successfully located, then 'Resolved' appears in the status bar, otherwise 'Hostname Resolution Failed' appears.

3.3.3.3.7 Configuring NAT

The device features a configurable Network Address Translation (NAT) and Network Address Port Translation (NAPT) mechanism, allowing you to control the network addresses and ports of packets routed through the device. When enabling multiple computers on your network to access the Internet using a fixed number of public IP addresses, you can define static NAT/NATP rules which map (translate) LAN IP addresses (LAN computers) to NAT IP addresses and/or ports.


By default, the device operates in NAPT routing mode (see "Configuring Network Connections" on page 287). The NAT/NAPT mechanism is useful for managing Internet usage in your LAN, or complying with various application demands. For example, you can assign your primary LAN computer with a single NAT IP address to assure its permanent connection to the Internet. Another example is when an application server with which you wish to connect such as a security server, requires that packets have a specific IP address – you can define a NAT rule for that address.



For example, if you have LAN IP addresses of 192.168.1.10 to 192.168.1.15 (i.e., six PC's), and you have obtained from your ISP the NAT IP addresses 192.168.71.12 through 192.168.71.15 (i.e., four NAT addresses), you can map the six LAN IP addresses to the four NAT IP addresses. This would mean that only four of the six LAN computers may have WAN access at the same time. You can also ensure that a computer always has access to the Internet, by defining a new rule mapping its LAN IP address to one of the NAT IP address (and excluding this NAT IP address from the second rule for the other computers).

➤ **To configure NAT:**

1. Click the **NAT** item (**Configuration** tab > **Data** menu > **Firewall and ACL** submenu > **NAT**); the following page appears:

Figure 3-153: Configuring NAT

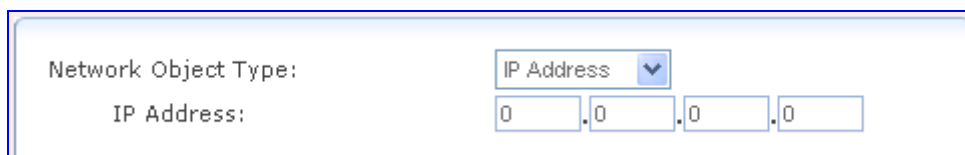
NAT IP Addresses Pool						
IP Address						Action
New IP Address						

NAT/NAPT Rule Sets						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						
New Entry						
New Entry						

2. Define additional public IP addresses obtained from your ISP as your NAT IP addresses (the primary IP address used by the WAN device for dynamic NAPT must not be added):

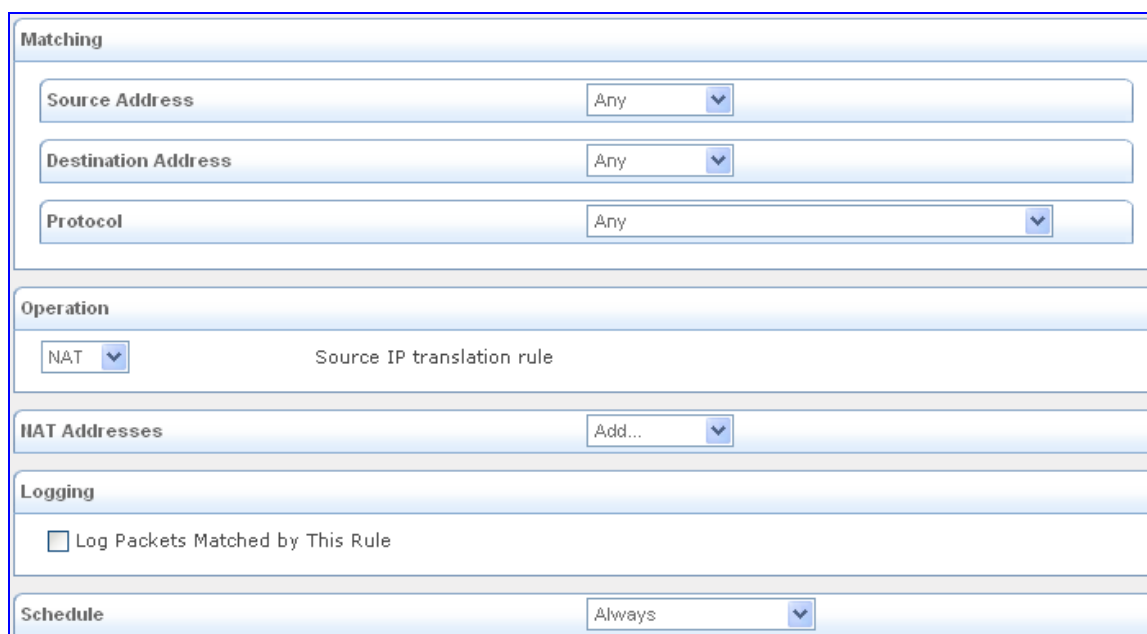
- a. Under the 'NAT IP Addresses Pool' group, click the **New IP Address** link; the following page appears:

Figure 3-154: Defining Public IP Address



- b. From the 'Network Object Type' drop-down list, select between 'IP Address', 'IP Subnet' or 'IP Range', and then enter the information respectively.
 - c. Click **OK** to save the settings; you are returned to the main page.
3. Define a new NAT/NAPT rule:
 - a. Under the 'NAT/NAPT Rule Sets' group, click the **New Entry** link; the following page appears:

Figure 3-155: Defining NAT/NAPT Rule



This page is divided into two main groups: 'Matching' and 'Operation'. The 'Matching' group defines the LAN addresses to be translated to the external addresses, which are defined in the 'Operation' group.

4. Configure the 'Matching' group parameters to define characteristics of the packets matching the rule.
 - a. **Source Address:** source address of packets sent or received by the device. Specify the computer or group of computers to which you want to apply the rule. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all the device's LAN hosts. If you want to add a new address, select 'User Defined' to add a new Network Object representing the new host (see "Configuring Network Objects" on page 284).
 - b. **Destination Address:** destination address of packets sent or received the device. This address can be configured in the same manner as the source address.
 - c. **Protocol:** specify a traffic protocol. Selecting the 'Show All Services' option expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option to add a new Service representing the protocol (see "Configuring Protocols" on page 283).

5. Configure the 'Operation' group parameters to define the operation that will be applied to the IP addresses matching the criteria defined above. The operations available are NAT or NAPT:
 - **NAT:** The NAT address into which the original IP address is translated. The drop-down list displays all of your available NAT addresses/ranges, from which you can select an entry. If you want to add a single address or a sub-range from the given pool/range, select the 'User Defined' option to add a new Network Object representing the new host (see "Configuring Network Objects" on page 284).
 - **NAPT:** The NAPT address into which the original IP address is translated. The drop-down list displays all of your available NAPT addresses/ranges, from which you can select an entry. If you want to add a single address or a sub-range from the given pool/range, select 'User Defined' to add a new Network Object representing the new host (see "Configuring Network Objects" on page 284). Enter a single port or select 'Range' to enter a range of ports.
6. Select the 'Log Packets Matched by This Rule' check box to log the first packet from a connection that was matched by this rule.
7. From the 'Schedule' drop-down list, select the time during which the rule is active. By default, the rule is always active. However, you can configure scheduler rules by selecting 'User Defined', and then defining the day and time period during which the rule is active. Once a scheduler rule(s) is defined, the 'Schedule' drop-down list allows you to choose an available rule (for adding user-defined schedule rules, see "Configuring Scheduler Rules" on page 285).

3.3.3.3.8 Configuring the Access List

The Access list is designed to allow comprehensive control over the firewall's behavior. You can define specific set of rules for ingress (inbound) and egress (outbound) traffic and control the order of logically similar sets of rules. These rules can later be assigned to the device's LAN and/or WAN interfaces (see "Configuring Advanced Filtering").



Note: Only one Access List group can be assigned to an interface. Therefore, ensure that your Access List group includes all the required rules that you want to later assign to a specific interface.

➤ To configure Access List rules:

1. Open the **Access Lists** table (**Configuration** tab > **Data** menu > **Firewall and ACL** submenu > **Access List**); the following appears:

Figure 3-156: Access Lists Table

Access Lists						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
New ACL						+


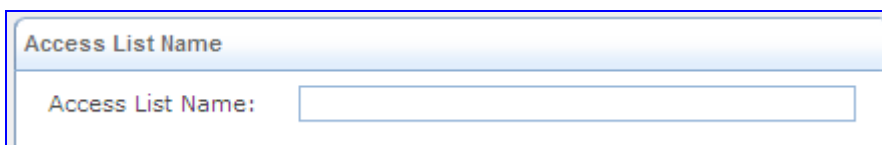
2. Add a new Access List group name:
 - a. Click the **New ACL**  link; the 'Access List Name' page appears.

Figure 3-157: Defining Access List Name




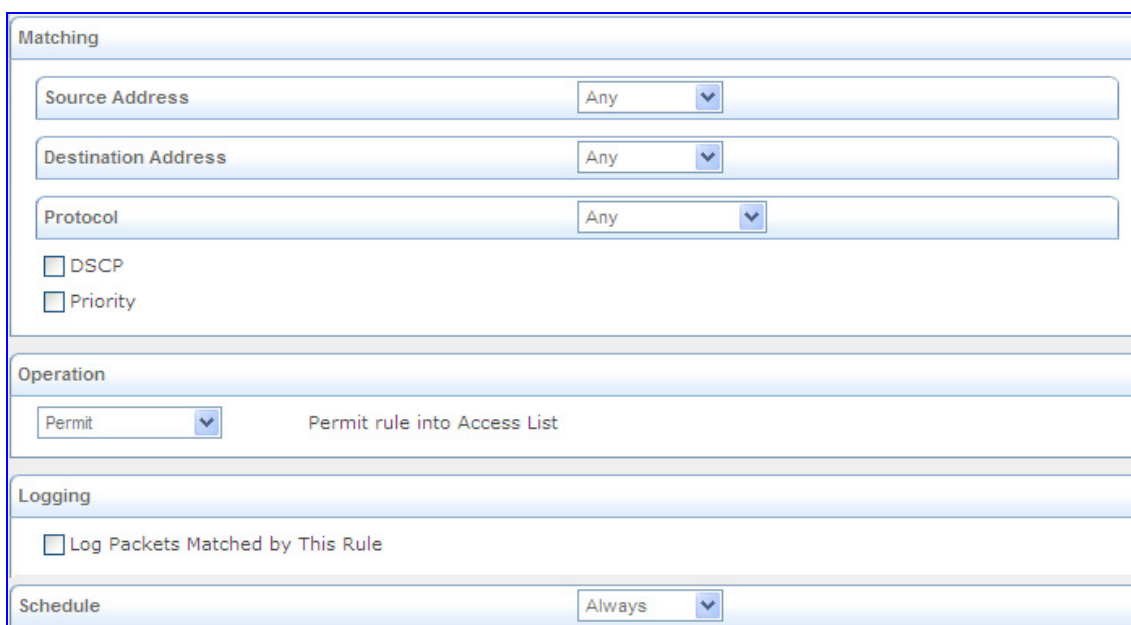
- b. In the 'Access List Name' field, enter a name for the Access List rule group, and then click **OK**; the Access Lists table re-appears, displaying the newly added Access List rule group.
3. Add rules to the Access List group:
 - a. Under the Access List name that you defined (in Step 2), click the **New Entry**  link; the following page appears for defining a rule:

Figure 3-158: Adding an Access List Rules





















The 'Matching' and 'Operation' groups define the operation to be executed when matching conditions apply.

- b. Configure the 'Matching' parameters to define characteristics of the packets matching the rule:
 - ◆ **Source Address:** Specify the source address (i.e., computers) of packets sent or received by the device. Select an address or a name from the list to apply the rule on the corresponding host, or 'Any' to apply the rule on all the device's LAN hosts. If you want to add a new address, select the 'User Defined' option to add a new Network Object representing the new host (see "Configuring Network Objects" on page 284).
 - ◆ **Destination Address:** Destination address of packets sent or received by the device. This address can be configured in the same manner as the source address.
 - ◆ **Protocol:** Specify a traffic protocol. Selecting the 'Show All Services' option expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option to add a new Service representing the protocol (see "Configuring Protocols" on page 283).

- ♦ **DSCP:** Select this check box to display two DSCP fields, which enable you to specify a hexadecimal DSCP value and its mask assigned to the packets matching the priority rule.
 - ♦ **Priority:** Select this check box to display a drop-down list in which you can select a priority level assigned to the packets matching the priority rule.
- c. Configure the 'Operation' parameters to define the action that the rule performs:
- ♦ **Permit Established:** Allow access to packets that match the criteria defined. The data transfer session is handled using Stateful Packet Inspection (SPI), meaning that other packets matching this rule are automatically allowed access.
 - ♦ **Permit:** Allow access to packets that match the criteria defined, without keeping track of the data transfer session state.
 - ♦ **Deny:** Deny access to packets that match the source and destination IP addresses and service ports defined above.
- d. Select the 'Log Packets Matched by This Rule' check box to log the first packet from a connection that was matched by this rule.
- e. From the 'Schedule' drop-down list, select the time during which the rule is active. By default, the rule is always active. However, you can configure scheduler rules by selecting 'User Defined', and then defining the day and time period during which the rule is active. Once a scheduler rule(s) is defined, the 'Schedule' drop-down list allows you to choose an available rule (for adding user-defined schedule rules, see "Configuring Scheduler Rules" on page 285).
4. Click **OK** to save your changes; the Access Lists table re-appears, displaying the defined rules under the Access List Rule ID:

Figure 3-159: Added Access List Rules

Access Lists						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Firewall						
<input checked="" type="checkbox"/> 0	1.1.1.1	Any	HTTPS - TCP Any -> 443	Permit	Active	   
<input checked="" type="checkbox"/> 1	1.1.1.1	Any	SSH - TCP Any -> 22	Permit	Active	   
<input checked="" type="checkbox"/> 2	1.1.1.3	Any	RTP (Block) - UDP Any -> 6600-6700	Deny	Active	   
<input checked="" type="checkbox"/> 3	1.1.1.3	Any	RTP - UDP Any -> 6000-8000	Permit	Active	   
New Entry						
New ACL						

The order of the rules appearing under a specific Access List name represents both the order in which they are defined and the sequence by which they are applied. You

can change this order, by using the **Move Up**  and **Move Down**  icons.

5. Assign the Access List rule ID to the required LAN or WAN interface (see "Configuring Advanced Filtering").

3.3.3.3.9 Configuring Advanced Filtering

The Advanced Filtering allows you to assign Access List rules (defined in "Configuring the Access List" on page 249) to the device's LAN and/or WAN interfaces.

➤ To assign Access List rules to the device's LAN/WAN interfaces:

1. Click the **Advanced Filtering** item (**Configuration** tab > **Data** menu > **Firewall and ACL** submenu > **Advanced Filtering**); the following page appears listing the device's LAN/WAN interfaces and a corresponding drop-down list containing the defined Access list rules (in "Configuring the Access List" on page 249):

Figure 3-160: Advanced Filtering

Interface	Out Access List	In Access List
WAN Ethernet	Select... ▼	WAN Firewall ▼
LAN switch VLAN 1	Select... ▼	Select... ▼
VPN IPSec	Select... ▼	Select... ▼

2. From the drop-down list corresponding to the interface to which you want to apply an Access List rules, select the required Access List group name.
3. Click **OK**.

3.3.3.4 QoS

The device's Quality of Service (QoS) provides the capability to provide better service to selected network traffic. This is achieved by shaping the traffic and processing higher priority traffic before lower priority traffic.

The **QoS** menu provides the following items:

- **General QoS** (see "Configuring General QoS Settings" on page 253)
- **Match Rules** (see "Configuring Matching Rules" on page 253)
- **Traffic Shaping** (see "Configuring Traffic Shaping" on page 256)
- **DSCP Settings** (see "Configuring DSCP Settings" on page 260)
- **802.1p Settings** (see "Configuring 802.1p Settings" on page 262)

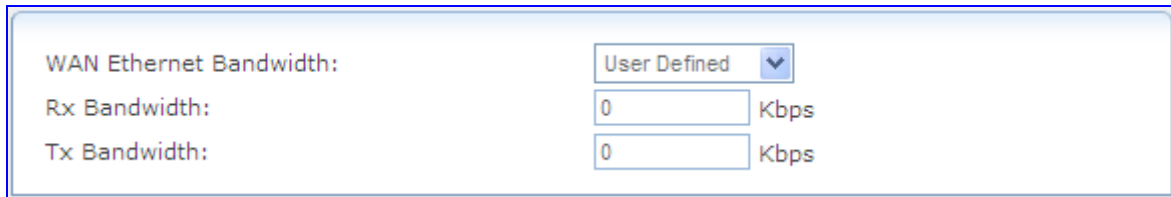
3.3.3.4.1 Configuring General QoS Settings

The **General QoS** item allows you to configure your WAN bandwidth.

➤ **To configure the device's WAN bandwidth:**

1. Click the **General QoS** item (**Configuration** tab > **Data** menu > **QoS** submenu > **General QoS**); the following page appears:

Figure 3-161: Configuring General WAN Bandwidth



2. From the 'WAN Devices Bandwidth (Rx/Tx)' drop-down list, select the required Rx/Tx bandwidth. If you do not see an appropriate entry, select 'User Defined', and then enter your Tx and Rx bandwidths in the fields below:
 - 'Rx Bandwidth': defines the device's Internet traffic receiving rate (in Kbps).
 - 'Tx Bandwidth': defines the device's outbound transmission rate (in Kbps).



Notes:

- For correct QoS performance, ensure that the bandwidth values are correct.
- For T1 WAN interface, the maximum Tx bandwidth per T1 physical link is 1.544 Mbps.

3.3.3.4.2 Configuring Matching Rules

Matching of packet rules allows you to manage and avoid traffic congestion by defining inbound and outbound priority rules for each element on your device. These rules determine the priority assigned to the packets traveling through the element. QoS parameters (DSCP marking and packet priority) are set per packet on an application basis. You can set QoS parameters using flexible rules, according to the following parameters:

- Source/destination IP address, MAC address or host name
- Device
- Source/destination ports
- Limit the rule for specific days and hours

The device supports two priority marking methods for packet prioritization:

- DSCP (see "Configuring DSCP Settings" on page 260).
- 802.1p Priority (see "Configuring 802.1p Settings" on page 262).

The matching of packets by rules is connection-based, known as Stateful Packet Inspection (SPI), using the same connection-tracking mechanism used by the device's firewall. Once a packet matches a rule, all subsequent packets with the same attributes receive the same QoS parameters, both inbound and outbound. A packet can match more than one rule. Therefore:

- The first class rule has precedence over all other class rules (scanning is stopped once the first rule is reached).
- The first traffic-priority (classless) rule has precedence over all other traffic-priority rules.
- There is no prevention of a traffic-priority rule conflicting with a class rule. In this case, the priority and DSCP setting of the class rule (if given) takes precedence.

Tx Traffic Shaping classes can be assigned to Matching Rules. These classes are defined in "Configuring Traffic Shaping" on page 256.

Connection-based QoS also allows inheriting QoS parameters by some of the applications that open subsequent connections. For instance, you can define QoS rules on SIP, and the rules also apply to both control and data ports (even if the data ports are unknown). This feature applies to all applications that have ALG in the firewall such as SIP, MSN Messenger/Windows Messenger, Port Triggering applications (see "Configuring Port Triggering" on page 244), PPTP, and IPSec.

➤ **To define matching-of-packet rules:**

1. Click the **Match Rules** item (**Configuration** tab > **Data** menu > **QoS** submenu > **Match Rules**); the following page appears:

Figure 3-162: Configuring Traffic Priority

QoS Input Rules						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
All Devices						
New Entry						+
WAN Ethernet Rules						
New Entry						+
LAN switch VLAN 4001 Rules						
New Entry						+
QoS Output Rules						
Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
All Devices						
New Entry						+
WAN Ethernet Rules						
New Entry						+
LAN switch VLAN 4001 Rules						
New Entry						+

This page is organized into two groups - 'QoS Input Rules' and 'QoS Output Rules' - for prioritizing inbound and outbound traffic, respectively. Each group lists all the devices on which rules can be set. You can set rules on all devices using the 'All Devices' group.

2. Click the **New Entry** link corresponding to the traffic direction (i.e., 'QoS Input Rules' or 'QoS Output Rules') and the device on which to set the rule; the following page appears:

Figure 3-163: Adding a Traffic Priority Rule

The screenshot shows a web-based configuration interface for adding a traffic priority rule. The interface is organized into four main sections: Matching, Operation, Logging, and Schedule. In the Matching section, there are three dropdown menus for Source Address, Destination Address, and Protocol, all currently set to 'Any'. Below these are checkboxes for 'Access List' (which is disabled with a red 'X' and the text 'No Access Lists Available'), 'DSCP', 'Priority', and 'Length'. The Operation section contains checkboxes for 'Set DSCP', 'Set Priority', and 'Set Tx Class Name', followed by a label 'Apply QoS on:' and a dropdown menu set to 'Connection'. The Logging section has a checkbox labeled 'Log Packets Matched by This Rule'. The Schedule section features a dropdown menu set to 'Always'.

3. Under the 'Matching' group, define characteristics of the packets matching the QoS rule:
 - **Source Address:** source address of packets sent or received by the device. The drop-down list allows you to specify a computer (address or a name) or group of computers on which you want to apply the rule. Select 'Any' to apply the rule to all the device's LAN hosts. To add a new address, select 'User Defined' and then add a new Network Object representing the new host (see "Configuring Network Objects" on page 284).
 - **Destination Address:** destination address of packets sent or received by the device. This address can be configured in the same manner as the source address.
 - **Protocol:** You may also specify a traffic protocol. Selecting the 'Show All Services' option from the drop-down lists expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option and then add a new Service representing the protocol (see "Configuring Protocols" on page 283).
 - **Access List:** Select this check box to display a drop-down list from which you can select an Access List group (defined in "Configuring the Access List" on page 249) to which the packets are assigned.
 - **DSCP:** Select this check box to display two DSCP fields, which enable you to specify a hexadecimal DSCP value and its mask assigned to the packets matching the priority rule.

- **Priority:** Select this check box to display a drop-down list from which you can select a priority level assigned to the packets matching the priority rule.
 - **Device:** Select this check box to display a drop-down list from which you can select a network device on which the packet-rule matching is performed.
 - **Length:** Select this check box if you want to specify the length of packets or the length of their data portion.
4. Under the 'Operation' group, define the following operation/s on packets that match the priority rule:
 - **Set DSCP:** Select this check box if you want to change the DSCP value (hexadecimal) on packets matching the rule, prior to routing them further.
 - **Set Priority:** Select this check box if you want to change a priority (where zero is the lowest and seven the highest) of the packets matching the rule. Each priority level is assigned a default queue number, where Queue 0 has the lowest priority. The device's QoS supports up to eight queues. The matching between a priority level and a queue number can be edited in the '802.1p Settings' page (see "Configuring 802.1p Settings" on page 262).
 - **Set Tx Class Name:** Select the check box and then from the drop-down list, select the defined Tx Class.
 - **Apply QoS on:** Select whether to apply QoS on a connection or just the first packet. When applying on a connection, the data transfer session is handled using Stateful Packet Inspection (SPI). This means that other packets matching this rule are automatically allowed to access, and the same QoS scheme is applied to them.
 5. Under the 'Logging' group, select the 'Log Packets Matched by This Rule' to log the first packet from a connection that was matched by this rule.
 6. From the 'Schedule' drop-down list, select the time during which the rule is active. By default, the rule is always active. However, you can configure scheduler rules by selecting 'User Defined', and then defining the day and time period during which the rule is active. Once a scheduler rule(s) is defined, the 'Schedule' drop-down list allows you to choose an available rule (for adding user-defined schedule rules, see "Configuring Scheduler Rules" on page 285).
 7. Click **OK** to save your changes.

The order of appearance of the rules represents both the order in which they were defined and the sequence by which they are applied. You may change this order, by using the

Move Up  and **Move Down**  icons.

3.3.3.4.3 Configuring Traffic Shaping

Traffic shaping allows you to define Tx (transmission) traffic classes for all the LAN and WAN interfaces. These traffic shaping classes can later be assigned to matching packet priority rules (defined in "Configuring Matching Rules" on page 253).

Traffic Shaping allows you to manage and avoid congestion where a high speed LAN meets limited broadband bandwidth. A user may have, for example, a 100 Mbps Ethernet LAN with a 100 Mbps WAN interface router. The router may communicate with the ISP using a modem with a bandwidth of 2 Mbps. This typical configuration makes the modem, having no QoS module, the bottleneck.

The router sends traffic as fast as it is received, while its well-designed QoS algorithms are left unused. Traffic shaping limits the bandwidth of the router, artificially forcing the router to be the bottleneck. A traffic shaper is essentially a regulated queue that accepts uneven and/or bursty flows of packets and transmits them in a steady, predictable stream so that the network is not overwhelmed with traffic. While Traffic Priority allows basic prioritization of packets, Traffic Shaping provides more sophisticated definitions, such as the following:

- Bandwidth limit for each device
- Bandwidth limit for classes of rules
- Prioritization policy
- TCP serialization on a device

The bandwidth of a device can be divided to reserve constant portions of bandwidth to predefined traffic types. Such a portion is known as a Traffic Class. When not used by its predefined traffic type, or owner (for example VoIP), the bandwidth is available to all other traffic. However when needed, the entire class is reserved solely for its owner. Moreover, you can limit the maximum bandwidth that a class can use even if the entire bandwidth is available. When a shaping class is first defined for a specific traffic type, two shaping classes are created. The second class is the 'Default Class', which is responsible for all the packets that do not match the defined shaping class, or any other classes that may be defined on the device.

➤ **To configure traffic shaping:**

1. Click the **Traffic Shaping** item (**Configuration** tab > **Data** menu > **QoS** submenu > **Traffic Shaping**); the following page appears:

Figure 3-164: Configuring Traffic Shaping

Device	Tx Bandwidth (Kbps)	Rx Bandwidth (Kbps)	TCP Serialization	Action
New Entry				

2. Click the **New Entry** link; the following page appears.

Figure 3-165: Adding Device for Traffic Shaping

Device:	<input type="text" value="Default WAN device"/>
---------	---

3. From the 'Device' drop-down list, select the device ('Default WAN Device' or 'Default LAN Device') for which you want to shape the traffic. If you want to apply the settings on all LAN devices, select the 'Default LAN Device'.

4. Click **OK**; the following page appears:

Figure 3-166: Defining Device Traffic Shaping

Device:	Default WAN device
Tx Traffic Shaping	
Tx Bandwidth:	Unlimited ▼
TCP Serialization:	Disabled ▼
Devices:	
Queue Policy:	Strict Priority ▼

5. From the 'Tx Bandwidth' drop-down list, select the device's bandwidth transmission rate limit. If you want to specify a TX bandwidth, see Step 8.
6. From the 'TCP Serialization' drop-down list, select whether TCP Serialization is enabled or disabled. You can enable TCP Serialization for active voice calls only or for all traffic. If you select 'Enable', the 'Maximum Delay' field appears for defining the maximal allowed transmission time frame (in milliseconds) of a single packet. Any packet that requires a longer transmission time is fragmented to smaller sections. This avoids transmission of large, bursty packets that may cause delay or jitter for real-time traffic such as VoIP. If you insert a delay value in milliseconds, the delay in number of bytes is automatically updated on refresh.
7. From the 'Queue Policy' drop-down list, select the Tx traffic queueing method. This can be based on a shaping class (Class Based) or on the pre-defined priority levels (Strict Priority). Note that when based on shaping class, the class's bandwidth requirements are met regardless of the priority, and only excess bandwidth is given to traffic with a higher priority. However, when unlimited bandwidth is selected for the Tx traffic, the queue policy can only be based on the pre-defined priority levels (i.e., Strict Priority).
8. If you want to specify a TX bandwidth, select 'Specify' from the 'Tx Bandwidth' drop-down list and then enter the maximum Tx bandwidth.
 - a. In the table, click the New **Entry** link; the following page appears:

Figure 3-167: Adding Tx Shaping Class

Name:	VoIP
-------	------

- b. In the 'Name' field, enter a new Tx traffic shaping class name (e.g., Class A), and then click **OK** to save the settings; the class is added to the table.

Figure 3-168: Class Name Added to Table

Device: Default WAN device

Tx Traffic Shaping

Tx Bandwidth: Specify Kbps

TCP Serialization: Disabled

Devices:

Queue Policy: Class Based

Queue ID	Name	Priority	Queue Size	Bandwidth		Status	Action
				Reserved	Maximum		
<input checked="" type="checkbox"/> 1	VoIP	0		0 Kbps	Unlimited	Active	
default	default	4		0 Kbps	Unlimited	Active	

[New Entry](#)

- c. Click the newly added class name; the following page appears:

Figure 3-169: Defining Shaping Class

Name: VoIP

Queue Priority: 0 (Highest)

Queue Size: Default

Bandwidth: Reserved 0 Maximum Unlimited Kbps

Policy: Priority

Schedule: Always

- d. Configure the following fields:
- ◆ **Name:** Name of the class.
 - ◆ **Queue Priority:** Priority level of the class (where zero is the highest and seven the lowest).
 - ◆ Queue Size:
 - ◆ **Bandwidth:** Reserved transmission bandwidth in kilobits per second. You can limit the maximum allowed bandwidth by selecting the 'Specify' option and then defining the Kbits/s.

- ◆ **Policy:** Class policy determines the policy of routing packets inside the class:
 - ✓ **Priority:** Priority queuing utilizes multiple queues, so that traffic is distributed among queues based on priority. This priority is defined according to packet's priority, which can be defined explicitly by a DSCP value or by a 802.1p value.
 - ✓ **FIFO:** The "First In, First Out" priority queue. This queue ignores any previously-marked priority that packets may have.
 - ✓ **Fairness:** The fairness algorithm ensures no starvation by granting all packets a certain level of priority.
 - ✓ **RED:** The Random Early Detection algorithm utilizes statistical methods to drop packets in a "probabilistic" way before queues overflow. Dropping packets slows a source down enough to keep the queue steady and reduces the number of packets that would be lost when a queue overflows and a host is transmitting at a high rate.
 - ✓ **WRR:** Weighted Round Robin utilizes a process scheduling function that prioritizes traffic according to the pre-defined 'Weight' parameter of a traffic's class. This level of prioritizing provides more flexibility in distributing bandwidth between traffic types, by defining additional classes within a parent class.
 - ◆ **Schedule:** By default, the class is always active. However, you can configure scheduler rules to define time segments during which the class may be active.
- e. Click **OK**.
9. Click **OK**.

3.3.3.4.4 Configuring DSCP Settings

The **DSCP Settings** item defines Differentiated Services Code Point (DSCP). Differentiated Services (Diffserv) is a Class of Service (CoS) model that enhances best-effort Internet services by differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, as appropriate for voice calls, video playback or other delay-sensitive applications, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.




































Diffserv defines a field in IP packet headers referred to as DSCP. Hosts or routers passing traffic to a Diffserv-enabled networks typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handling or scheduling behavior.

The device provides a table of predefined DSCP values, which are mapped to 802.1p priority marking method. You can edit or delete any of the existing DSCP settings, as well as add new entries. Each DSCP value is assigned a default queue number as a part of its 802.1p priority settings. The device's QoS supports up to eight queues, where Queue 0 has the lowest priority.

➤ **To add, edit or delete DSCP settings:**

1. Click the **DSCP Settings** item (**Configuration** tab > **Data** menu > **QoS** submenu > **DSCP Settings**); the following page appears:

Figure 3-170: Configuring DSCP Settings

DSCP Value (hex)	802.1p Priority	Action
0x0	0 (Queue 0 - Low)	 
0x2	0 (Queue 0 - Low)	 
0x4	4 (Queue 1 - Medium)	 
0x6	4 (Queue 1 - Medium)	 
0x8	2 (Queue 0 - Low)	 
0xA	1 (Queue 0 - Low)	 
0xC	3 (Queue 0 - Low)	 
0xE	2 (Queue 0 - Low)	 
0x10	7 (Queue 2 - High)	 
0x12	6 (Queue 2 - High)	 
0x14	7 (Queue 2 - High)	 
0x16	6 (Queue 2 - High)	 
0x18	5 (Queue 1 - Medium)	 
0x1A	5 (Queue 1 - Medium)	 
0x1C	5 (Queue 1 - Medium)	 
0x1E	5 (Queue 1 - Medium)	 
0x2E	7 (Queue 2 - High)	 
New Entry		



2. To edit an existing entry, click the corresponding **Edit**  icon. To add a new entry, click the **New Entry** link. In both cases, the following page appears.

Figure 3-171: Defining DSCP to 802.1p Priority Mapping

DSCP Value (hex):	<input type="text"/>
802.1p Priority:	0 (Queue 0 - Low) 

3. In the 'DSCP Value (hex)' field, enter a hexadecimal number for the DSCP value.
4. From the '802.1p Priority' drop-down list, select an 802.1p priority level (each priority level is mapped to low/medium/high priority).
5. Click **OK** to save the settings.



Note: The DSCP value overriding the priority of incoming packets with an unassigned value (priority 0, assumed to be a no-priority-set) is "0x0".

3.3.3.4.5 Configuring 802.1p Settings

The IEEE 802.1p priority marking method is a standard for prioritizing network traffic at the data link/Mac sub-layer. 802.1p traffic is simply classified and sent to the destination, with no bandwidth reservations established. The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest. In addition, the device maps these eight levels to priority queues, where Queue 0 has the lowest priority. The device's QoS supports up to eight queues. By default, the higher the level and queue values, the higher priority they receive. Therefore, the more critical the traffic, the higher priority level and queue number it should receive.

➤ To change the mapping between a priority value and a queue value:

1. Click the **802.1p Settings** item (**Configuration** tab > **Data** menu > **QoS** submenu > **802.1p Settings**); the following page appears:

Figure 3-172: Configuring 802.1p Settings

802.1p Value	Queue
0	Queue 0 - Low
1	Queue 0 - Low
2	Queue 0 - Low
3	Queue 0 - Low
4	Queue 1 - Medium
5	Queue 1 - Medium
6	Queue 2 - High
7	Queue 2 - High

2. From the corresponding drop-down list, select the desired level.
3. Click **OK**.

3.3.3.5 VPN

The **VPN** menu allows you to configure Virtual Private Networking (VPN) over the Internet, and includes the following items:

- **IPSec** (see "Configuring IPSec" on page 262)
- **PPTP** (see "Configuring PPTP Server" on page 265)
- **L2TP** (see "Configuring L2TP Server" on page 266)

3.3.3.5.1 Configuring IPSec

Internet Protocol Security (IPSec) is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks. The IPSec protocols include:

- **AH** (Authentication Header) provides packet-level authentication.
- **ESP** (Encapsulating Security Payload) provides encryption and authentication.
- **IKE** (Internet Key Exchange) negotiates connection parameters, including keys for the other two services.

Services supported by the IPSec protocols (AH, ESP) include confidentiality (encryption), authenticity (proof of sender), integrity (detection of data tampering), and replay protection (defense against unauthorized resending of data). IPSec also specifies methodologies for key management. Internet Key Exchange (IKE), the IPSec key management protocol, defines a series of steps to establish keys for encrypting and decrypting information; it defines a common language on which communications between two parties is based. Developed by the Internet Engineering Task Force (IETF), IPSec and IKE together standardize the way data protection is performed, thus making it possible for security systems developed by different vendors to interoperate.

➤ **To configure IPSec:**

1. Click the **IPSec** item (**Configuration** tab > **Data** menu > **VPN** submenu > **IPSec**); the following page appears:

Figure 3-173: Configuring VPN IPSec

The screenshot shows the IPSec configuration interface. It has three main sections: 'Block Unauthorized IP', 'Anti-Replay Protection', and 'Connections'. The 'Block Unauthorized IP' section has a checkbox labeled 'Enabled' which is checked, and two input fields: 'Maximum Number of Authentication Failures' with the value '5' and 'Block Period (in seconds):' with the value '60'. The 'Anti-Replay Protection' section also has a checked 'Enabled' checkbox. The 'Connections' section is a table with three columns: 'Name', 'Status', and 'Action'.

Name	Status	Action
------	--------	--------

The 'Connections' group displays a list of IPSec connections (to create an IPSec connection, see "Configuring Network Connections" on page 287).

2. To block unauthorized IP to the device, perform the following:
 - a. Select the 'Block Unauthorized IP' check box.
 - b. In the 'Maximum Number of Authentication Failures' field, enter the maximum number of packets to authenticate before blocking the origin's IP address.
 - c. In the 'Block Period' field, enter the time frame during which the device drops packets from an unauthorized IP address.
3. To enable dropping of packets that are recognized (by their sequence number) as already been received, select the 'Anti-Replay Protection' check box.
4. Configure the device's IPSec public keys:
 - a. Click the **Settings** button; the following page appears.

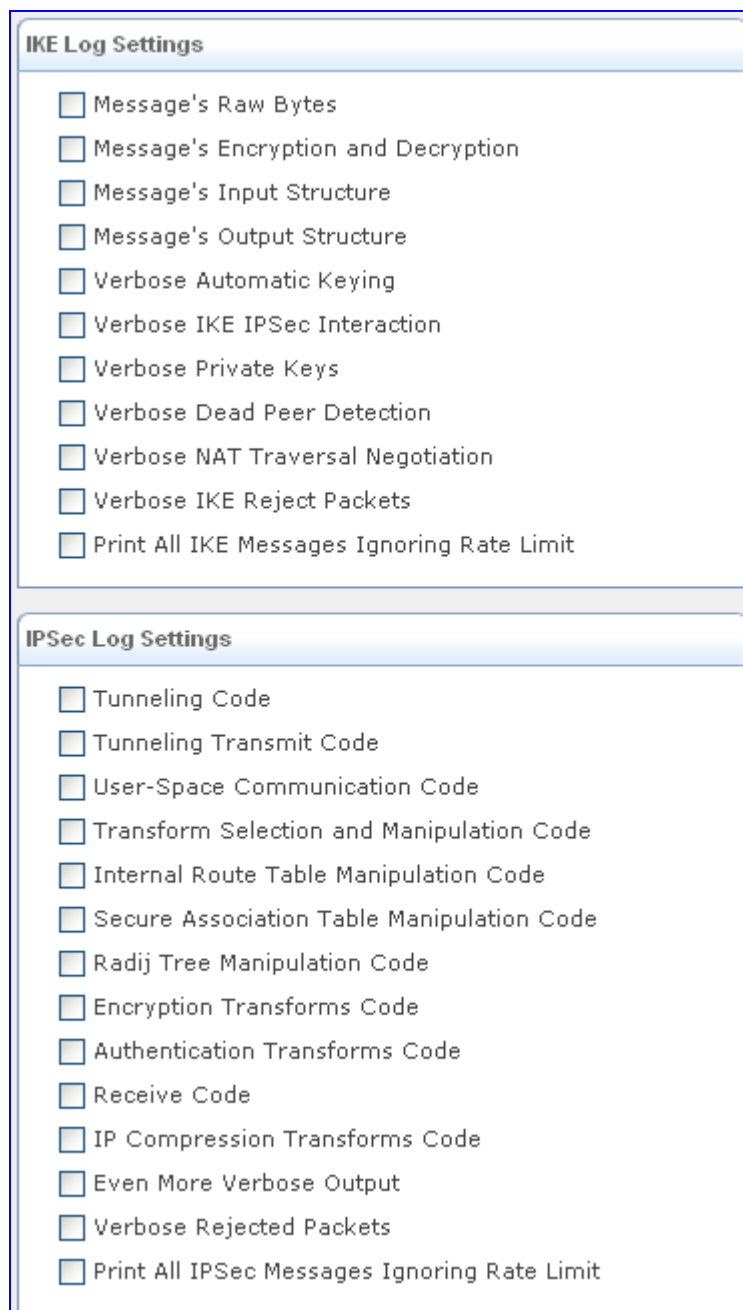
Figure 3-174: Recreating IPSec Public Key

The screenshot shows the 'Recreating IPSec Public Key' page. It has a label 'Public Key:' and a 'Recreate Key' button. Below the label is a text area containing a long string of hexadecimal characters. The text area has a vertical scrollbar on the right side.

```
01 03 6e dc ed e0 ce 04 1f 43 8f 89 71 5a 9b 21 cf
24 b3 85 c1 8c 18 a7 e2 90 4e 31 0c e8 24 a9 6b
8d 9b 82 69 23 03 e7 51 37 7b e0 68 2f 5a 26 a4
cd ff c6 7f ce 83 12 7c 51 c8 83 56 78 a8 a9 15 34
8b 0a 1e eb 62 4a 5a 16 bc 74 67 82 42 6a 37 f5
6b dd 9a 7b ae 56 bc 66 13 15 6c e9 08 8f d9 13
05 8b d4 f3 7c a1 8d 40 29 d2 69 87 8f 47 a3 05
```

- b. Click the **Recreate Key** button to recreate the public key, or the **Refresh** button to refresh the displayed key.
 - c. Click **Close**; you are returned to the previous page.
5. Configure the IPSec log display for identifying and analyzing the history of the IPSec package commands, attempts to create connections, etc:
 - a. Click the **Log Settings** button; the following page appears.

Figure 3-175: IPSec Log Settings



IKE Log Settings

- ☐ Message's Raw Bytes
- ☐ Message's Encryption and Decryption
- ☐ Message's Input Structure
- ☐ Message's Output Structure
- ☐ Verbose Automatic Keying
- ☐ Verbose IKE IPSec Interaction
- ☐ Verbose Private Keys
- ☐ Verbose Dead Peer Detection
- ☐ Verbose NAT Traversal Negotiation
- ☐ Verbose IKE Reject Packets
- ☐ Print All IKE Messages Ignoring Rate Limit

IPSec Log Settings

- ☐ Tunneling Code
- ☐ Tunneling Transmit Code
- ☐ User-Space Communication Code
- ☐ Transform Selection and Manipulation Code
- ☐ Internal Route Table Manipulation Code
- ☐ Secure Association Table Manipulation Code
- ☐ Radj Tree Manipulation Code
- ☐ Encryption Transforms Code
- ☐ Authentication Transforms Code
- ☐ Receive Code
- ☐ IP Compression Transforms Code
- ☐ Even More Verbose Output
- ☐ Verbose Rejected Packets
- ☐ Print All IPSec Messages Ignoring Rate Limit

- b. Select the check boxes relevant to the information you want the IPSec log to record.
 - c. Click **OK** to save the settings.

3.3.3.5.2 Configuring PPTP Server

The device can act as a Point-to-Point Tunneling Protocol Server (PPTP Server), accepting PPTP client connection requests.

➤ **To configure PPTP:**

1. Click the **PPTP** item (**Configuration** tab > **Data** menu > **VPN** submenu > **PPTP**); the following page appears:

Figure 3-176: Configuring VPN PPTP Server

Server			
<input type="checkbox"/> Enabled Click here to create VPN users			
Remote Address Range			
Start IP Address:	192	.168	.0.245
End IP Address:	192	.168	.0.254
Connections			
Name	Status	Action	

2. Under the 'Server' group, perform the following:
 - a. Select the 'Enabled' check box to enable the PPTP feature. Note that checking this box creates a PPTP server, but does not define remote users.
 - b. Click the **Click here to create VPN users** link to define remote users that are granted access to your home network (see "Creating VPN Users" on page 267).
 - c. Click the **Advanced** button to display additional parameters and configure the following:
 - ◆ In the 'Max Idle Time to Disconnect in Seconds' field, specify the amount of idle time (during which no data is sent or received) that should elapse before the device disconnects a PPTP connection.
 - ◆ Select the 'Authentication Required' check box to enable PPTP to use authentication, and then select the algorithms the server may use when authenticating its clients.
 - ◆ Select the 'Encryption Required' check box to enable PPTP to use encryption, and then select the algorithms the server may use when encrypting data.
 - ◆ From the 'MPPE Encryption Mode' drop-down list, select the Microsoft Point-to-Point Encryption mode.
3. Under the 'Remote Address Range' group, in the 'Start IP Address' and 'End IP Address' fields, specify the range of IP addresses that are granted by the PPTP server to the PPTP client.



Note: The server settings must be compatible with the client settings, described in "Configuring Network Connections" on page 287.

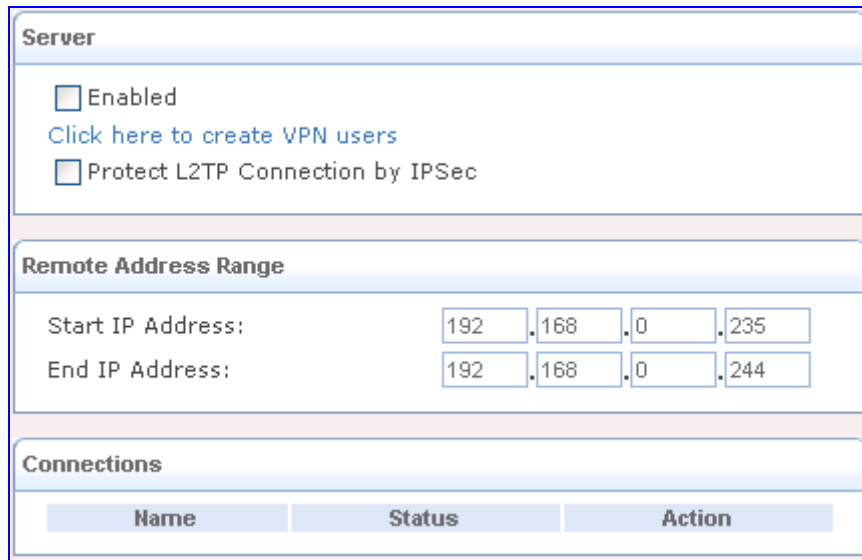
3.3.3.5.3 Configuring L2TP Server

The device can act as a Layer 2 Tunneling Protocol Server (L2TP Server), accepting L2TP client connection requests.

➤ **To configure L2PT:**

1. Click the **L2TP** item (**Configuration** tab > **Data** menu > **VPN** submenu > **L2TP**); the following page appears:

Figure 3-177: Configuring VPN L2TP Server



Server			
<input type="checkbox"/> Enabled			
Click here to create VPN users			
<input type="checkbox"/> Protect L2TP Connection by IPSec			
Remote Address Range			
Start IP Address:	192	168	0.235
End IP Address:	192	168	0.244
Connections			
Name	Status	Action	

2. Under the 'Server' group, perform the following:
 - a. Select the 'Enabled' check box to enable the L2TP feature. Note that checking this box creates a L2TP server (if not yet created with the wizard), but does not define remote users.
 - b. Click the **Click here to create VPN users** link to define remote users that are granted access to your home network (see "Creating VPN Users" on page 267).
 - c. Select the 'Protect L2TP Connection by IPSec' to secure the L2TP connection by the IP Security (IPSec) protocol. When enabled, the following entry appears:
 - ◆ **Create Default IPSec Connection:** When creating an L2TP Server with the connection wizard, a default IPSec connection is created to protect it. If you wish to disable this feature, clear this option. However, if L2TP protection is enabled by IPSec (see previous entry), you must provide an alternative, active IPSec connection for users to be able to connect. When this feature is enabled, the following entry appears.
 - ✓ **L2TP Server IPSec Shared Secret:** change the IPSec shared secret provided when the connection was created.
 - d. Click the **Advanced** button, and then configure the following:
 - ◆ In the 'Max Idle Time to Disconnect in Seconds' field, specify the amount of idle time (during which no data is sent or received) that should elapse before the device disconnects an L2TP connection.
 - ◆ Select the 'Authentication Required' check box to enable L2TP to use authentication, and then select the algorithms the server may use when authenticating its clients.
 - ◆ Select the 'Encryption Required' check box to enable L2TP to use encryption and then select the algorithms the server may use when encrypting data.

- ◆ From the 'MPPE Encryption Mode' drop-down list, select the Microsoft Point-to-Point Encryption mode: Stateless or Stateful.
3. Under the 'Remote Address Range' group, in the 'Start IP Address' and 'End IP Address' fields, specify the range of IP addresses that are granted by the L2TP server to the L2TP client.



Note: The server settings must be compatible with the client settings, described in "Configuring Network Connections" on page 287.

3.3.3.5.4 Creating VPN Users

The procedure below describes how to add users and user groups, after clicking the **Click here to create VPN users** link when configuring a PPTP server and L2TP server (see "Configuring PPTP Server" on page 265 and "Configuring L2TP Server" on page 266 respectively). You can also group users according to your preferences. The "Administrator" user is the pre-defined default user.

➤ To add a user:

1. After clicking the **Click here to create VPN users** link, the following page appears:

Figure 3-178: Adding Users

Users			
Full Name	User Name	Permissions	Action
Administrator	admin		
New User			

Groups			
Name	Description	Members	Action
Users			
New Group			

2. Under the 'Users' group, click the **New User** link; the following page appears:

Figure 3-179: Adding a New User

General

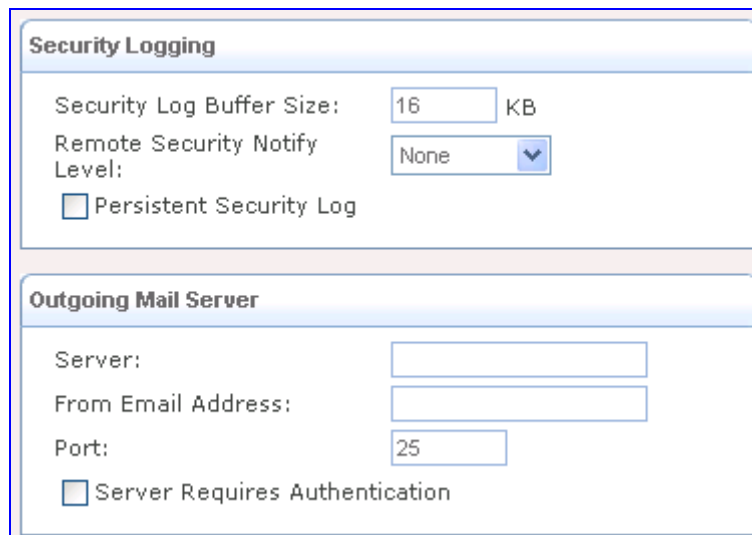
Full Name:
 User Name:
 New Password (case sensitive):
 Retype New Password:
 Permissions: ☐ Remote Access by VPN

E-Mail Notification

[Click here to configure notification Mail Server](#)
 Notification Address:
 System Notify Level: None
 Security Notify Level: None

3. Under the 'General' group, configure the following parameters:
 - a. **Full Name:** remote user's full name.
 - b. **User Name:** name that a user uses to access your network.
 - c. **New Password:** user's password.
 - d. **Retype New Password:** if a new password is assigned, type it again to verify its correctness.
 - e. **Primary Group:** this check box only appears after a user is defined, enabling you to assign the user to a primary group.
 - f. **Permissions:** select the 'Remote Access by VPN' check box to grant remote access to the device using the VPN protocol.
4. Under the 'E-Mail Notification' group, you can use e-mail notification to receive indications of system events for a predefined severity classification. The available types of events are 'System' or 'Security' events. The available severity of events are 'Error', 'Warning', 'Information', and 'Debug'. If the 'Information' level is selected, the user receives notification of the 'Information', 'Warning' and 'Error' events. If the 'Warning' level is selected, the user receives notification of the 'Warning' and 'Error' events, and so on.
 - a. Ensure that you have configured an outgoing mail server. Click the **Click here to configure notification Mail Server** link to configure the outgoing mail server (see Step 5).
 - b. Notification Address: user's e-mail address.
 - c. Select the 'System' and 'Security' notification levels in the 'System Notify Level' and 'Security Notify Level' drop-down lists respectively.
5. Configure an outgoing mail server:

Figure 3-180: Defining Outgoing Mail Server



The screenshot shows two configuration panels. The top panel, titled 'Security Logging', contains the following settings: 'Security Log Buffer Size' is set to 16 KB; 'Remote Security Notify Level' is set to None; and the 'Persistent Security Log' checkbox is unchecked. The bottom panel, titled 'Outgoing Mail Server', contains the following settings: 'Server' is an empty text field; 'From Email Address' is an empty text field; 'Port' is set to 25; and the 'Server Requires Authentication' checkbox is unchecked.

- a. **Server:** enter the hostname of your outgoing (SMTP) server.
- b. **From Email Address:** each email requires a 'from' address and some outgoing servers refuse to forward mail without a valid 'from' address for anti-spam considerations.
- c. **Port:** enter the port that is used by your outgoing mail server.
- d. **Server Requires Authentication:** if your outgoing mail server requires authentication, select this check box and enter your user name and password in the 'User Name' and 'Password' fields respectively.

6. Under the 'Security Logging' group, configure the following parameters:
 - **Security Log Buffer Size:** size of the security log buffer in Kilobytes.
 - **Remote Security Notify Level:** remote security notification level - None, Error, Warning, and Information.
 - **Persistent Security Log:** select this check box to save the security log to the flash memory.
7. Click **OK** to save your settings.

You can assemble your defined users into different groups, based on different criteria, for example, home users versus office users. By default, new users are added to the default group "Users".

➤ **To add a user group:**

1. After clicking the **Click here to create VPN users** link, the following page appears:

Figure 3-181: Adding Users

Users			
Full Name	User Name	Permissions	Action
Administrator	admin		
New User			

Groups			
Name	Description	Members	Action
Users			
New Group			

2. Under the 'Groups' section, click the **New Group** link; the following page appears:

Figure 3-182: Adding a User Group

Name:

Description:

Group Members

☐ Administrator

☐ Susan

3. In the 'Name' field, enter a name for the group.
4. In the 'Description' field, enter a short description for the group (optional).
5. Under the Group Members section, select the users that you want to assign to this group. A user can belong to more than one group.
6. Click **OK** to save your settings.

3.3.3.6 Data Services

The **Data Services** submenu allows you to configure various services (applications), and includes the following menus:

- **DDNS** (see "Configuring DDNS" on page 270)
- **DNS Server** (see "Configuring DNS Server" on page 271)
- **DHCP Server** (see "Configuring DHCP Server" on page 272)

3.3.3.6.1 Configuring DDNS

The Dynamic DNS (DDNS) service enables you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessible from various locations on the Internet. Typically, when you connect to the Internet, your service provider assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, whilst maintaining a constant domain name. When using the DDNS service, each time the IP address provided by your ISP changes, the DNS database changes accordingly to reflect the change. In this way, even though your IP address changes often, your domain name remains constant and accessible.


To use the DDNS feature, you must first obtain a DDNS account. For example, you can open a free account at <http://www.dyndns.com/account/create.html>. When applying for an account, you will need to specify a user name and password.

Use the DDNS feature to define different static host names for each of your WAN connections. Moreover, you can define more than one static host name for each WAN connection, by simply repeating the following procedure for the same connection.

➤ To create a dynamic DNS:

1. Click the **DDNS** item (**Configuration** tab > **Data** menu > **Data Services** submenu > **DDNS**); the following page appears:

Figure 3-183: Configuring Dynamic DNS (DDNS) Services

Host Name	Status	Provider	User Name	Action
New Dynamic DNS Entry				

2. Click the **New Dynamic DNS Entry** link to add a new DDNS entry; the following page appears:

Figure 3-184: Adding a DDNS

Host Name:	<input type="text"/>
Connection:	WAN Ethernet ▼
Provider:	dyndns.org ▼
Click here to initiate and manage your subscription	
User Name:	<input type="text"/>
Password:	<input type="password"/>
<input type="checkbox"/> Wildcard	
Mail Exchanger:	<input type="text"/>
<input type="checkbox"/> Backup MX	
<input type="checkbox"/> Offline	
SSL Mode:	None ▼

3. In the 'Host Name' field, enter your full DDNS domain name.
4. From the 'Connection' field, select the connection to which you want to couple the DDNS service. The DDNS service only uses the selected device, unless failover is enabled. In this case, the failed-to device is used instead (assuming its route rules consent), until the selected device is up again.
5. From the 'Provider', select your DDNS service provider; the page displays parameters required by the selected provider. To open the selected provider's account creation Web page, click the link **Click here to initiate and manage your subscription**.
6. The parameters described below are available if you select the provider dyndns (in Step 5), which includes all available parameters.
 - **User Name:** enter your DDNS user name.
 - **Password:** enter your DDNS password.
 - **Wildcard:** select this check box to enable use of special links such as `http://www.<your host>.dyndns.com`.
 - **Mail Exchanger:** enter your mail exchange server address to redirect all e-mails arriving at your DDNS address to your mail server.
 - **Backup MX:** select this check box to designate the mail exchange server to be a backup server.
 - **Offline:** if you wish to temporarily take your site offline (prevent traffic from reaching your DDNS domain name), check this box to enable redirection of DNS requests to an alternative URL, predefined in your DDNS account. The availability of this feature depends on your account's level and type of service.
 - **SSL Mode:** secured DDNS services are accessed using HTTPS. Upon connection, the device validates the DDNS server's certificate. Use this entry to choose the certificate's validation method.
 - ◆ **None:** do not validate the server's certificate.
 - ◆ **Chain:** validate the entire certificate chain. If you select this option, the 'Validate Time' drop-down lists appears to validate the certificate's expiration time. If the certificate has expired, the connection terminates immediately.
 - ◆ **Direct:** ensures that the server's certificate is directly signed by the root certificate. If selected, the 'Validate Time' drop-down lists appears for validation of the certificate's expiration time, as described above.
7. Click **OK**.

3.3.3.6.2 Configuring DNS Server

Domain Name System (DNS) provides a service that translates domain names into IP addresses and vice versa. The device's DNS server is an auto-learning DNS, which means that when a new computer is connected to the network the DNS server learns its name and automatically adds it to the DNS table. Other network users may immediately communicate with this computer using either its name or its IP address. In addition, your device's DNS:

- Shares a common database of domain names and IP addresses with the DHCP server
- Supports multiple subnets within the LAN simultaneously
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database (using the Web interface)










- Permits a computer to have multiple host names
- Permits a host name to have multiple IPs (needed if a host has multiple network cards)

The DNS server does not require configuration. However, you may wish to view the list of computers known by the DNS, edit the host name or IP address of a computer on the list, or manually add a new computer to the list.

➤ **To create a DNS entry:**

1. Click the **DNS Server** item (**Configuration** tab > **Data** menu > **Data Services** submenu > **DNS Server**); the following page appears:

Figure 3-185: Configuring a DNS Server

Host Name	IP Address	Source	Action
voice_entity	192.168.0.2	DHCP	 
itamari-ailogix	192.168.0.3	DHCP	 
ACL_686945	192.168.0.6	DHCP	 
voice_entity	192.168.2.2	DHCP	 
New DNS Entry			

2. Click the **New DNS Entry** link; the following page appears:

Figure 3-186: Adding a DNS Server

Host Name:	<input type="text" value="new-host"/>
IP Address:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

3. In the 'Home Name' field, enter the computer's host name.
4. In the 'IP Address' field, enter the computer's IP address.
5. Click **OK** to save the settings.

3.3.3.6.3 Configuring DHCP Server

Your device's Dynamic Host Configuration Protocol (DHCP) server makes it possible to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to such hosts. The device's default DHCP server is the LAN bridge. A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as 'taken'. At this point the host is configured with an IP address for the duration of the lease. The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease then it also receives current information about network services, as it did with the original lease, allowing it to update its network configurations to reflect any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration it can send a release message to the DHCP server, which then makes the IP address available for use by others.



Note: By default, the device's DHCP server is enabled. Therefore, when connecting the device to your enterprise's LAN, the device responds to DHCP requests and consequently distributes IP addresses (instead of your Enterprise's DHCP server, if exists).

Your device's DHCP server:

- Displays a list of all DHCP host devices connected to the device
- Defines the range of IP addresses that can be allocated in the LAN
- Defines the length of time for which dynamic IP addresses are allocated
- Provides the above configurations for each LAN device and can be configured and enabled/disabled separately for each LAN device
- Can assign a static lease to a LAN PC so that it receives the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computers
- Provides the DNS server with the host name and IP address of each PC that is connected to the LAN

The device can also act as a DHCP relay, escalating DHCP responsibilities to a WAN DHCP server. In this case, the device acts merely as a router, while its LAN hosts receive their IP addresses from a DHCP server on the WAN. With the device's optional Zero Configuration Technology feature, the IP Auto Detection method detects statically-defined IP addresses in addition to the device's DHCP clients. It learns all the IP addresses on the LAN, and integrates the collected information with the database of the DHCP server. This allows the DHCP server to issue valid leases, thus avoiding conflicting IP addresses used by other computers in the network.

➤ **To configure DHCP:**

1. Click the **DHCP Server** item (**Configuration** tab > **Data** menu > **Data Services** submenu > **DHCP Server**); the following page appears:

Figure 3-187: Configuring DHCP Server

Name	Service	Subnet Mask	Dynamic IP Range	Action
WAN Ethernet	Disabled			
LAN switch VLAN 1	DHCP Server	255.255.255.0	192.168.0.3 - 192.168.0.8	

The page displays a summary of the services currently being provided by the DHCP server.



Note: If a device is listed as "Disabled" in the 'Service' column, then DHCP services are not being provided to hosts connected to the network through that device. This means that the device does not assign IP addresses to these computers, which is useful if you wish to work with static IP addresses only.


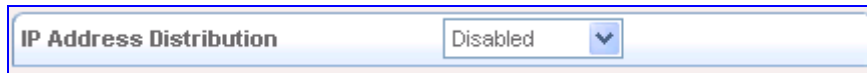
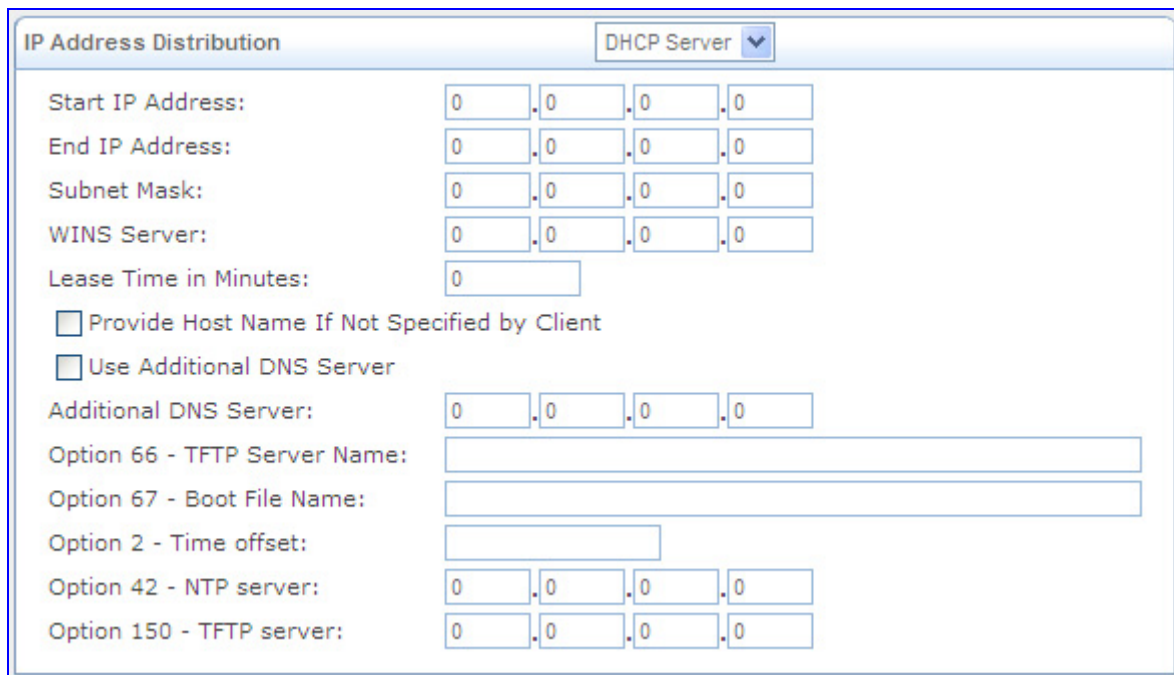
2. Click the **Edit**  icon corresponding to the required interface; the following page appears:

Figure 3-188: Defining IP Distribution Type



3. From the 'IP Address Distribution' drop-down list, choose either 'DHCP Server', 'DHCP Relay' (or 'Disabled' if you want to disable DHCP).
4. If you selected 'DHCP Server', the following fields appear:

Figure 3-189: Defining DHCP Server Parameters



- a. **Start IP Address:** First IP address that can be assigned to a LAN host. Since the device's default IP address is 192.168.1.1, this address must be 192.168.1.2 or greater.
- b. **End IP Address:** Last IP address in the range that can be used to automatically assign IP addresses to LAN hosts.
- c. **Subnet Mask:** Mask used to determine to what subnet an IP address belongs (e.g., 255.255.0.0).
- d. **WINS Server:** The Windows Internet Naming Service (WINS) Server IP address that is given in a lease.
- e. **Lease Time In Minutes:** Each LAN host is assigned an IP address by the DHCP server for a this amount of time, when it connects to the network. When the lease expires, the server determines if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use become available for other computers on the network.
- f. **Provide Host Name If Not Specified by Client:** If the DHCP client does not have a host name, the device automatically assigns one.
- g. **Use Additional DNS Server:** The additional DNS server address allows the network administrator to provision the DHCP clients with another DNS server (other than the device itself).

- h. **Option 66 - TFTP Server Name:** This option is used to identify a TFTP server.
 - i. **Option 67 - Boot File Name:** This option is used to identify the boot file name.
 - j. **Option 2 - Time offset:** Specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC). The offset is expressed as a two's complement 32-bit integer. A positive offset indicates a location east of the zero meridian and a negative offset indicates a location west of the zero meridian. The code for the time offset option is 2, and its length is 4 octets.
 - k. **Option 42 - NTP server:** Network Time Protocol (NTP) Servers option specifies a list of IP addresses indicating NTP servers available to the client. Servers should be listed in order of preference. The code for this option is 42. Its minimum length is 4, and the length must be a multiple of 4.
 - l. **Option 150 - TFTP server:** DHCP option (RFC 2132) contains one or more IPv4 addresses that the client may use. The current use of this option is for downloading configuration from a VoIP server via TFTP; however, the option may be used for purposes other than contacting a VoIP configuration server.
 - m. Click **OK** to save the settings.
5. If you selected 'DHCP Relay', the following appears:

Figure 3-190: Defining DHCP Relay (DHCP for LAN Bridge)

Address	Action
New IP Address	

- a. Click the **New IP Address** link; the following page appears:

Figure 3-191: Defining DHCP Server's IP Address

IP Address: . . .










- b. In the 'IP Address' field, enter the IP address of the DHCP server.
- c. Click **OK** to save the settings, and then click **OK** again.
- d. You now need to configure the WAN to operate in routing mode, which is necessary for DHCP relay:
 - a. Click the **Connections** item (**Configuration** tab > **Data Settings** menu > **Data System** > **Connections**).
 - b. Click the **Edit** icon corresponding to the 'WAN Ethernet' connection.
 - c. Select the **Routing** tab and then from the 'Routing Mode' drop-down list, select 'Route'.
 - d. Click **OK** to save the settings.

You can also view a list of computers currently recognized by the DHCP server:

- To view a list of computers currently recognized by the DHCP server and to add a new computer with a static IP address:

1. Click the **DHCP Server** item (**Configuration** tab > **Data Settings** menu > **Services** > **DHCP Server**).
2. Click the **Connection List** button located at the bottom of the page; the following page appears.

Figure 3-192: Computers Recognized by DHCP Server

Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
voice entity	192.168.0.2	00:90:8f:1b:33:7b	Detected	LAN switch VLAN 1	Active	60 Minutes	 
itamarl-ailogix	192.168.0.3	00:16:35:63:df:9c	Static	LAN switch VLAN 1	Active	49 Minutes	 
ACL_686945	192.168.0.6	00:90:8f:0a:7b:61	Static	LAN switch VLAN 1	Active	41 Minutes	 
voice entity	192.168.2.2	00:90:8f:1b:33:7b	Detected	LAN switch VLAN 1	Expired		 
New Static Connection 							

3. To define a new connection with a fixed IP address, click the **New Static Connection** link; the following page appears:

Figure 3-193: Defining New Static Connection (IP Address)

Host Name:

IP Address: . . .

MAC Address: : : : : :

4. Enter a host name for this connection.
5. Enter the fixed IP address that you would like to have assigned to the computer.
6. Enter the MAC address of the computer's network card.



Note: A device's fixed IP address is actually assigned to the specific network card's (NIC) MAC address installed on the LAN computer. If you replace this network card then you must update the device's entry in the DHCP Connections list with the new network card's MAC address.

7. Click **OK** to save the settings.

3.3.3.7 Data Routing

The **Data Routing** submenu allows you to configure the device's routing rules, and includes the following items:

- **General Routing** (see "Configuring General Routing Settings" on page 277)
- **BGP & OSPF** (see "Configuring BGP and OSPF" on page 281)

3.3.3.7.1 Configuring General Routing

You can choose to setup your device to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to destinations. The **Data Routing** item allows you to add, edit and delete routing rules from the routing table.

This page also allows you to add or edit the device's default route devices by changing their metric value.

The device supports platforms with multiple physical WAN devices (ports), which can be used for traffic load balancing, failover, and various routing policies. The multiple WAN features may also be used to define multiple logical devices (e.g. PPTP VPN, PPPoE) on device's with a single WAN port.

- **Load balancing:** traffic load (bandwidth) is distributed between two WAN interfaces. Load balancing uses the IP pairs technique, in which traffic between a pair of source and destination IP addresses is routed to the same WAN device for a certain time frame. A router load balancing on a per-destination basis uses the parallel routes in a round-robin fashion, and forwards an entire destination-based flow in each pass.
- **DSCP-based policy routing:** you may specify that traffic matching a certain DSCP value is routed to a specific device. This is useful for routing different types of data to different WAN devices. It is also useful if you want to segregate the voice traffic from the data traffic over two lower-cost broadband circuits in an effort to have better voice quality.
- **Failover:** traffic is routed to an active WAN device in case its current WAN device fails, ensuring connectivity. This transfer of traffic is done regardless of DSCP-based policy routing rules. An example scenario is Inbound Failover where if a connection fails and its IP is no longer accessible, the device notifies the other party to use a different IP, using Dynamic DNS. The device supports the following types of failover:
 - Full Link Redundancy: two or more active WAN devices, usually with equal speed must be configured. A device set as the default gateway functions as the main device, while the other one(s) work in the backup mode. This means that if one of the devices fails, the next one take its place. In this configuration, the devices can also work in conjunction with the Load Balancing feature to enhance the WAN throughput.
 - Rollover Connection: during uptime, a rollover device is kept inactive. This is usually a slow link, for example, a dialup. When all other failover devices lose connectivity, the rollover device becomes active automatically, and may keep the same IP as the main device. This allows the use of a slow connection as a backup to the main fast connection. When a failover device regains connectivity, the rollover device becomes inactive again. Note that if dialup is done by demand, activating the backup device may take a noticeable amount of time. The failover process consists of three phases:
 - a. Detection – performed using a DNS test.
 - b. Action – when a DNS test fails, the failover process simply removes the route records of the failed connection. This enables you to reach the desired failover behavior by configuring the device's routing rules correctly.
 - c. Recover – during failover, tests continue to run on the failed connection. When a test succeeds, the connection recovers its route records.



Notes:

- Only default route devices can participate in load balancing.
- DSCP-based policy routing takes precedence over load balancing. If most of the traffic falls under the DSCP-based policy routing rules, it is then forwarded accordingly, regardless of the load balancing. Load balancing, in this case, is by best-effort load balancing, and balances the remaining traffic not directed by the DSCP-based policy routing rules.

➤ **To configure general routes:**

1. Click the **General Routing** item (**Configuration** tab > **Data** menu > **Data Routing** submenu > **General Routing**); the following page appears:

Figure 3-194: Configuring General Routing

Name	Destination	Gateway	Netmask	Metric	Status	Action
<div> <div>New Route</div> <div>+</div> </div>						
Routing Information Protocol (RIP) <input type="checkbox"/> Enabled						
<input type="checkbox"/> Poison Reverse <input type="checkbox"/> Do not Advertise Direct Connected Routes						
Internet Group Management Protocol (IGMP) <input checked="" type="checkbox"/> Enabled						
<input checked="" type="checkbox"/> IGMP Fast Leave <input type="checkbox"/> IGMP Multicast to Unicast						
Domain Routing (add route entry according to interface from which DNS record is received) <input type="checkbox"/> Enabled						

To view additional parameters on the page, click the **Advanced** button.

2. To add a new routing rule:
 - a. Under the 'Routing Table' group, click the **New Route** link; the following page appears:

Figure 3-195: Adding a Routing Rule

Name:	LAN switch VLAN 1
Destination:	0 . 0 . 0 . 0
Netmask:	255 . 255 . 255 . 255
Gateway:	0 . 0 . 0 . 0
Metric:	0

- b. Define the following fields:
 - ◆ **Name:** select the network device.
 - ◆ **Destination:** enter the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.

- ♦ **Netmask:** network mask is used in conjunction with the destination to determine when a route is used.
- ♦ **Gateway:** enter the device's IP address.
- ♦ **Metric:** measurement of a route's preference. Typically, the lowest metric is the most preferred route. If multiple routes have the same metric value, the default route is the first in the order of appearance.

3. To add or edit a default route:

- a. Under the 'Default Routes' group, click the required device whose default route you want to edit or click the **New Default Route** link to add a default route; the following page appears:

Figure 3-196: Editing the Default Route

Device:	PPTP VPN ▼
Metric:	4

- b. If adding a default route, From the 'Device' drop-down list, select the WAN device.
- c. In the 'Metric' field, enter a value for the metric route preference.
- d. Click **OK** to save the settings.



Notes:

- To add an additional (logical) default route device, you must first define a new WAN device that has an IP address.
- Although multiple devices may be configured as default routes, only one serves as the default route—the one with the lowest metric value, or, if metric values are identical, the first in order.

4. To enable load balancing between multiple WAN devices:


- a. Under the 'Load Balancing' group, select the 'Enabled' check box; the load balancing table appears.
- b. Select the devices on which load balancing is performed by checking their respective check boxes.
- c. Click the **Edit**  icon corresponding to the device for which you want to modify the weight in the balancing procedure (determines the ratio of IP pairs provided to each device); the following page appears:

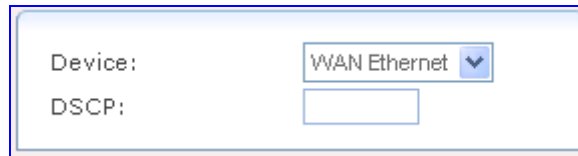
Figure 3-197: Defining Load Balancing

Device:	WAN Ethernet
Weight:	1

- d. In the 'Weight' field, enter the numeric ratio to represent the weight of the device.
- e. Click **OK** to save the settings.

5. To add a DSCP-based policy route:
 - a. Under the 'DSCP-Based Policy Routing' group, click the **New Route** link; the following page appears:

Figure 3-198: Adding DSCP-Based Route



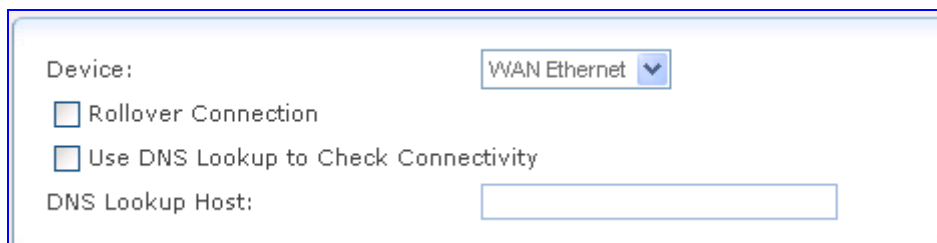
- b. From the 'Device' drop-down list, select the network device.
- c. In the 'DSCP' field, specify the DSCP value. All traffic matching this DSCP value is routed to the selected device.
- d. Click **OK** to save the settings.



Note: The DSCP-based policy routing ensures that specified traffic is routed via a certain WAN device, but if this WAN device is defined as the default route, other traffic may also be routed through it. If you want your device to be dedicated to transmitting only traffic matching the DSCP value you specified, you must clear the check box corresponding to the default route for that device.

6. To enable failover between multiple WAN devices:
 - a. Under the 'Failover' group, select the 'Enabled' check box; the failover table appears under the group.
 - b. Click the **Add Device** link; the following page appears:

Figure 3-199: Defining Failover between WAN Devices



- c. From the 'Device' drop-down list, select the WAN device to configure as failover.
 - d. Select the 'Rollover Connection' check box to configure the WAN device as a rollover connection type of failover.
 - e. Select the 'Use DNS Lookup to Check Connectivity' check box to enable periodic connectivity check using a DNS query, and then in the 'DNS Lookup Host' field, enter the URL that the periodic check queries.
 - f. Click **OK** to save the settings.
7. To enable connections defined above to use RIP:
 - a. Under the 'Routing Information Protocol (RIP)' group, select the 'Enabled' check box.
 - ◆ **Poison Reverse:** the device advertises acquired route information with a high metric for other routers to disregard it.
 - ◆ **Do not Advertise Direct Connected Routes:** the device does not advertise the route information to the same subnet device from which it was obtained.

8. To enable Internet Group Management Protocol (IGMP) multicasting:
 - a. Under the 'Internet Group Management Protocol (IGMP)' group, select the 'Enabled' check box. When a host sends a request to join a multicast group, the device listens and intercepts the group's traffic, forwarding it to the subscribed host. The device keeps record of subscribed hosts. When a host requests to cancel its subscription, the device queries for other subscribers and stops forwarding the multicast group's traffic after a short timeout.
 - ◆ **IGMP Fast Leave:** if a host is the only subscriber, the device stops forwarding traffic to it immediately upon request (i.e., no query delay).
 - ◆ **IGMP Multicast to Unicast:** the device converts incoming multicast data stream into unicast format to route it to the specific LAN host that requested the data. Therefore, the device prevents flooding the rest of the LAN hosts with irrelevant multicast traffic.
9. To add a route entry according to the interface from which DNS record is received, under the 'Domain Routing' group, select the 'Enabled' check box. When the device's DNS server receives a reply from an external DNS server, it adds a routing entry for the IP address of the reply through the device from which it arrived. This means that future packets from this IP address are routed through the device from which the reply arrived.
10. Click **OK** to save the settings.

3.3.3.7.2 Configuring BGP and OSPF

The BGP and OSPF feature is an implementation of two routing protocols used to deliver up-to-date routing information to a network or a group of networks, called Autonomous System.

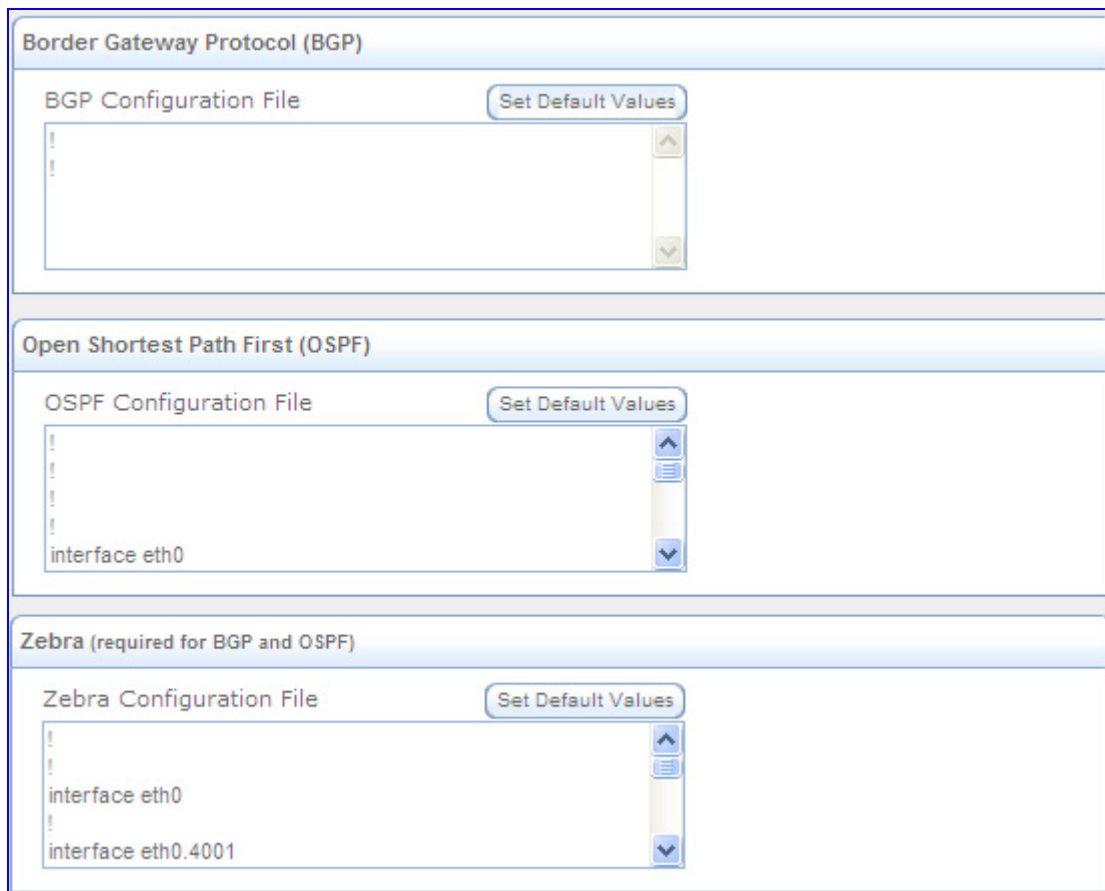
- **Border Gateway Protocol (BGP):** The main routing protocol of the Internet. It is used to distribute routing information among Autonomous Systems (for more information, refer to the protocol's RFC at <http://www.ietf.org/rfc/rfc1771.txt>).
- **Open Shortest Path First Protocol (OSPF):** An Interior Gateway Protocol (IGP) used to distribute routing information within a single Autonomous System (for more information, refer to the protocol's RFC at <http://www.ietf.org/rfc/rfc2328.txt>). The feature's routing engine is based on the Quagga GNU routing software package. By using the BGP and OSPF protocols, this routing engine enables the device to exchange routing information with other routers within and outside an Autonomous System.

If the OSPF daemon is activated, the device starts sending the 'Hello' packets to other routers to create adjacencies. After determining the shortest path to each of the neighboring routers, Zebra updates the routing table according to the network changes. If the BGP daemon is activated, the device starts to advertise routes it uses to other BGP-enabled network devices located in the neighboring Autonomous System(s). The BGP protocol uses TCP as its transport protocol. Therefore, the device first establishes a TCP connection to routers with which it communicates. KeepAlive messages are sent periodically to ensure the liveness of the connection. When a change in the routing table occurs, the device advertises an Update message to its peers. This update message adds a new route or removes the unfeasible one from their routing table.

➤ To enable BGP and OSPF:

1. Click the **BGP & OSPF** item (**Configuration** tab > **Data** menu > **Data Routing** submenu > **BGP & OSPF**); the following page appears:

Figure 3-200: Page Displaying Area for Configuration File



The screenshot shows a web-based configuration interface with three main sections, each with a title bar and a 'Set Default Values' button:

- Border Gateway Protocol (BGP)**: Contains a text area for the BGP Configuration File, which is currently empty.
- Open Shortest Path First (OSPF)**: Contains a text area for the OSPF Configuration File. It shows the text 'interface eth0'.
- Zebra (required for BGP and OSPF)**: Contains a text area for the Zebra Configuration File. It shows the text 'interface eth0' and 'interface eth0.4001'.

2. Create a configuration file for the protocol daemon and also for Zebra. Zebra is Quagga's IP routing management daemon which provides kernel routing table updates, interface lookups, and redistribution of routes between the routing protocols. To view examples of the configuration files, browse to <http://www.quagga.net/docs/quagga.pdf>.
3. Enter the configuration files in their respective code fields. Alternatively, click the **Set Default Values** button located to the right of each code field. The default values displayed are as follows:
 - **BGP:**

```
!router bgp <AS number> ; The exclamation mark is Quagga's
comment character. The router bgp string is a command that
activates the BGP daemon. The exclamation mark emphasizes
that the command must be followed by an exact Autonomous
System's ID number.

log syslog ; instructs the daemon to send its log messages
to the system log.
```
 - **OSPF:**

```
router ospf ; activates the OSPF daemon
log syslog
```


- **Zebra:**

```
interface eth1 ; instructs the daemon to query and update
routing information via a specific WAN device
log syslog
```

4. Click **OK** to save the settings.

3.3.3.8 Objects and Rules

The **Objects and Rules** submenu allows you to configure objects and rules. Once defined, they can later be used in other configurations (e.g., in Access List rules). This submenu includes the following items:

- **Protocols** (see "Configuring Protocols" on page 283)
- **Network Objects** (see "Configuring Network Objects" on page 284)
- **Scheduler Rules** (see "Configuring Scheduler Rules" on page 285)


























3.3.3.8.1 Configuring Protocols

The **Protocols** item displays a list of preset and user-defined applications and common port settings. You can use protocols in various security features such as Port Forwarding. You can add new protocols to support new applications or edit existing ones according to your needs.

➤ **To define a protocol:**

1. Click the **Protocols** item (**Configuration** tab > **Data** menu > **Objects and Rules** submenu > **Protocols**); the following page appears:

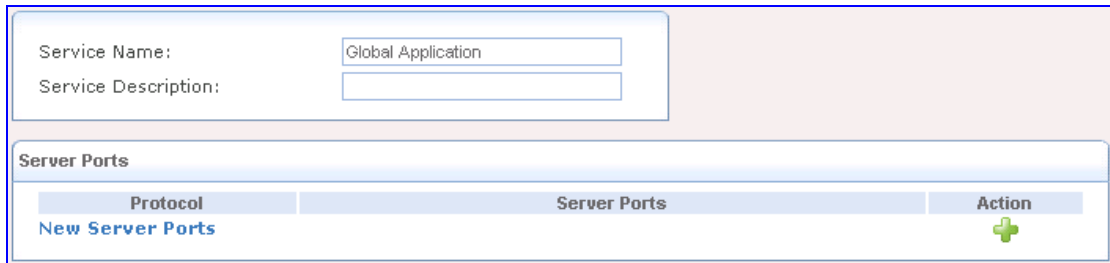
Figure 3-201: Viewing Pre-defined Protocols

Protocols	Ports	Action
FTP	TCP Any -> 21	 
HTTP	TCP Any -> 80	 
HTTPS	TCP Any -> 443	 
IMAP	TCP Any -> 143	 
L2TP	UDP Any -> 1701	 
Ping	ICMP Echo Request	 
POP3	TCP Any -> 110	 
SMTP	TCP Any -> 25	 
SNMP	UDP Any -> 161	 
Telnet	TCP Any -> 23	 
TFTP	UDP 1024-65535 -> 69	 
Traceroute	UDP 32769-65535 -> 33434-33523	 
New Entry		

2. Click the **Advanced** button for a complete list of the supported protocols.

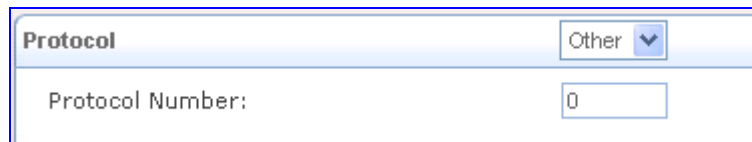
3. Click the **New Entry** link; the following page appears:

Figure 3-202: Adding a Service Protocol



4. In the 'Service Name' field, enter a name for the service protocol.
5. In the 'Service Description' field, enter a brief description of this service.
6. Click the **New Server Ports** link; the following page appears:

Figure 3-203: Defining Service Server Ports



7. From the 'Protocol' drop-down list, select any of the protocols available, or add a new one by selecting 'Other'.
8. Enter the relevant information, and then click **OK** to save the settings.

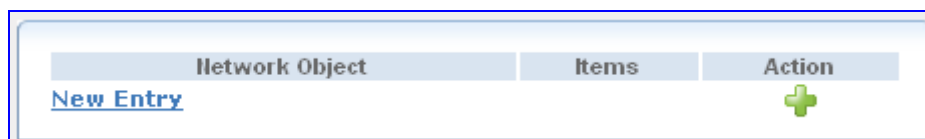
3.3.3.8.2 Configuring Network Objects

Network Objects is a method used to logically define a set of LAN hosts according to specific criteria such as MAC address, IP address, or host name. Defining such a group can assist when configuring system rules. For example, network objects can be used when configuring security filtering such as IP address, host name, or MAC address filtering. You can use network objects to apply security rules based on host names instead of IP addresses. This may be useful, since IP addresses change from time to time. It is also possible to define network objects according to MAC addresses, making rule application more persistent against network configuration settings. Moreover, the device supports DHCP Options 60, 61, and 77. DHCP Option 60 enables application of security and QoS rules on a network object according to its unique vendor class ID. For example, a vendor's IP telephone can be identified and applied with specific QoS priority rules.

➤ To define a network object:




1. Click the **Network Objects** item (**Configuration** tab > **Data** menu > **Objects and Rules** submenu > **Network Objects**); the following page appears:

Figure 3-204: Configuring Network Objects




- Click the **New Entry** link; the following page appears:

Figure 3-205: Defining Name for Network Object

Network Object					
Description:	<input type="text" value="Global Object"/>				
<table border="1"> <thead> <tr> <th>Item</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>New Entry</td> <td></td> </tr> </tbody> </table>		Item	Action	New Entry	
Item	Action				
New Entry					

- In the 'Description' field, enter a name for the network object.
- Click the **New Entry** link; the following page appears:

Figure 3-206: Defining Network Object Type

Network Object Type:	<input type="text" value="IP Address"/> 
IP Address:	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

- From the 'Network Object Type' drop-down list, select a network object type; the page displays the respective fields for entering the relevant information. The group definition can be according to one of the following:
 - IP Address: enter an IP address common to the group.
 - IP Subnet: enter a subnet IP address and a subnet mask.
 - IP Range: enter first and last IP addresses in the range.
 - MAC Address: enter a MAC address and mask.
 - Host Name: enter a host name common to the group.
 - DHCP Option: enter a vendor class ID.
- Click **OK** to save the settings.


3.3.3.8.3 Configuring Scheduler Rules

Scheduler rules are used for limiting the activation of Firewall rules to specific time periods, specified in days of the week, and hours.

➤ **To define a scheduler rule:**

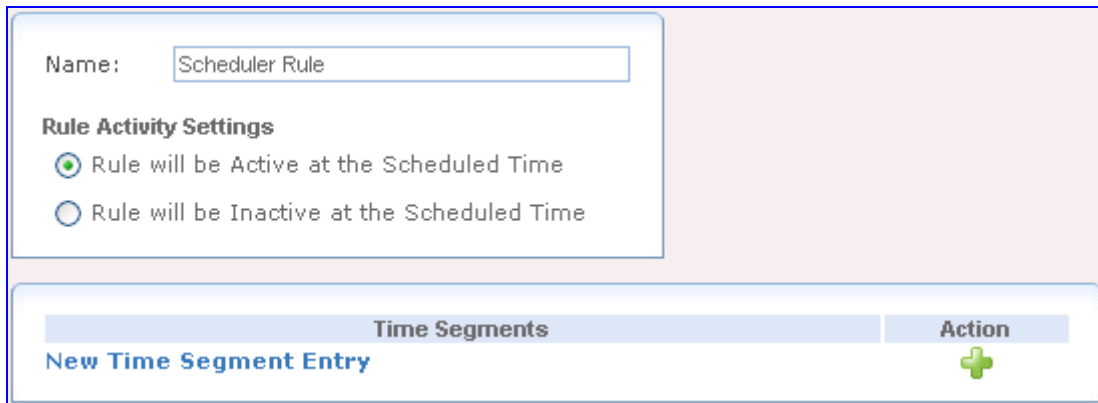
- Click the **Scheduler Rules** item (**Configuration** tab > **Data** menu > **Objects and Rules** submenu > **Scheduler Rules**); the following page appears:

Figure 3-207: Configuring Scheduler Rules

Name	Settings	Status	Action
New Entry			

2. Click the **New Entry** link; the following page appears:

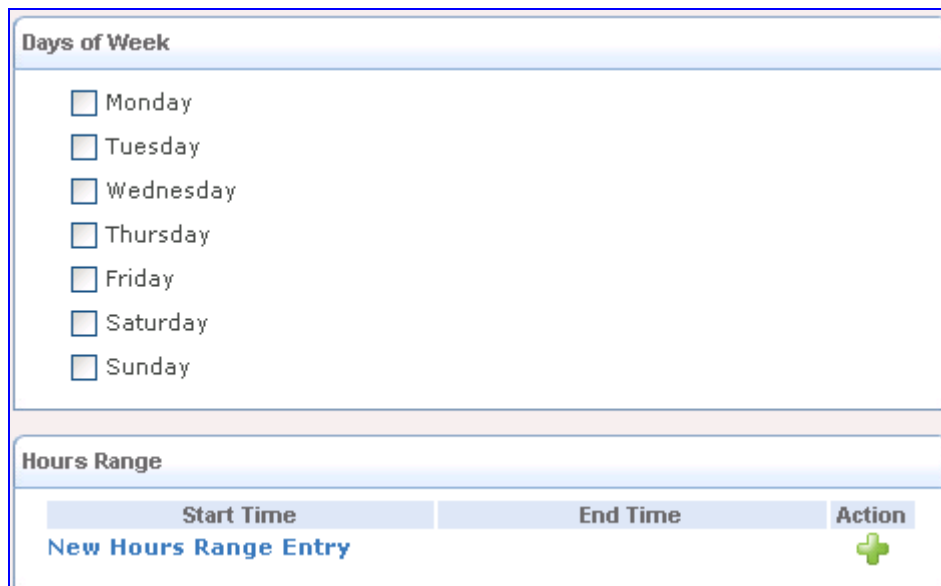
Figure 3-208: Defining Scheduler Rule Name



The screenshot shows a web form for defining a scheduler rule. It has a 'Name' field with the text 'Scheduler Rule'. Below it is a 'Rule Activity Settings' section with two radio buttons: 'Rule will be Active at the Scheduled Time' (selected) and 'Rule will be Inactive at the Scheduled Time'. At the bottom, there is a table with two columns: 'Time Segments' and 'Action'. The 'Time Segments' column contains a link 'New Time Segment Entry'. The 'Action' column contains a green plus icon.

3. In the 'Name' field, enter a name for the Scheduler rule.
4. Under the 'Rule Activity Settings' group, specify whether the rule is active or inactive during the designated time period, by selecting the appropriate option.
5. Click the **New Time Segment Entry** link to define the rule's time segment; the following page appears:

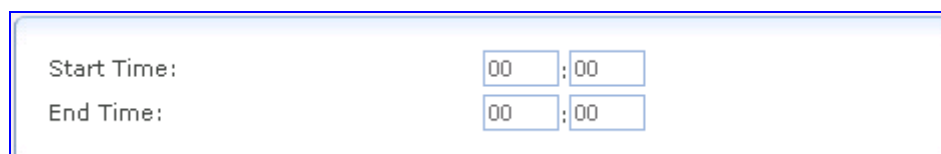
Figure 3-209: Defining Time Segment



The screenshot shows a web form for defining a time segment. It has two main sections: 'Days of Week' and 'Hours Range'. The 'Days of Week' section has a list of days from Monday to Sunday, each with an unchecked checkbox. The 'Hours Range' section has a table with three columns: 'Start Time', 'End Time', and 'Action'. The 'Start Time' and 'End Time' columns are empty. The 'Action' column contains a green plus icon. Below the table is a link 'New Hours Range Entry'.

6. Under the 'Days of Week' group, select the day(s) of the week on which the rule is active or inactive.
7. Under the 'Hours Range' group, click the **New Hours Range Entry** link to define a specific hour range for the rule; the following page appears:

Figure 3-210: Defining Hour Range



The screenshot shows a web form for defining an hour range. It has two rows: 'Start Time' and 'End Time'. Each row has two input fields for hours and minutes, separated by a colon. The 'Start Time' row has '00' in the hours field and '00' in the minutes field. The 'End Time' row has '00' in the hours field and '00' in the minutes field.

8. Enter the desired start and end time values for the rule.



Note: The defined start and end time is applied to all days of the week that you selected previously.

9. Click **OK** to return to the previous page, and then click **OK** again to return to the main page.

3.3.3.9 Configuring Network Connections

The device supports various network connections, both physical and logical. The **Data System > Connections** item enables you to configure the various parameters for your physical connections, the LAN and WAN, and create new connections, using tunneling protocols over existing connections such as PPP and VPN.

Every network connection in the device can be configured as one of three types: WAN, LAN or DMZ (Demilitarized). For example, you may define that a LAN connection on the device operates as a WAN network. This means that all hosts in this LAN are referred to as WAN computers, both by computers outside the device and by the device itself. WAN and firewall rules may be applied, such as on any other WAN network. Another example is that a network connection can be defined as a DMZ network. Although the network is physically inside the device, it functions as an unsecured, independent network for which the device merely acts as a router.



Note: When defining a network connection as a DMZ network:









- Change the connection's routing mode to 'Route'.
- Add a routing rule on your external gateway (which may be with your ISP) informing of the DMZ network behind the device.

You can configure the following network connections:

- WAN – Internet connection:
 - Point-to-Point Protocol over Ethernet
 - Ethernet Connection
 - Point-to-Point Tunneling Protocol
 - Layer 2 Tunneling Protocol
 - Dynamic Host Configuration Protocol
 - Manual IP Address Configuration
- Virtual Private Network over the Internet:
 - Layer 2 Tunneling Protocol over Internet Protocol Security
 - Layer 2 Tunneling Protocol Server
 - Point-to-Point Tunneling Protocol Virtual Private Network
 - Point-to-Point Tunneling Protocol Server
 - Internet Protocol Security

- Internet Protocol Security Server
- LAN Ethernet switch
- Advanced connections:
 - LAN Bridging
 - VLAN Interface
 - Internet Protocol over Internet Protocol
 - General Routing Encapsulation
- **To access the Network Connection list table:**
- Click the **Connections** item (**Configuration** tab > **Data** menu > **Data System** submenu > **Connections**); the following page appears:

Figure 3-211: Configuring Network Connections

Name	Status	Action
 LAN switch	1 Ports Connected	
 WAN Ethernet	Connected	
 LAN switch VLAN 1	Connected	 
New Connection		

The page displays the configured WAN and LAN connections:

- **LAN Switch:** represents all the device's ports.
- **WAN Ethernet:** connects the device to another network either directly or through an external modem.

3.3.3.9.1 Network Connection Wizard

The logical network connections can easily be created using the Connection wizard. This wizard consists of a series of Web pages, intuitively structured to gather all the information needed to create a logical connection. The procedure for configuring a connection using the wizard is described below.


- **To create a connection using the wizard:**
- 1. In the 'Connections' page, click the **New**  icon; the wizard appears.

Figure 3-212: Defining a New Connection

☒ **Internet Connection**
 Connect to the Internet using your external DSL modem, Cable modem or Ethernet connection so you can browse the Web and read email.

☐ **Connect to a Virtual Private Network over the Internet**
 Connect MSBG to a business network using a Virtual Private Network (VPN) so you can work from home, workplace or another location.

☐ **Advanced Connection**
 Manually configure a new connection.

2. Select whether you want to configure an Internet connection, a VPN connection, or advanced connections:
 - **For configuring an Internet connection:**
 - a. Select the 'Internet Connection' option, and then click **Next**; the following wizard page appears:

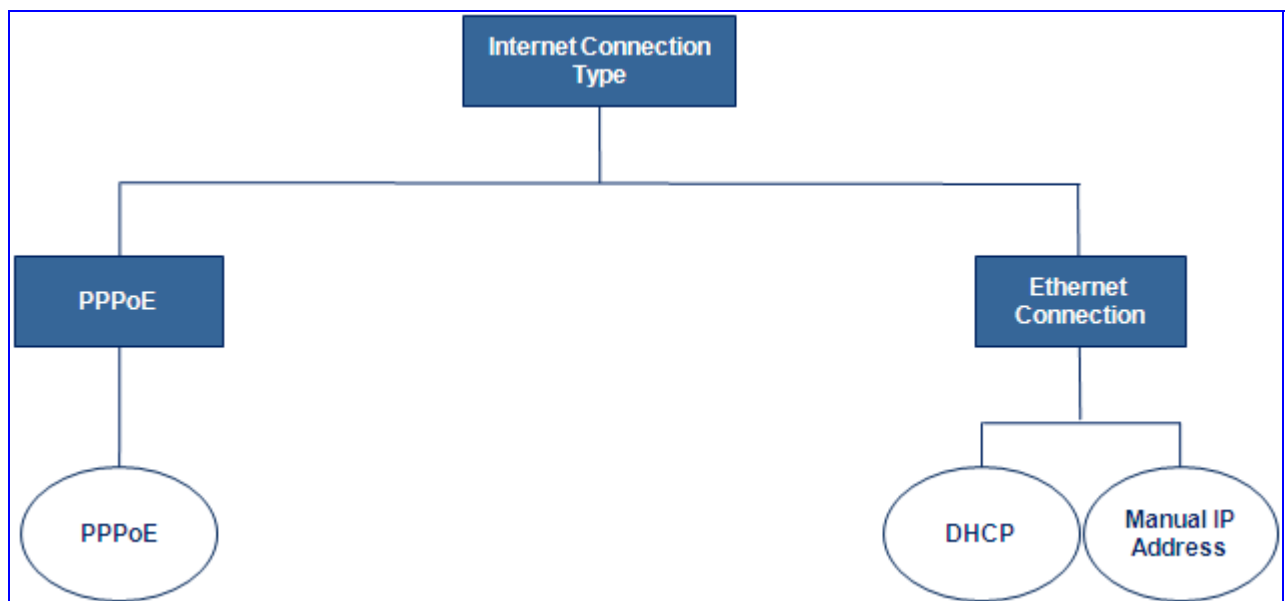
Figure 3-213: Defining Internet Connection Type



- b. Select the required Internet connection type, click **Next**, and then follow the instructions provided by the wizard.

The tree-like structure of the Internet Connection options are shown below:

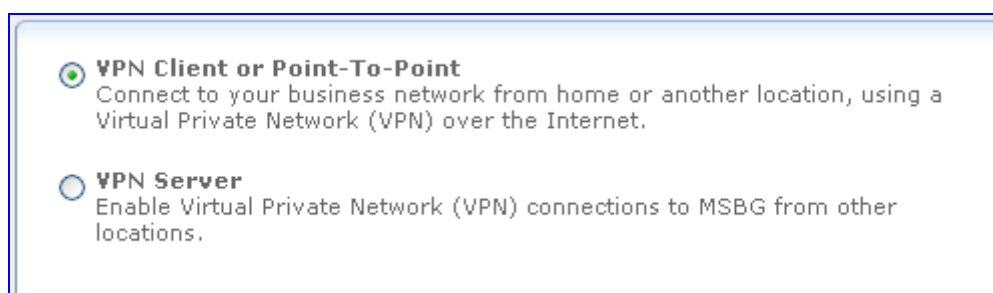
Figure 3-214: Internet Connection Types



- ◆ **Point-to-Point Protocol over Ethernet (PPPoE):** relies on two widely accepted standards, PPP and Ethernet. PPPoE enables your home network PCs that communicate on an Ethernet network to exchange information with PCs on the Internet. PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.
- ◆ **Ethernet connection:** configures the physical WAN Ethernet connection. It is the most basic method intended for connections that do not require user name and password to connect to the Internet. The IP address can be assigned automatically using a DHCP server or manually defined.

- For configuring a **VPN-over-Internet** connection:
 - a. Select the 'Connect to a Virtual Private Network over the Internet' option, and then click **Next**; the following wizard page appears:

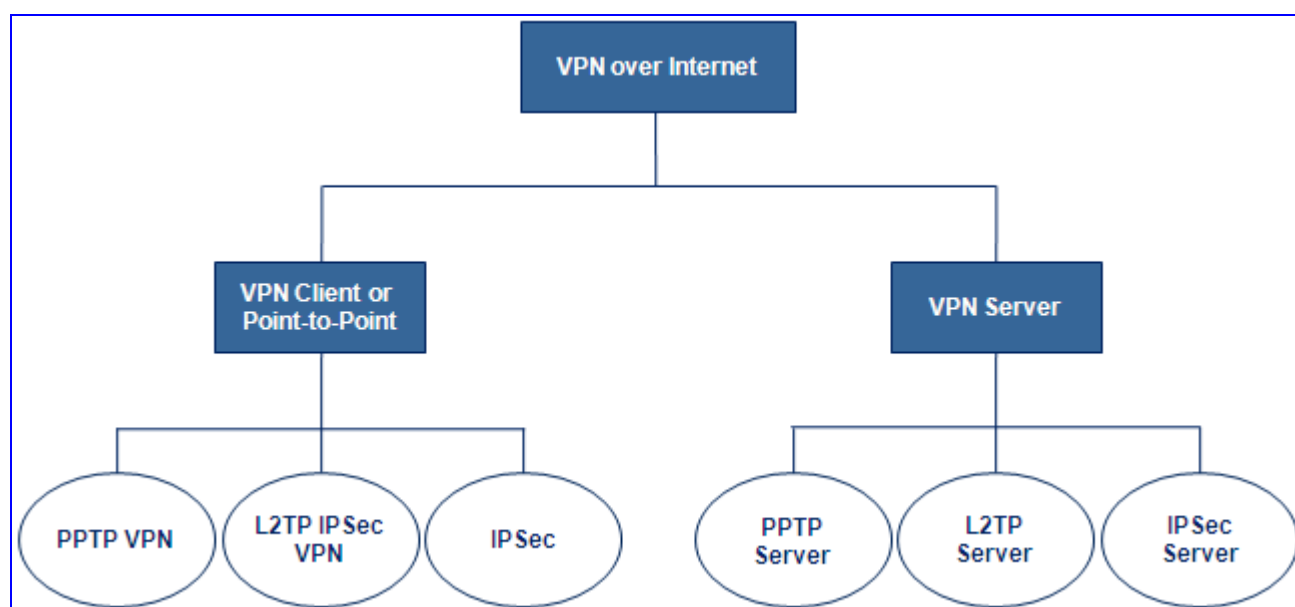
Figure 3-215: Defining Virtual Private Network over Internet



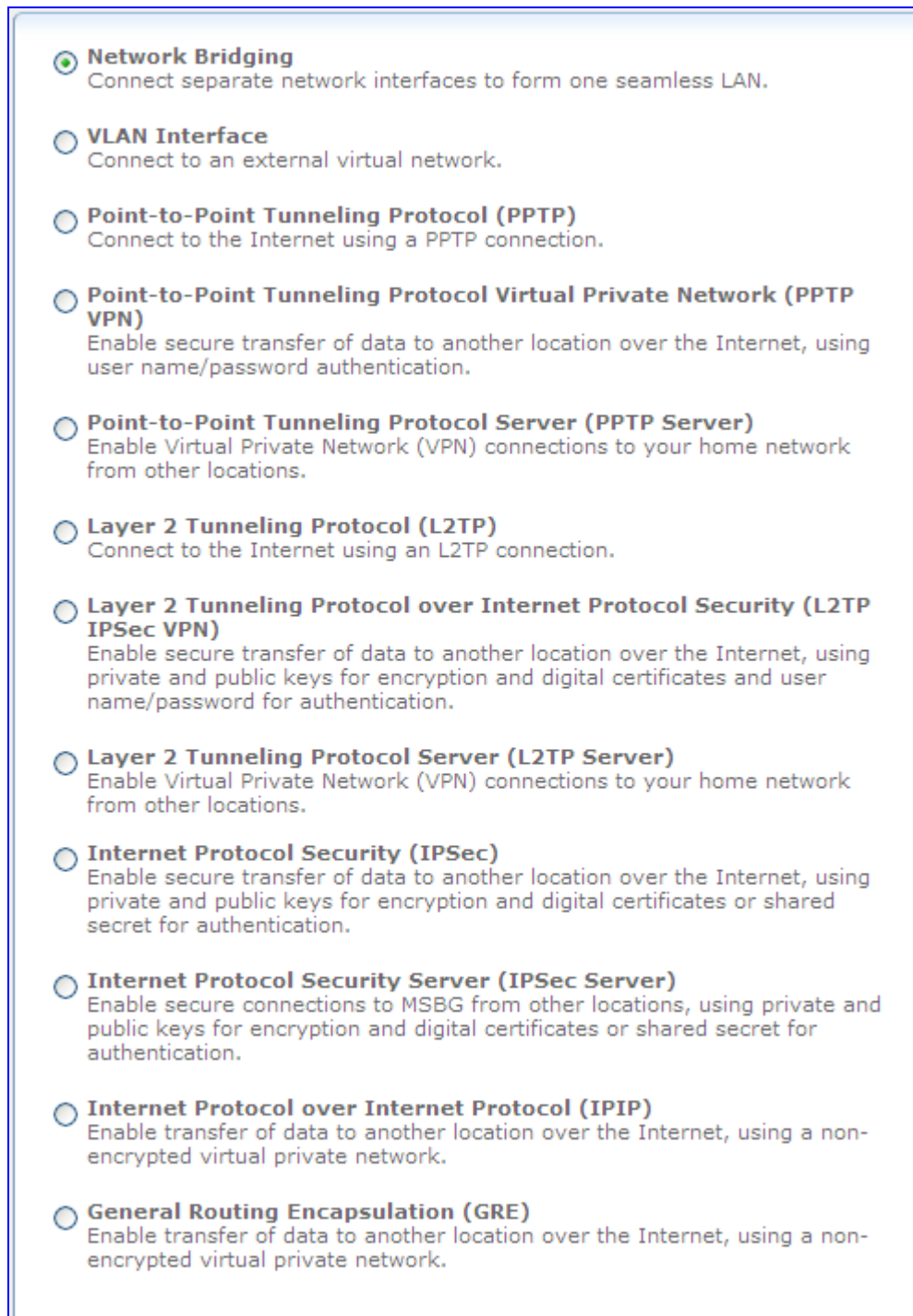
- b. Select the VPN connection type, click **Next**, and then follow the instructions provided by the wizard.

You can connect the device to a business network using a VPN so you can work from home, your workplace or another location. The device can either act as a VPN server (accepting VPN client connection requests) or a VPN client. The VPN over Internet options are shown below:

Figure 3-216: VPN Connection Types



- **For manually configuring a new connection:**
 - a. Select the 'Advanced Connection' option, and then click **Next**; the following wizard page appears:



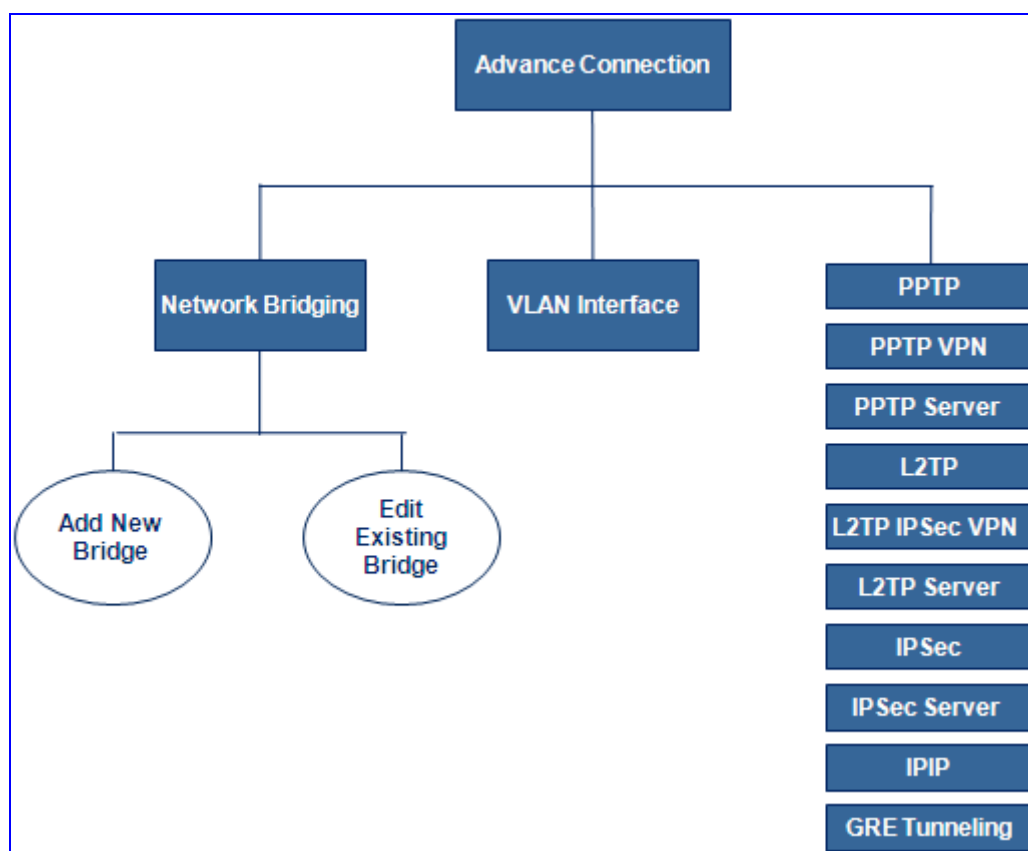
The screenshot shows a network configuration wizard with the following options:

- ☒ **Network Bridging**
Connect separate network interfaces to form one seamless LAN.
- ☐ **VLAN Interface**
Connect to an external virtual network.
- ☐ **Point-to-Point Tunneling Protocol (PPTP)**
Connect to the Internet using a PPTP connection.
- ☐ **Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)**
Enable secure transfer of data to another location over the Internet, using user name/password authentication.
- ☐ **Point-to-Point Tunneling Protocol Server (PPTP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.
- ☐ **Layer 2 Tunneling Protocol (L2TP)**
Connect to the Internet using an L2TP connection.
- ☐ **Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates and user name/password for authentication.
- ☐ **Layer 2 Tunneling Protocol Server (L2TP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.
- ☐ **Internet Protocol Security (IPsec)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates or shared secret for authentication.
- ☐ **Internet Protocol Security Server (IPsec Server)**
Enable secure connections to MSBG from other locations, using private and public keys for encryption and digital certificates or shared secret for authentication.
- ☐ **Internet Protocol over Internet Protocol (IPIP)**
Enable transfer of data to another location over the Internet, using a non-encrypted virtual private network.
- ☐ **General Routing Encapsulation (GRE)**
Enable transfer of data to another location over the Internet, using a non-encrypted virtual private network.

- b. Select the required connection type, click **Next**, and then follow the instructions provided by the wizard.

The Advanced Connection wizard tree is illustrated below:

Figure 3-217: Advanced Connection Wizard Tree



3. When the wizard completes the initial configuration (by clicking **Finish**), the new connection type appears listed in the Network Connections page.

3.3.3.9.2 LAN Switch

The LAN Switch interface represents all the device's ports. The switch ports are physical sockets on the device to which different cables connect. You can assign VLAN's to each port.

➤ To view and edit LAN switch ports:




1. In the 'Connections' page, click the **Edit**  icon corresponding to the **LAN switch** connection; the **General** tab page is displayed.

Figure 3-218: General Tab - LAN Switch

Name:	LAN Switch
Device Name:	eth0
Status:	1 Ports Connected
Network:	LAN
Connection Type:	Hardware Ethernet Switch
Download Rate:	100 Mbps
Upload Rate:	100 Mbps
MAC Address:	00:90:8f:22:2e:31
IP Address Distribution:	Disabled
Received Packets:	4492
Sent Packets:	2797
Time Span:	0:26:17

2. Select the **Switch** tab; the displayed table lists all available ports, their status, and the VLANs of which they are members. Untagged packets (packets with no VLAN tag) that arrive at a port are tagged with the VLAN number that appears under the PVID (Port VLAN Identifier) column.

Figure 3-219: Switch Tab

HW Switch Ports				
Port	Status	PVID	VLANs	Action
<input checked="" type="checkbox"/> Port 0	Disconnected	1		
<input checked="" type="checkbox"/> Port 1	Connected 100.0 Mbps Full-Duplex	1		
<input checked="" type="checkbox"/> Port 2	Disconnected	1		



You can edit the configuration of each port by clicking the corresponding **Edit**  icon.

Figure 3-220: Assigning VLAN to Port

VLAN

Default VLAN ID:

VLAN ID	Egress Policy	Action
1	Untagged (Remove VLAN Header)	
New Entry		



- a. In the 'Default VLAN ID' field, enter the port's VLAN identifier. You may add additional identifiers to the VLAN by clicking the **New**  icon.

Figure 3-221: Defining VLANs

VLAN ID:

Egress Policy: Untagged (Remove VLAN Header) 

- b. In the 'VLAN ID' field, enter the new VLAN ID.
- c. From the 'Egress Policy' drop-down list, select whether or not to tag incoming packets with the port's VLAN header.
- d. Click **OK**.

3. Select the **STP** tab.

Figure 3-222: STP Tab

STP:

Bridge ID:

Designated Root:

Priority:

Hello Time:

Max Age:

Forward Delay:

☒ Enabled

Seconds

Seconds

Seconds

STP Ports

Port	Id	Cost	Protocol	State	Role	Designated Root	Designated Cost	Flags
Port 0			N/A		N/A	N/A	N/A	N/A
Port 1								
Port 2			N/A		N/A	N/A	N/A	N/A

4. Select the 'STP' check box to enable the Spanning Tree Protocol on the device. You should use this to ensure that there are no loops in your network configuration, and apply these settings in case your network consists of multiple switches, or other bridges apart from those created by the device.
 - Bridge ID: Identifies the bridge priority and MAC address.
 - Designated Root: Indicates the ID of the bridge with the lowest path cost to the instance ID.
 - Priority: Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the root bridge. The default value is 32768. The port priority value is provided in increments of 4096. For example, 4096, 8192, 12288, and so on. The range is 0 to 65535.
 - Hello Time: Specifies the device Hello Time. The Hello Time indicates the amount of time (in seconds) a root bridge waits between configuration messages. The default is 2 seconds. The range is 1 to 10 seconds.
 - Max Age: Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time (in seconds) a bridge waits before sending configuration messages. The default is 20 seconds. The range is 6 to 40 seconds.
 - Forward Delay: Specifies the device forward delay time. The Forward Delay Time indicates the amount of time (in seconds) a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds. The range is 4 to 30 seconds.
 - STP Ports:
 - ◆ Priority: Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 and 240. The priority value is in increments of 16.
 - ◆ Cost: Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

- ◆ Point-to-Point: Specifies if a point-to-point links is established, or permits the device to establish a point-to-point link. The possible field values are Enable, Disable, or Auto.
- ◆ Edge: Specifies if a edge links is established, or permits the device to establish a point-to-point link. The possible field values are Enable, Disable, or Auto.

3.3.3.9.3 WAN Ethernet

The WAN Ethernet connection can connect the device to another network directly or via an external modem. The Connection Wizard provides three methods to configure this connection:

- Dynamic Host Configuration Protocol (see "Dynamic Host Control Protocol" on page 295)
- Manual IP Address Configuration (see "Manual WAN IP Address" on page 296)
- Point-to-Point Protocol over Ethernet (see "Point-to-Point Protocol over Ethernet (PPPoE)" on page 297)

3.3.3.9.3.1 Dynamic Host Control Protocol

The Dynamic Host Configuration Protocol (DHCP) connection wizard utility is one of the three methods used to configure the physical WAN Ethernet connection. It is a dynamic negotiation method, where the client obtains an IP address automatically from the service provider when connecting to the Internet.

➤ **To configure a DHCP connection:**


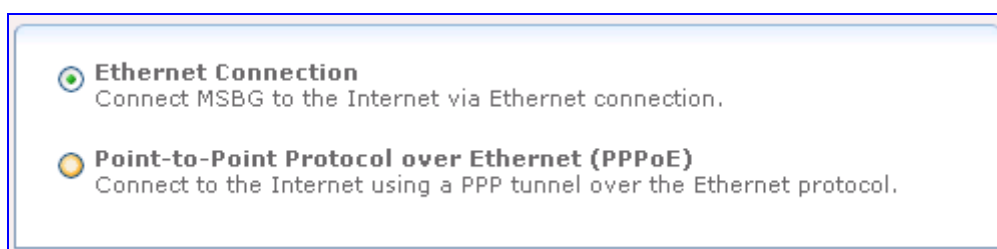
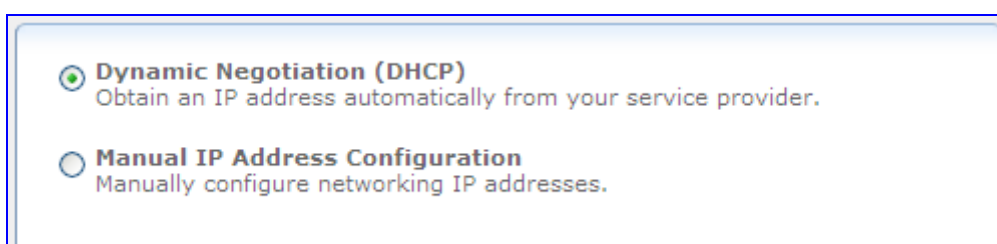
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Internet Connection' option, and then click **Next**; the Internet connection options are displayed.

Figure 3-223: Ethernet Connection Option



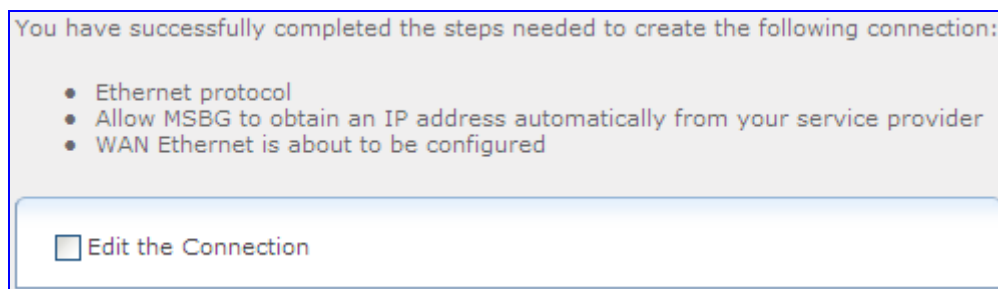
3. Select the 'Ethernet Connection' option, and then click **Next**; the following page appears.

Figure 3-224: Selecting Internet Ethernet Connection



4. Select the 'Dynamic Negotiation (DHCP)' option, and then click **Next**; a summary of the new connection is shown.

Figure 3-225: Internet Connection for External Cable Modem Added



5. Select the 'Edit the Connection' check box if you want to edit the new connection after clicking **Finish**.
6. Click **Finish** to save the settings; the WAN Ethernet connection is added and an IP address is obtained from a DHCP server.

3.3.3.9.3.2 Manual WAN IP Address

The Manual IP Address Configuration connection wizard utility is one of the three methods used to configure the physical WAN Ethernet connection. It is used to manually configure the networking IP addresses when connecting to the Internet.

➤ To manually configure the IP address:


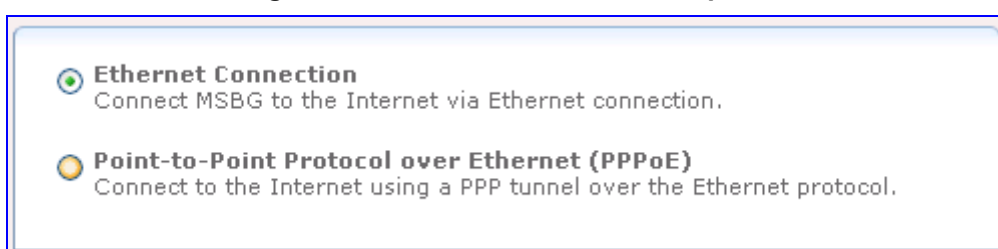
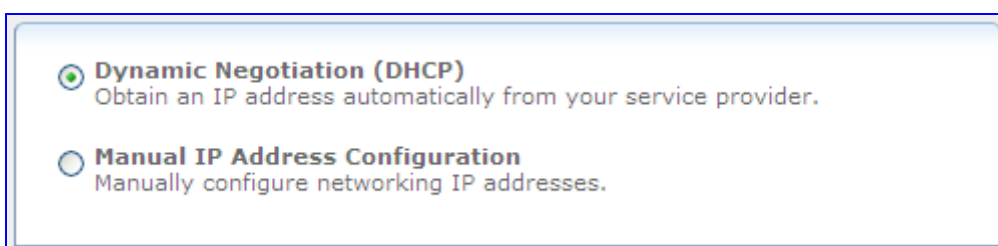
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Internet Connection' option, and then click **Next**; the Internet connection options are displayed.

Figure 3-226: Ethernet Connection Option



3. Select the 'Ethernet Connection' option, and then click **Next**; the following page appears.

Figure 3-227: Selecting Internet Ethernet Connection



4. Select the 'Manual IP Address Configuration' option, and then click **Next**; a summary of the new connection is shown.

Figure 3-228: Manual IP Address Configuration

IP Address:	10	.	13	.	4	.	12
Subnet Mask:	255	.	255	.	0	.	0
Default Gateway:	10	.	13	.	0	.	1
Primary DNS Server:	0	.	0	.	0	.	0
Secondary DNS Server:	0	.	0	.	0	.	0

5. Enter the IP address, subnet mask, default gateway, and DNS server addresses in their respective fields. These values should either be provided to you by your ISP or configured by your system administrator.
6. Click **Next**; a summary of the new connection is shown.

Figure 3-229: Manual WAN Ethernet Added Successfully

You have successfully completed the steps needed to create the following connection:

- Ethernet protocol
- Manually configured MSBG's networking IP addresses. The designated IP address will be 10.13.4.12
- WAN Ethernet is about to be configured

☐ Edit the Connection

7. Select the 'Edit the Connection' check box if you want to edit the new connection after clicking **Finish**.
8. Click **Finish** to save the settings; the WAN Ethernet connection is added.

3.3.3.9.3.3 Point-to-Point Protocol over Ethernet (PPPoE)

Point-to-Point Protocol over Ethernet (PPPoE) relies on two widely accepted standards, PPP and Ethernet. PPPoE enables your home network PCs that communicate on an Ethernet network to exchange information with PCs on the Internet. PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multi-point architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.

➤ **To create a PPPoE connection:**


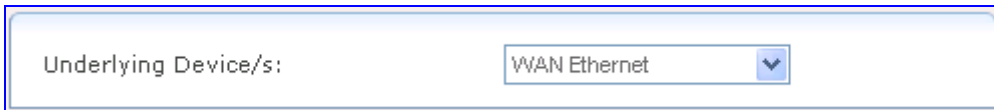
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Internet Connection' option, and then click **Next**.

Figure 3-230: Defining Internet Connection Type



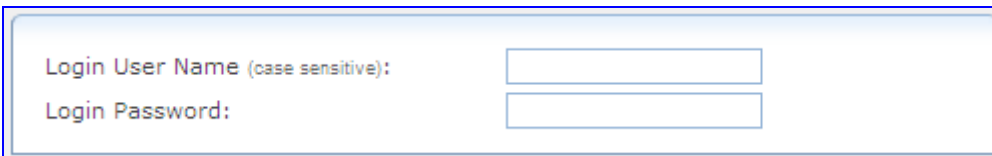
3. Select the 'Point-to-Point Protocol over Ethernet (PPPoE)' option, and then click **Next**.

Figure 3-231: Selecting Underlying Device



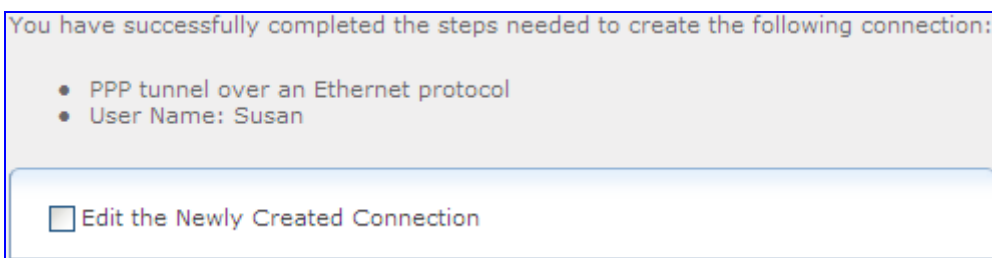
4. Select the underlying device for which you want to create the connection, and then click **Next**.

Figure 3-232: Defining PPPoE Properties



5. In the 'Login User Name' and 'Login Password' fields, enter the PPPoE username and password provided by your ISP, and then click **Next**; the following is displayed if successfully configured:

Figure 3-233: PPPoE Connection Added Successfully



6. Select the 'Edit the Newly Created Connection' check box if you want to edit the new connection after clicking **Finish**.
7. Click **Finish** to save the settings; the new PPPoE connection is added to the network connections list.

For editing the PPPoE connection, follow the procedure below:

➤ **To edit the PPPoE connection:**

1. In the 'Connections' page, click the **WAN PPPoE** link; the **General** tab appears displaying general properties.
2. Select the **Settings** tab to edit various settings (see "Editing Existing Connections" on page 328).
3. Select the **Routing** tab to edit the routing parameters (see "Editing Existing Connections" on page 328).
4. Select the **PPP** tab.
 - Service Name: Specify the networking peer's service name, if provided by your ISP.
 - On Demand: Select this check box to initiate the PPP session only when packets are sent over the Internet.
 - Time Between Reconnect Attempts: Specify the duration between PPP reconnected attempts, as provided by your ISP.
 - PPP Authentication: PPP currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. Select the authentication protocols that the device may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Support Microsoft CHAP', 'Support Microsoft CHAP Version 2', or both are selected.
 - ◆ Login User Name: As agreed with ISP.
 - ◆ Login Password: As agreed with ISP.
 - ◆ Support Unencrypted Password (PAP): PAP is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.
 - ◆ Support Challenge Handshake Authentication (CHAP): CHAP is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.
 - ◆ Support Microsoft CHAP: Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.
 - ◆ Support Microsoft CHAP Version 2: Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.
 - PPP Encryption: PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link. Select the encryption methods that the device may use when negotiating with a PPTP server. Select all the methods if no information is available about the server's encryption methods. Note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication protocols.
 - ◆ Require Encryption: Select this check box to ensure that the PPP connection is encrypted.

- ◆ Support Encryption (40 Bit Keys): Select this check box if your peer supports 40 bit encryption keys.
 - ◆ Support Maximum Strength Encryption (128 Bit Keys): Select this check box if your peer supports 128 bit encryption keys.
 - ◆ MPPE Encryption Mode: Select the Microsoft Point to Point Encryption (MPPE) mode. This is a means of representing PPP packets in an encrypted form.
 - ◆ PPP Compression: The PPP Compression Control Protocol (CCP) is responsible for configuring, enabling, and disabling data compression algorithms on both ends of the point-to-point link. It is also used to signal a failure of the compression/ decompression mechanism in a reliable manner. For each compression algorithm, select one of the following from the drop down menu:
 - ✓ Reject: Reject PPP connections with peers that use the compression algorithm.
 - ✓ Allow: Allow PPP connections with peers that use the compression algorithm.
 - ✓ Require: Ensure a connection with a peer is using the compression algorithm.
5. Select the **Advanced** tab to enable the firewall for this network connection (see "Editing Existing Connections" on page 328).

3.3.3.9.4 LAN Bridge

The LAN bridge connection is used to combine several LAN devices under one virtual network. Note that when a bridge is removed, its formerly underlying devices inherit the bridge's DHCP settings. For example, the removal of a bridge that is configured as DHCP client automatically configures the LAN devices formerly constituting the bridge as DHCP clients with the exact DHCP client configuration.

➤ To create a LAN bridge:


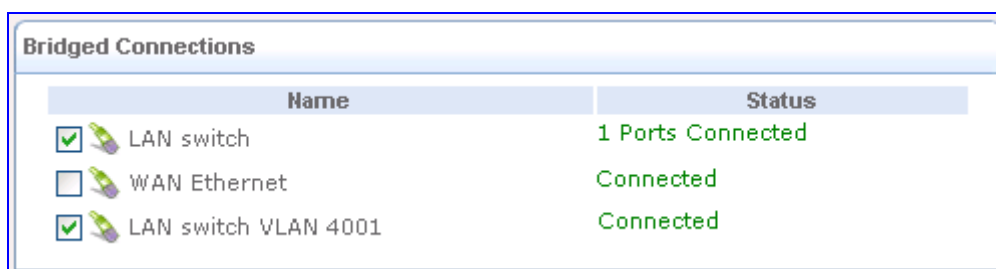
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Advanced Connection' option, and then click **Next**; the 'Advanced Connection' page appears.
3. Select the 'Network Bridging' option, and then click **Next**; the following page appears.

Figure 3-234: Selecting LAN Interfaces for Bridge Connection



4. Add new connections or remove existing ones, by selecting or clearing their respective check boxes.

- Click **Next**; the LAN bridge is successfully added.

Figure 3-235: LAN Bridge Successfully Added

You have successfully completed the steps needed to create the following connection:

- Network Bridge
- LAN Hardware Ethernet Switch VLAN 4001, LAN Hardware Ethernet Switch VLAN 1 will be bridged
- Bridged connections are about to lose their IP settings. If the bridge is removed the connections should be configured
- MSBG Management Console might lose its connectivity

☐ Edit the Connection

- Select the 'Edit the Connection' check box if you want to edit the new connection after clicking **Finish**.
- Click **Finish** to save the settings; the new bridge is added to the network connections list.

3.3.3.9.5 Virtual LAN Interface (VLAN)

A virtual LAN interface enables you to group workstations together into one broadcast domain, even if they are not located on the same LAN segment. The device allows you to create virtual Ethernet-based networks according to the IEEE 802.1Q standard.

➤ **To create a VLAN interface:**


- In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
- Select the 'Advanced Connection' option, and then click **Next**; the 'Advanced Connection' page appears.
- Select the 'VLAN Interface' option, and then click **Next**; the following page appears.

Figure 3-236: Adding a VLAN Interface

Underlying Device: WAN Ethernet ▼

VLAN ID: 1

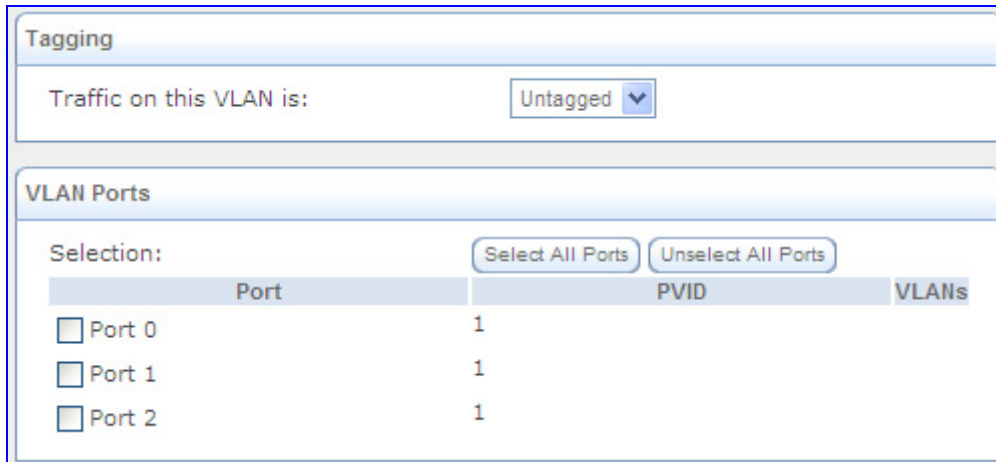


Note: By default, all the device's physical LAN devices are enslaved by the device's LAN bridge. A VLAN cannot be created over an enslaved network device. Therefore, remove a device from the bridge before creating a VLAN over it.

- From the 'Underlying Device' drop-down list, select the underlying device for this interface. The list displays the device's Ethernet connections.

5. In the 'VLAN ID' field, enter a value for the VLAN ID, and then click **Next**. If you chose to create the VLAN over the WAN, skip to Step 9. If you chose to create the VLAN over the LAN bridge, the following page appears.

Figure 3-237: Assigning VLAN to LAN Ports



Tagging

Traffic on this VLAN is: Untagged ▼

VLAN Ports

Selection: Select All Ports Unselect All Ports

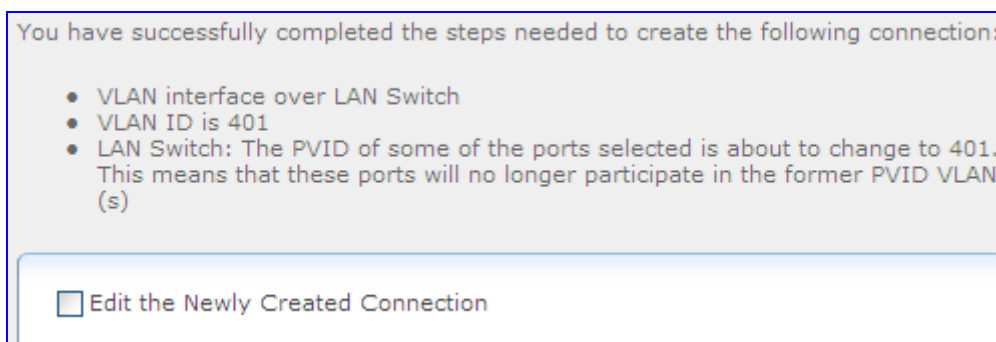
Port	PVID	VLANs
<input type="checkbox"/> Port 0	1	
<input type="checkbox"/> Port 1	1	
<input type="checkbox"/> Port 2	1	

6. From the 'Traffic on this VLAN is' drop-down list, select one of the following:
 - 'Untagged': the VLAN is determined based on information such as the ID of a port on which the data arrives (PVID).
 - 'Tagged': adds a tag header (a 32-bit label serving as a VLAN ID) to the frames transferred over the VLAN.

Note: If the created virtual network is intended for VLAN-unaware hosts, it is recommended that you select the 'Untagged' option.

7. In the 'VLAN Ports' group, select the LAN bridge ports on which you want to enable the VLAN.
8. Click **Next**; a summary of the VLAN configuration is displayed.

Figure 3-238: VLAN Added Successfully



You have successfully completed the steps needed to create the following connection:

- VLAN interface over LAN Switch
- VLAN ID is 401
- LAN Switch: The PVID of some of the ports selected is about to change to 401. This means that these ports will no longer participate in the former PVID VLAN(s)

☐ Edit the Newly Created Connection

9. Select the 'Edit the Newly Created Connection' check box if you want to edit the new connection after clicking **Finish**.
10. Click **Finish** to save the settings; the new VLAN interface is added to the network connections list.

➤ **To edit the VLAN interface connection:**

1. In the 'Connections' page, click the VLAN link (e.g., "LAN Switch VLAN 401"); the **General** tab appears displaying general properties.
2. Select the **Settings** tab to edit various settings (see "Editing Existing Connections" on page 328).
3. Select the **Advanced** tab.

Figure 3-239: VLAN Interface Advanced Tab

- a. If your VLAN interface is over WAN, then you can enable the firewall for this network connection by selecting the 'Internet Connection Firewall' check box.
- b. You can add alias names (additional IP addresses) to the device by clicking under the 'Additional IP Addresses' group the **New IP Address** link. This enables you to access the device using these aliases in addition to the device's defined IP address.
- c. When creating a VLAN interface over a LAN connection, it is possible to determine the IP header's Differentiated Services Code Point (DSCP) priority value according to the VLAN header's 802.1p Class of Service (CoS) tag. The DSCP value can then be used for Quality of Service (Qos) traffic prioritization.
 - a. Select the 'Enabled' check box.
 - b. Click the **New DSCP Remark** link; the following page appears:

Figure 3-240: Defining DSCP Remarkings

- c. Map the required 802.1p CoS value to a DSCP value, and then click **OK**; the new value pair appears in the table.
4. Click **OK** to save the settings.

3.3.3.9.6 Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) is a protocol developed by Microsoft targeted at creating VPN connections over the Internet. This enables remote users to access the device via any ISP that supports PPTP on its servers. PPTP encapsulates network traffic, encrypts content using Microsoft's Point-to-Point Encryption (MPPE) protocol that is based on RC4, and routes using the generic routing encapsulation (GRE) protocol. PPTP is targeted at serving two purposes:

- Connecting the device to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established using user name and password authentication.
- Connecting the device to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using user name and password authentication.

➤ To create a PPTP connection:


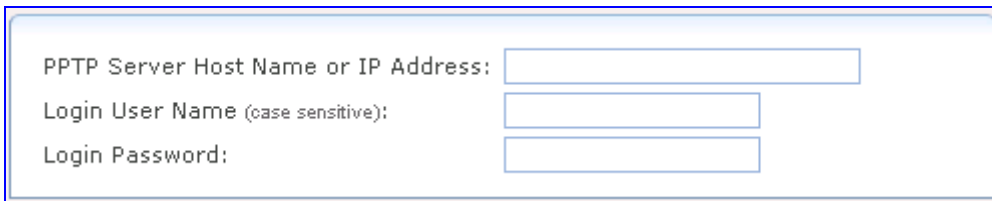
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Advanced Connection' option, and then click **Next**; the 'Advanced Connection' page appears.
3. Select the 'Point-to-Point Tunneling Protocol (PPTP)' option, and then click **Next**; the following page appears.

Figure 3-241: Defining PPTP Properties



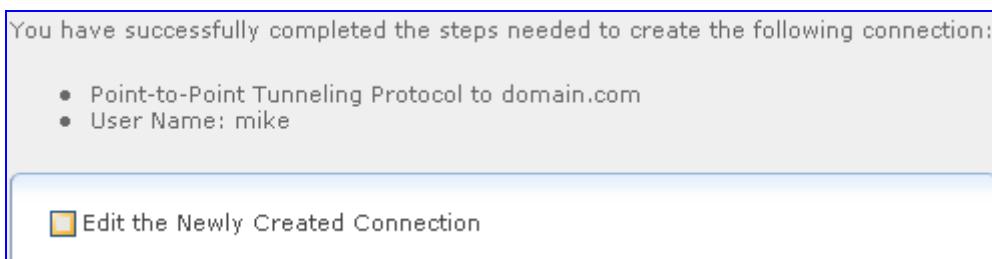
PPTP Server Host Name or IP Address:

Login User Name (case sensitive):

Login Password:

4. In the 'PPTP Server Host Name or IP Address' field, enter the PPTP server host name or IP address provided by your ISP.
5. In the 'Login User Name' and 'Login Password' fields, enter the username and password provided by your ISP.
6. Click **Next**; the following is displayed if successfully configured:

Figure 3-242: PPTP Connection Added Successfully



You have successfully completed the steps needed to create the following connection:

- Point-to-Point Tunneling Protocol to domain.com
- User Name: mike

☐ Edit the Newly Created Connection

7. Select the 'Edit the Newly Created Connection' check box if you want to edit the new connection after clicking **Finish**.
8. Click **Finish** to save the settings; the new PPTP connection is added to the network connections list.

The following procedure describes how to create a PPTP VPN connection.

➤ **To create a PPTP VPN connection:**


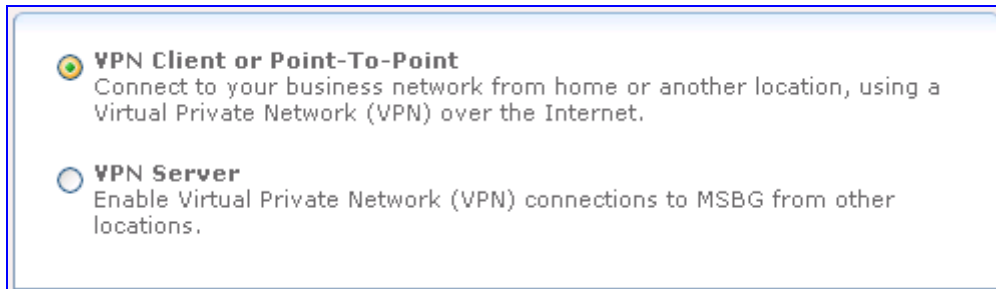
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Connect to a Virtual Private Network over the Internet' option, and then click **Next**.

Figure 3-243: Selecting VPN Type for IPSec

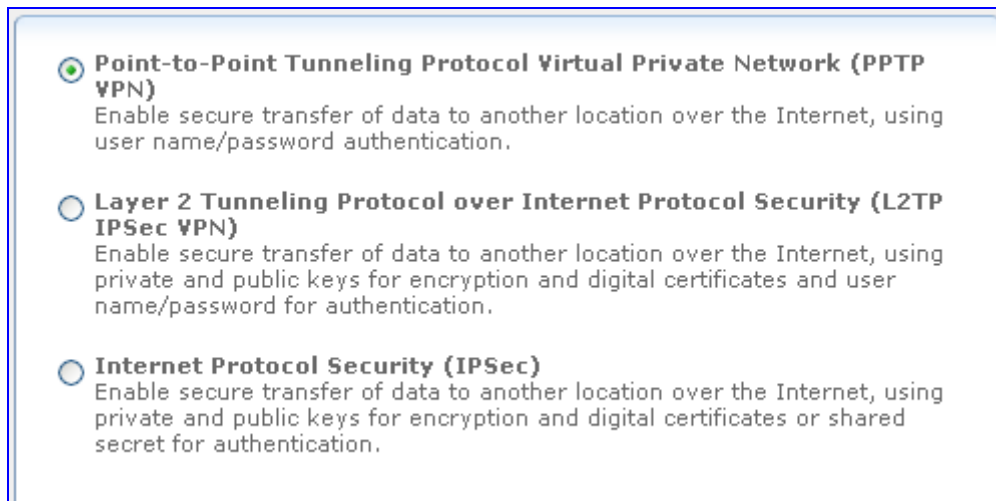


☒ **VPN Client or Point-To-Point**
Connect to your business network from home or another location, using a Virtual Private Network (VPN) over the Internet.

☐ **VPN Server**
Enable Virtual Private Network (VPN) connections to MSBG from other locations.

3. Select the 'VPN Client or Point-To-Point' option, and then click **Next**.

Figure 3-244: Selecting Protocol to Connect to Remote VPN Server



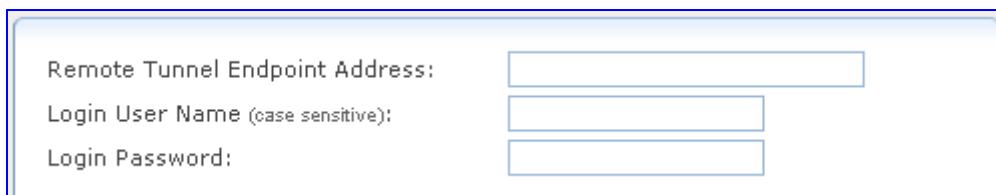
☒ **Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)**
Enable secure transfer of data to another location over the Internet, using user name/password authentication.

☐ **Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPsec VPN)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates and user name/password for authentication.

☐ **Internet Protocol Security (IPsec)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates or shared secret for authentication.

4. Select the 'Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)' option, and then click **Next**.

Figure 3-245: Defining PPTP VPN Properties



Remote Tunnel Endpoint Address:

Login User Name (case sensitive):

Login Password:

5. In the 'Remote Tunnel Endpoint Address' field, enter the remote tunnel endpoint address. This is the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.
6. In the 'Login User Name' and 'Login Password' fields, enter the username and password provided by the administrator of the network you are trying to access.

7. Click **Next**; the following is displayed if successfully configured:

Figure 3-246: PPTP VPN Successfully Added

You have successfully completed the steps needed to create the following connection:

- Point-to-Point Tunneling Protocol to 192.172.0.1 VPN server
- User Name: Sue

☐ Edit the Newly Created Connection

8. Select the 'Edit the Newly Created Connection' check box if you want to edit the new connection after clicking **Finish**.
9. Click **Finish** to save the settings; the new PPTP VPN connection is added to the network connections list.

To view and edit the PPTP connection, follow the procedure below:

➤ **To edit the PPTP connection:**

1. In the 'Connections' page, click the **PPTP VPN** link; the **General** tab appears displaying general properties.
2. Select the **Settings** tab to edit various settings (see "Editing Existing Connections" on page 328).
3. Select the **Routing** tab to edit the routing parameters (see "Editing Existing Connections" on page 328).
4. Select the **PPP** tab.

Figure 3-247: PPP Tab

☐ On Demand (will attempt to connect only when packets are sent)

Time Between Reconnect Attempts: Seconds

PPP Authentication

Login User Name (case sensitive):

Login Password:

☐ Support Unencrypted Password (PAP)

☐ Support Challenge Handshake Authentication (CHAP)

☒ Support Microsoft CHAP (MS-CHAP)

☒ Support Microsoft CHAP Version 2 (MS-CHAP v2)

PPP Encryption

☒ Require Encryption (disconnect if server declines)

☒ Support Encryption (40 bit keys)

☒ Support Maximum Strength Encryption (128 bit keys)

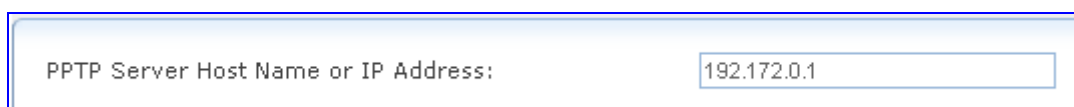
MPPE Encryption Mode:

- On Demand: Select this check box to initiate the PPP session only when packets are sent over the Internet.
- Time Between Reconnect Attempts: Specify the duration between PPP reconnected attempts, as provided by your ISP.

- PPP Authentication: PPP currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. Select the authentication protocols that the device may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Support Microsoft CHAP', 'Support Microsoft CHAP Version 2', or both are selected.
 - ◆ Login User Name: As agreed with ISP.
 - ◆ Login Password: As agreed with ISP.
 - ◆ Support Unencrypted Password (PAP): PAP is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.
 - ◆ Support Challenge Handshake Authentication (CHAP): CHAP is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.
 - ◆ Support Microsoft CHAP: Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.
 - ◆ Support Microsoft CHAP Version 2: Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.
- PPP Encryption: PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link. Select the encryption methods that the device may use when negotiating with a PPTP server. Select all the methods if no information is available about the server's encryption methods. Note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication protocols.
 - ◆ Require Encryption: Select this check box to ensure that the PPP connection is encrypted.
 - ◆ Support Encryption (40 Bit Keys): Select this check box if your peer supports 40 bit encryption keys.
 - ◆ Support Maximum Strength Encryption (128 Bit Keys): Select this check box if your peer supports 128 bit encryption keys.
 - ◆ MPPE Encryption Mode: Select the Microsoft Point to Point Encryption (MPPE) mode. This is a means of representing PPP packets in an encrypted form.

5. Select the **PPTP** tab.

Figure 3-248: PPTP Tab



PPTP Server Host Name or IP Address:

- In the 'PPTP Server Host Name or IP Address' field, enter the connection's host name or IP address obtained from your ISP.
6. Select the **Advanced** tab to enable the firewall for this network connection (see "Editing Existing Connections" on page 328).

3.3.3.9.7 Point-to-Point Tunneling Protocol Server (PPTP Server)

The device can act as a Point-to-Point Tunneling Protocol Server (PPTP Server), accepting PPTP client connection requests.

➤ **To create a PPTP server:**


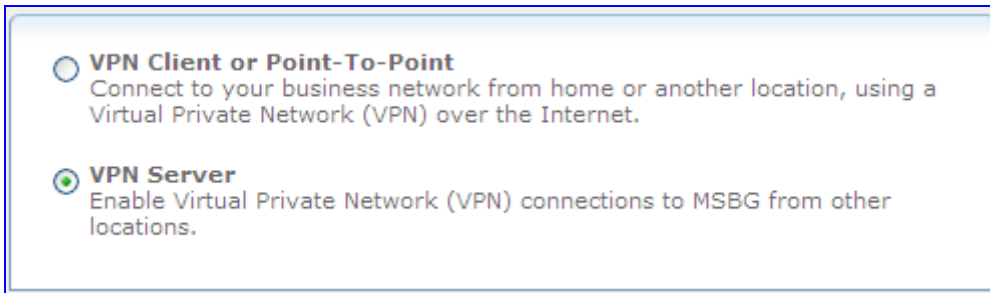
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Connect to a Virtual Private Network over the Internet' option, and then click **Next**.

Figure 3-249: VPN Connection Type



☐ **VPN Client or Point-To-Point**
Connect to your business network from home or another location, using a Virtual Private Network (VPN) over the Internet.

☒ **VPN Server**
Enable Virtual Private Network (VPN) connections to MSBG from other locations.

3. Select the 'VPN Server' option, and then click **Next**.

Figure 3-250: Selecting the VPN Protocol - PPTP Server



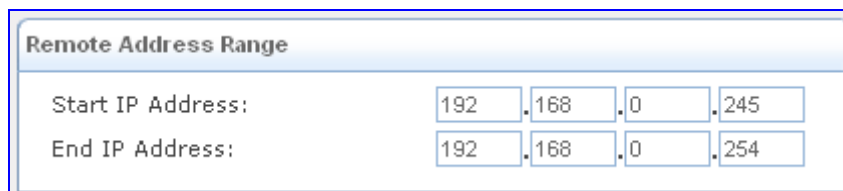
☒ **Point-to-Point Tunneling Protocol Server (PPTP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.

☐ **Layer 2 Tunneling Protocol Server (L2TP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.

☐ **Internet Protocol Security Server (IPSec Server)**
Enable secure connections to MSBG from other locations, using private and public keys for encryption and digital certificates or shared secret for authentication.

4. Select the 'Point-to-Point Tunneling Protocol Server (PPTP Server)' option, and then click **Next**.

Figure 3-251: Defining Remote Client Address Range



Remote Address Range				
Start IP Address:	192	168	0	245
End IP Address:	192	168	0	254

5. Specify the IP address range that the device reserves for remote users, and then click **Next**; the following is displayed if successfully configured:

Figure 3-252: PPTP Server Added Successfully

You have successfully completed the steps needed to create the following connection:

- Point-to-Point Tunneling Protocol Server enabled
- Remote Address Range: -

☐ Edit the Newly Created Connection

Note that the attention message alerting that there are no users with VPN permissions.

6. Select the 'Edit the Newly Created Connection' check box, and then click **Finish**.

Figure 3-253: Editing VPN Server

Server

Status: Waiting for Incoming Connections
☒ Enabled
[Click here to create VPN users](#)

Remote Address Range

Start IP Address:
End IP Address:

Connections

Name	Status	Action
------	--------	--------

7. Click the **Click here to create VPN users** link to define remote users that will be granted access to your home network.
8. Click **OK** to save settings; the new PPTP server connection is added to the Network Connection list.

3.3.3.9.8 Layer 2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol, enabling your device to create VPN connections. Derived from Microsoft's Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer 2 Forwarding (L2F) technology, L2TP encapsulates PPP frames into IP packets either at the remote user's PC or at an ISP that has an L2TP Remote Access Concentrator (LAC). The LAC transmits the L2TP packets over the network to the L2TP Network Server (LNS) at the corporate side. L2TP is targeted at serving two purposes:

- Connecting the device to the Internet when it is used as a cable modem, or when using an external cable modem. Such a connection is established using user name and password authentication.

- Connecting the device to a remote network using a Virtual Private Network (VPN) tunnel over the Internet. This enables secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates, and user name and password for authentication.

➤ **To create a L2TP connection:**


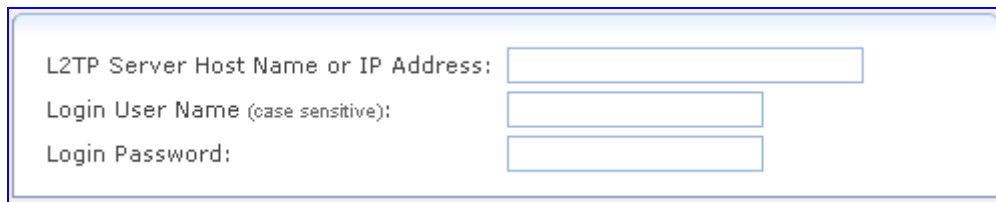
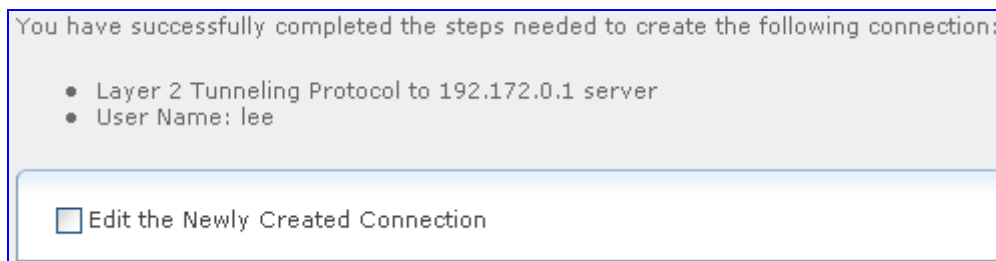
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Advanced Connection' option, and then click **Next**; the 'Advanced Connection' page appears.
3. Select the 'Layer 2 Tunneling Protocol (L2TP)' option, and then click **Next**.

Figure 3-254: Defining L2TP Properties



4. In the 'L2TP Server Host Name or IP Address' field, enter the L2TP server host name or IP address provided by your ISP.
5. In the 'Login User Name' and 'Login Password' fields, enter the username and password provided by your ISP.
6. Click **Next**; the following is displayed if successfully configured:

Figure 3-255: L2TP Connection Added Successfully



7. Select the 'Edit the Newly Created Connection' check box if you want to edit the new connection after clicking **Finish**.
8. Click **Finish** to save the settings; the new L2TP connection is added to the network connections list.

The following procedure describes how to create a L2TP VPN connection.

➤ **To create a L2TP VPN connection:**


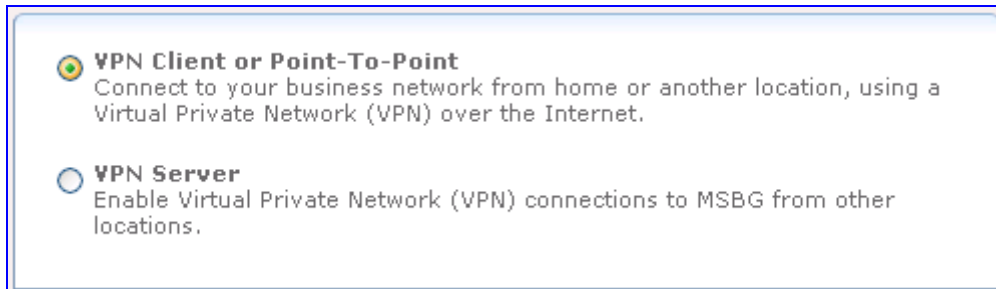
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Connect to a Virtual Private Network over the Internet' option, and then click **Next**.

Figure 3-256: Selecting VPN Type for IPSec

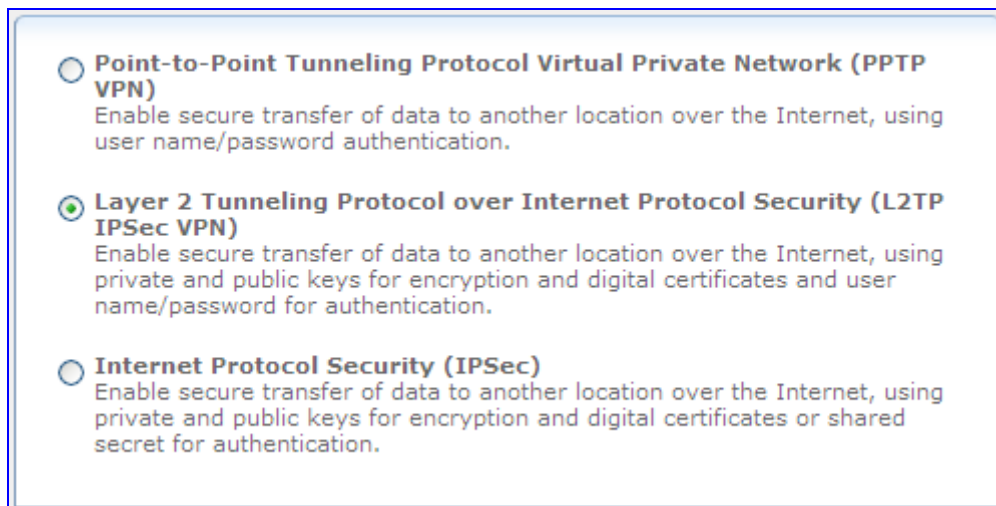


☒ **VPN Client or Point-To-Point**
Connect to your business network from home or another location, using a Virtual Private Network (VPN) over the Internet.

☐ **VPN Server**
Enable Virtual Private Network (VPN) connections to MSBG from other locations.

3. Select the 'VPN Client or Point-To-Point' option, and then click **Next**.

Figure 3-257: Selecting L2TP to Connect to Remote VPN Server



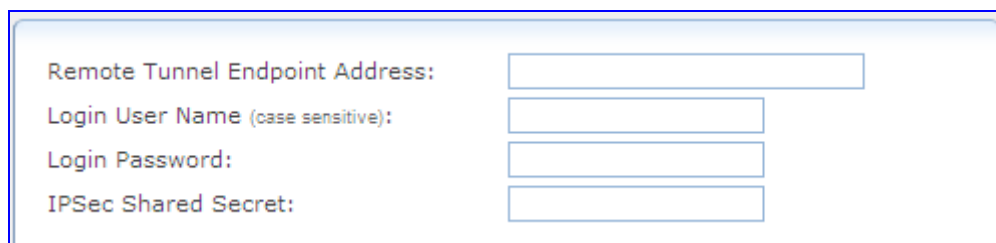
☐ **Point-to-Point Tunneling Protocol Virtual Private Network (PPTP VPN)**
Enable secure transfer of data to another location over the Internet, using user name/password authentication.

☒ **Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates and user name/password for authentication.

☐ **Internet Protocol Security (IPSec)**
Enable secure transfer of data to another location over the Internet, using private and public keys for encryption and digital certificates or shared secret for authentication.

4. Select the 'Layer 2 Tunneling Protocol over Internet Protocol Security (L2TP IPSec VPN)' option, and then click **Next**.

Figure 3-258: Defining L2TP Properties



Remote Tunnel Endpoint Address:

Login User Name (case sensitive):

Login Password:

IPSec Shared Secret:

5. In the 'Remote Tunnel Endpoint Address' field, enter the remote tunnel endpoint address. This is the IP address or domain name of the remote network computer, which serves as the tunnel's endpoint.
6. In the 'Login User Name' and 'Login Password' fields, enter the username and password provided by the administrator of the network you are trying to access.

7. In the 'IPSec Shared Secret' field, enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.
8. Click **Next**; the following is displayed if successfully configured:

Figure 3-259: L2TP Successfully Added

You have successfully completed the steps needed to create the following connection:

- Layer 2 Tunneling Protocol to 192.172.0.1 VPN server
- User Name: Lee

☐ Edit the Newly Created Connection

9. Select the 'Edit the Newly Created Connection' check box if you want to edit the new connection after clicking **Finish**.
10. Click **Finish** to save the settings; the new L2TP IPSec VPN connection is added to the network connections list.

To view and edit the L2TP connection, follow the procedure below:

➤ **To edit the L2TP connection:**

1. In the 'Connections' page, click the **L2TP VPN** link; the **General** tab appears displaying general properties.
2. Select the **Settings** tab to edit various settings (see "Editing Existing Connections" on page 328).
3. Select the **Routing** tab to edit the routing parameters (see "Editing Existing Connections" on page 328).
4. Select the **PPP** tab.

Figure 3-260: PPP Tab

☐ On Demand (will attempt to connect only when packets are sent)

Time Between Reconnect Attempts: Seconds

PPP Authentication

Login User Name (case sensitive):

Login Password:

☐ Support Unencrypted Password (PAP)

☐ Support Challenge Handshake Authentication (CHAP)

☒ Support Microsoft CHAP (MS-CHAP)

☒ Support Microsoft CHAP Version 2 (MS-CHAP v2)

PPP Encryption

☒ Require Encryption (disconnect if server declines)

☒ Support Encryption (40 bit keys)

☒ Support Maximum Strength Encryption (128 bit keys)

MPPE Encryption Mode:

- On Demand: Select this check box to initiate the PPP session only when packets are sent over the Internet.
- Time Between Reconnect Attempts: Specify the duration between PPP reconnected attempts, as provided by your ISP.
- PPP Authentication: PPP currently supports four authentication protocols: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft CHAP version 1 and 2. Select the authentication protocols that the device may use when negotiating with a PPTP server. Select all the protocols if no information is available about the server's authentication protocols. Note that encryption is performed only if 'Support Microsoft CHAP', 'Support Microsoft CHAP Version 2', or both are selected.
 - ◆ Login User Name: As agreed with ISP.
 - ◆ Login Password: As agreed with ISP.
 - ◆ Support Unencrypted Password (PAP): PAP is a simple, plain-text authentication scheme. The user name and password are requested by your networking peer in plain-text. PAP, however, is not a secure authentication protocol. Man-in-the-middle attacks can easily determine the remote access client's password. PAP offers no protection against replay attacks, remote client impersonation, or remote server impersonation.
 - ◆ Support Challenge Handshake Authentication (CHAP): CHAP is a challenge-response authentication protocol that uses MD5 to hash the response to a challenge. CHAP protects against replay attacks by using an arbitrary challenge string per authentication attempt.
 - ◆ Support Microsoft CHAP: Select this check box if you are communicating with a peer that uses Microsoft CHAP authentication protocol.
 - ◆ Support Microsoft CHAP Version 2: Select this check box if you are communicating with a peer that uses Microsoft CHAP Version 2 authentication protocol.
- PPP Encryption: PPP supports encryption facilities to secure the data across the network connection. A wide variety of encryption methods may be negotiated, although typically only one method is used in each direction of the link. Select the encryption methods that the device may use when negotiating with a PPTP server. Select all the methods if no information is available about the server's encryption methods. Note that PPP encryption can only be used with MS-CHAP or MS-CHAP-V2 authentication protocols.
 - ◆ Require Encryption: Select this check box to ensure that the PPP connection is encrypted.
 - ◆ Support Encryption (40 Bit Keys): Select this check box if your peer supports 40 bit encryption keys.
 - ◆ Support Maximum Strength Encryption (128 Bit Keys): Select this check box if your peer supports 128 bit encryption keys.
 - ◆ MPPE Encryption Mode: Select the Microsoft Point to Point Encryption (MPPE) mode. This is a means of representing PPP packets in an encrypted form.

5. Select the **L2TP** tab.

Figure 3-261: L2TP Tab

L2TP Server Host Name or IP Address:	<input type="text" value="192.172.0.1"/>
Shared Secret:	<input type="text"/>

- In the 'L2TP Server Host Name or IP Address' field, enter the connection's host name or IP address obtained from your ISP.
 - In the 'Shared Secret' field, enter the shared secret value obtained from your ISP.
6. Select the **Advanced** tab to enable the firewall for this network connection (see "Editing Existing Connections" on page 328).

3.3.3.9.9 Layer 2 Tunneling Protocol Server (L2TP Server)

The device can act as a Layer 2 Tunneling Protocol Server (L2TP Server), accepting L2TP client connection requests.

➤ **To create an L2TP server:**


1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Connect to a Virtual Private Network over the Internet' option, and then click **Next**.

Figure 3-262: VPN Connection Type

<input type="radio"/>	VPN Client or Point-To-Point Connect to your business network from home or another location, using a Virtual Private Network (VPN) over the Internet.
<input checked="" type="radio"/>	VPN Server Enable Virtual Private Network (VPN) connections to MSBG from other locations.

3. Select the 'VPN Server' option, and then click **Next**.

Figure 3-263: Selecting L2TP Server VPN Protocol

<input type="radio"/>	Point-to-Point Tunneling Protocol Server (PPTP Server) Enable Virtual Private Network (VPN) connections to your home network from other locations.
<input checked="" type="radio"/>	Layer 2 Tunneling Protocol Server (L2TP Server) Enable Virtual Private Network (VPN) connections to your home network from other locations.
<input type="radio"/>	Internet Protocol Security Server (IPSec Server) Enable secure connections to MSBG from other locations, using private and public keys for encryption and digital certificates or shared secret for authentication.

4. Select the 'Layer 2 Tunneling Protocol Server (L2TP Server)' option, and then click **Next**.

Figure 3-264: Defining L2TP Properties

The screenshot shows a web-based configuration window titled "Remote Address Range". It contains the following fields and options:

- Start IP Address:** A field with four sub-inputs, each containing the digit "0".
- End IP Address:** A field with four sub-inputs, each containing the digit "0".
- ☒ **Protect L2TP Connection by IPSec**
- L2TP Server IPSec Shared Secret:** An empty text input field.

5. In the 'Start IP Address' and 'End IP Address' fields, specify the address range that the device reserves for remote users.
6. By default, the L2TP connection is protected by the IP Security (IPSec) protocol (the option is selected). However, if you wish to keep this setting, you must provide a string that will serve as the 'L2TP Server IPSec Shared Secret'. Alternatively, clear this option to disable L2TP protection by IPSec.
7. Click **Next**; the following is displayed if successfully configured:

Figure 3-265: L2TP Server Added Successfully

The screenshot shows a success message box with the following content:

You have successfully completed the steps needed to create the following connection:

- Layer 2 Tunneling Protocol Server enabled
- Remote Address Range: 192.168.0.235 - 192.168.0.244

At the bottom, there is a button labeled ☐ Edit the Connection.

Note that the attention message alerting that there are no users with VPN permissions.

8. Select the 'Edit the Newly Created Connection' check box, and then click **Finish**.

Figure 3-266: Defining Advanced L2TP Properties

The screenshot shows a web-based configuration window titled "Server". It contains the following sections and fields:

- Status:** Waiting for Incoming Connections
- ☒ **Enabled**
- [Click here to create VPN users](#)
- ☒ **Protect L2TP Connection by IPSec**
- ☒ **Create Default IPSec Connection**
- L2TP Server IPSec Shared Secret:** 11111
- Remote Address Range:**
 - Start IP Address:** 192.168.0.235
 - End IP Address:** 192.168.0.244
- Connections:** A table with columns: Name, Status, Action.

9. Click the **Click here to create VPN users** link to define remote users that will be granted access to your home network.
10. Click **OK** to save settings; the new L2TP server connection is added to the Network Connection list.

3.3.3.9.10 Internet Protocol Security (IPSec)

Internet Protocol Security (IPSec) is a series of guidelines for the protection of Internet Protocol (IP) communications. It specifies procedures for securing private information transmitted over public networks.

➤ **To create an IPSec connection:**


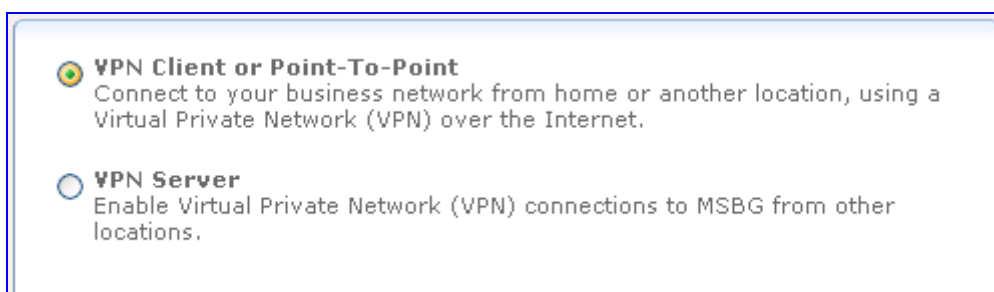
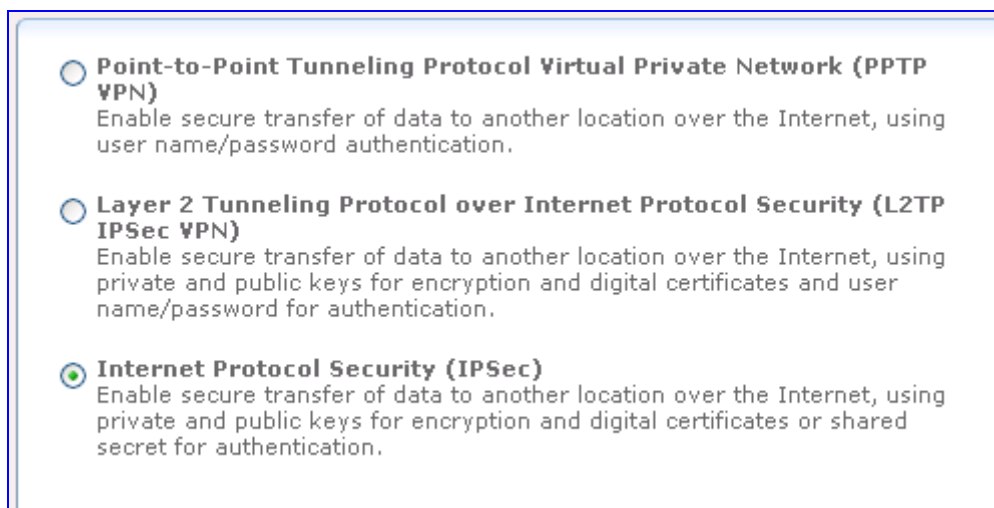
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Connect to a Virtual Private Network over the Internet' option, and then click **Next**.

Figure 3-267: Selecting VPN Type for IPSec



3. Select the 'VPN Client or Point-To-Point' option, and then click **Next**.

Figure 3-268: Selecting IPSec



4. Select the 'Internet Protocol Security Server (IPSec)' option, and then click **Next**.

Figure 3-269: Defining IPSec Properties

Host Name or IP Address of Destination Gateway:

Remote IP:

Encapsulation Type:

Shared Secret:

5. In the 'Host Name or IP Address of Destination Gateway' field, enter the host or IP address of the destination gateway.
6. From the 'Remote IP' drop-down list, select the method for specifying the remote IP address, which serves as the tunnel's endpoint. Use "Same as Gateway" when connecting your LAN to a remote gateway. When connecting your LAN to a remote network (a group of computers beyond a gateway), use one of the remaining three options. Also, use the transport encapsulation type in a gateway-to-gateway scenario only. Upon selection of an option, the screen refreshes providing you with the appropriate fields for entering the data.
 - Same as Gateway – the default option that uses the gateway IP entered above. When selecting this option, you must also select the encapsulation type, tunnel or transport, from its drop-down list.
 - IP Address – a 'Remote IP Address' field appears. Specify the IP address.
 - IP Subnet – 'Remote Subnet IP Address' and 'Remote Subnet Mask' fields appear. Specify these parameters.
 - IP Range – 'From IP Address' and 'To IP Address' fields appear. Specify the IP range.
7. In the 'Shared Secret' field, enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access.
8. Click **Next**; the following is displayed if successfully configured:

Figure 3-270: IPSec Added Successfully

You have successfully completed the steps needed to create the following connection:

- IPSec connection with

☐ Edit the Newly Created Connection

9. Select the 'Edit the Newly Created Connection' check box if you want to edit the new connection after clicking **Finish**.
10. Click **Finish** to save the settings; the new IPSec connection is added to the network connections list.



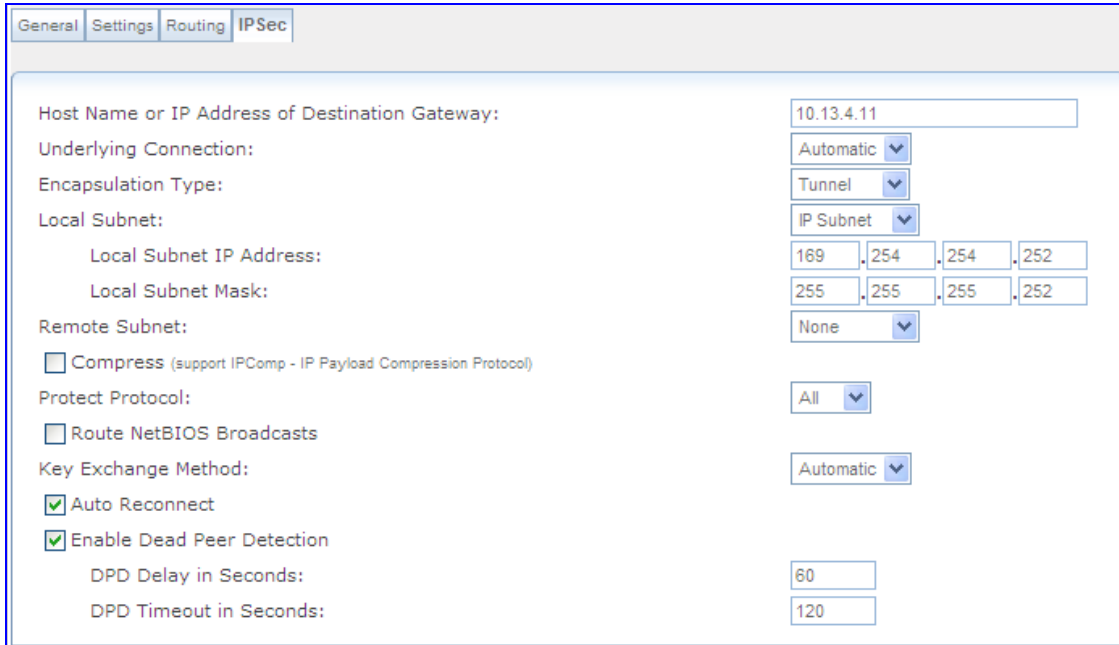
11. To define (edit) additional properties, click the **Edit**  icon corresponding to the **VPN IPSec**  connection in the connection list; the **General**, **Settings**, **Routing**, and **IPSec** tabs appear. For descriptions of the parameters in the **General**, **Settings**, and **Routing** tabs, see "Editing Existing Connections" on page 328. Click the **IPSec** tab; the following appears (only the first part of the page is displayed due to page size):

Figure 3-271: IPSec Tab

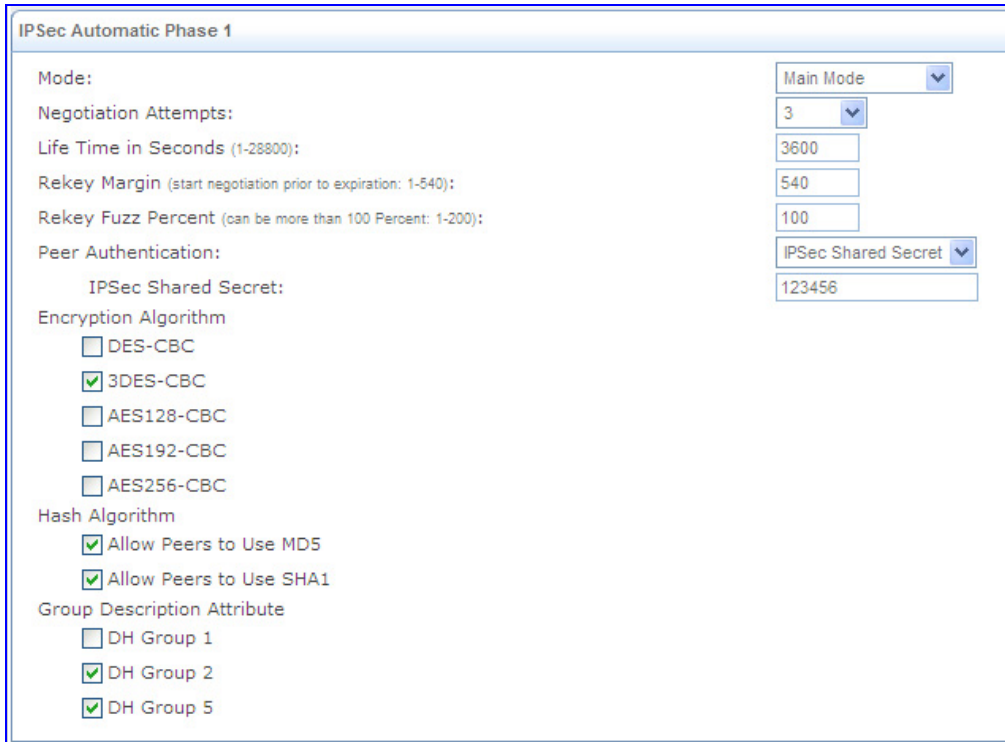


- **Host Name or IP Address of Destination Gateway:** The IP address of your IPSec peer. If your connection is an IPSec Server, this field displays "Any Remote Gateway".
- **Underlying Connection:** In a single WAN scenario, the underlying connection parameter is set to "Automatic" (non-configurable). However, if you have multiple WAN devices, a drop-down list appears, enabling you to choose the underlying WAN device. The IPSec connection only uses your chosen device, unless failover is enabled. In this case, the failed-to device is used instead (assuming its route rules consent), until the chosen device is up again. Note that if you select "Automatic", no attempt is made to return to the original device from the failed-to-device.
- **Encapsulation Type:** Select between 'Tunneling' or 'Transport' encapsulation. 'Transport' encapsulation is performed between two gateways (no subnets), and therefore needs no explicit configuration. 'Tunneling' requires that you configure the following parameters:
 - ◆ **Local Subnet:** Define your local endpoint, by selecting one of the following options:
 - ✓ **IP Subnet (default):** Enter the device's Local Subnet IP Address and Local Subnet Mask.
 - ✓ **IP Range:** Enter the 'From' and 'To' IP addresses, forming the endpoints range of the local subnet(s).
 - ✓ **IP Address:** Enter the Local IP Address to define the endpoint as a single host.
 - ✓ **None:** Select this option if you do not want to define a local endpoint. The endpoint is set to the gateway.

- ◆ **Remote Subnet:** This section is identical to the 'Local Subnet' section above, but is for defining the remote endpoint.
 - ✓ **Compress (Support IPComp protocol):** Select this check box to compress packets during encapsulation with the IP Payload Compression protocol. Note that this reduces performance (and is therefore unchecked by default).
- **Protect Protocol:** Select the protocols to protect with IPSec: All, TCP, UDP, ICMP or GRE. When selecting TCP or UDP, additional source port and destination port drop-down lists appear, enabling you to select 'All' or to specify 'Single' ports in order to define the protection of specific packets. For example, to protect L2TP packets, select UDP and specify 1701 as both single source and single destination ports.
- **Route NetBIOS Broadcasts:** Select this option to allow NetBIOS packets through the IPSec tunnel, which otherwise would not meet the routing conditions specified.
- **Key Exchange Method:** The IPSec key exchange method can be 'Automatic' (default) or 'Manual'. Selecting one of these options alters the rest of the page.
 - ◆ **Automatic key exchange settings:**
 - ✓ **Auto Reconnect:** The IPSec connection reconnects automatically if disconnected for any reason.
 - ✓ **Enable Dead Peer Detection:** The device detects whether the tunnel endpoint has ceased to operate, in which case it terminates the connection. Note that this feature is functional only if the other tunnel endpoint supports it. This is determined during the negotiation phase of the two endpoints.
 - ✓ **DPD Delay in Seconds:** The timeframe in which no traffic has passed through the tunnel. After this timeframe, the device sends a packet to test the tunnel endpoint, expecting a reply.
 - ✓ **DPD Timeout in Seconds:** The timeframe the device waits for the test reply, after which it terminates the connection.

IPSec Automatic Phase 1 – Peer Authentication:

Figure 3-272: IPSec Tab - IPSec Automatic Phase 1



IPSec Automatic Phase 1

Mode: Main Mode

Negotiation Attempts: 3

Life Time in Seconds (1-28800): 3600

Rekey Margin (start negotiation prior to expiration: 1-540): 540

Rekey Fuzz Percent (can be more than 100 Percent: 1-200): 100

Peer Authentication: IPSec Shared Secret

IPSec Shared Secret: 123456

Encryption Algorithm

- ☐ DES-CBC
- ☒ 3DES-CBC
- ☐ AES128-CBC
- ☐ AES192-CBC
- ☐ AES256-CBC

Hash Algorithm

- ☒ Allow Peers to Use MD5
- ☒ Allow Peers to Use SHA1

Group Description Attribute

- ☐ DH Group 1
- ☒ DH Group 2
- ☒ DH Group 5

- ✓ **Mode:** Select the IPSec mode – either 'Main Mode' or 'Aggressive Mode'. Main mode is a secured but slower mode, which presents negotiable propositions according to the authentication algorithms that you select in the check boxes. Aggressive Mode is faster but less secured. When selecting this mode, the algorithm check boxes are replaced by options, presenting strict propositions according to your selections.
- ✓ **Negotiation Attempts:** Select the number of negotiation attempts to be performed in the automatic key exchange method. If all attempts fail, the device waits for a negotiation request.
- ✓ **Life Time in Seconds:** The timeframe in which the peer authentication is valid.
- ✓ **Rekey Margin:** Specifies how long before connection expiry should attempts to negotiate a replacement begin. It is similar to that of the key life time and is given as an integer denoting seconds.
- ✓ **Rekey Fuzz Percent:** Specifies the maximum percentage by which Rekey Margin should be randomly increased to randomize re-keying intervals.
- ✓ **Peer Authentication:** Select the method by which the device authenticates your IPSec peer.
- ✓ **IPSec Shared Secret:** Enter the IPSec shared secret.
 - **RSA Signature** – Enter the peer's RSA signature (based on the device's public key).
 - **Certificate** – If a certificate exists on the device, it appears when you select this option. Enter the certificate's local ID and peer ID.
- ✓ **Encryption Algorithm:** Select the encryption algorithms that the device attempts to use when negotiating with the IPSec peer.

- ✓ **Hash Algorithm:** Select the hash algorithms that the device attempts to use when negotiating with the IPsec peer.
- ✓ **Group Description Attribute:** Select the Diffie-Hellman (DH) group description(s). Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel.

IPsec Automatic Phase 2 – Key Definition:

Figure 3-273: IPsec Tab - IPsec Automatic Phase 2



IPsec Automatic Phase 2

Life Time in Seconds (1-86400):

☐ Use Perfect Forward Secrecy (PFS)

Encryption Algorithm

- ☒ Allow AH Protocol (no encryption)
- ☐ Allow ESP Protocol with Null-Encryption (no encryption)
- ☐ Allow ESP Protocol with DES-CBC Encryption
- ☒ Allow ESP Protocol with 3DES-CBC Encryption
- ☐ Allow ESP Protocol with AES-CBC 128-bit Encryption
- ☐ Allow ESP Protocol with AES-CBC 192-bit Encryption
- ☐ Allow ESP Protocol with AES-CBC 256-bit Encryption

Authentication Algorithm (for ESP protocol)

- ☒ Allow Peers to Use MD5
- ☒ Allow Peers to Use SHA1

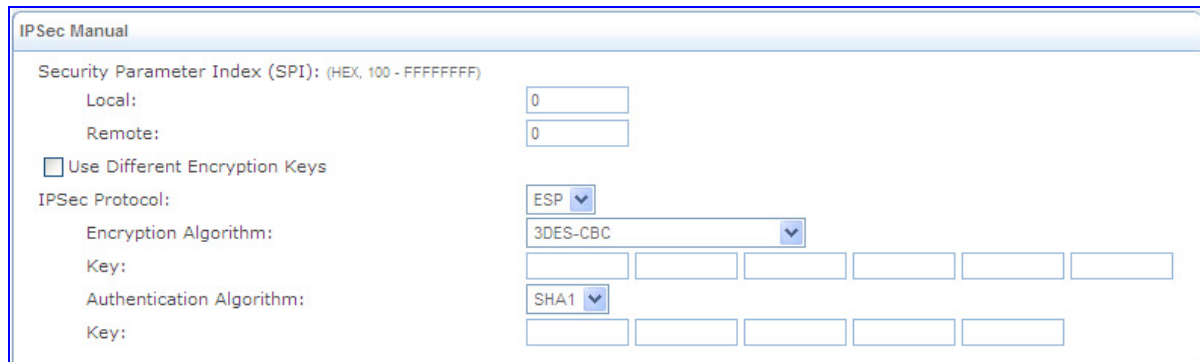
Hash Algorithm (for AH protocol)

- ☒ Allow Peers to Use MD5
- ☒ Allow Peers to Use SHA1

- ✓ **Life Time in Seconds:** The length of time before a security association automatically performs renegotiation.
- ✓ **Use Perfect Forward Secrecy (PFS):** Select whether Perfect Forward Secrecy of keys is required on the connection's keying channel (with PFS, penetration of the key-exchange protocol does not compromise keys negotiated earlier). Deselecting this option hides the next parameter.
 - **Group Description Attribute:** Select whether to use the same group chosen in phase 1, or reselect specific groups.
- ✓ **Encryption Algorithm:** Select the encryption algorithms that the device attempts to use when negotiating with the IPsec peer.
- ✓ **Authentication Algorithm (for ESP protocol):** Select the authentication algorithms that the device attempts to use when negotiating with the IPsec peer.
- ✓ **Hash Algorithm (for AH protocol):** Select the hash algorithms that the device attempts to use when negotiating with the IPsec peer.

◆ **Manual key definition:**

Figure 3-274: IPSec Tab - IPSec Manual



- ✓ **Security Parameter Index (SPI):** A 32 bit value that together with an IP address and a security protocol, uniquely identifies a particular security association. The local and remote values must be coordinated with their respective values on the IPSec peer.
- ✓ **Use Different Encryption Keys:** Selecting this option allows you to define both local and remote algorithm keys when defining the IPSec protocol.
- ✓ **IPSec Protocol:** Select between the ESP and AH IPSec protocols. The page refreshes accordingly:
 - **ESP** – Select the encryption and authentication algorithms, and enter the algorithm keys in hexadecimal representation.
 - **AH** – Select the hash algorithm, and enter the algorithm key in hexadecimal representation.

12. Click **OK** to save the settings.

3.3.3.9.11 Internet Protocol Security Server (IPSec Server)

The below procedure describes how to create an IPSec server.

➤ **To create an IPSec server connection:**


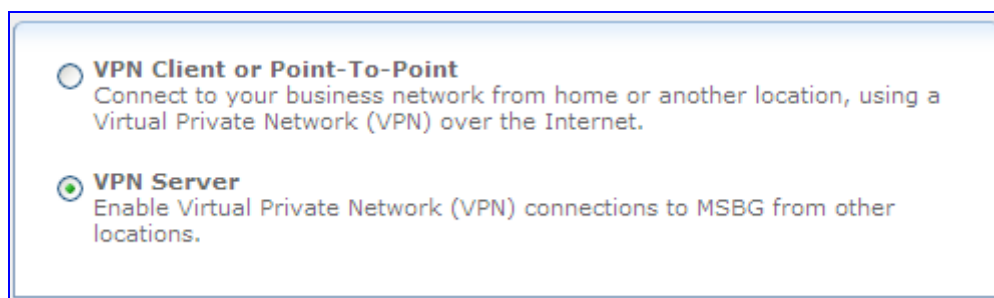
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Connect to a Virtual Private Network over the Internet' option, and then click **Next**.

Figure 3-275: VPN Connection Type



3. Select the 'VPN Server' option, and then click **Next**.

Figure 3-276: VPN Protocols



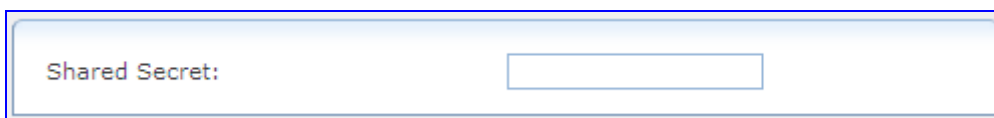
☐ **Point-to-Point Tunneling Protocol Server (PPTP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.

☐ **Layer 2 Tunneling Protocol Server (L2TP Server)**
Enable Virtual Private Network (VPN) connections to your home network from other locations.

☒ **Internet Protocol Security Server (IPSec Server)**
Enable secure connections to MSBG from other locations, using private and public keys for encryption and digital certificates or shared secret for authentication.

4. Select the 'Internet Protocol Security Server (IPSec Server)' option, and then click **Next**.

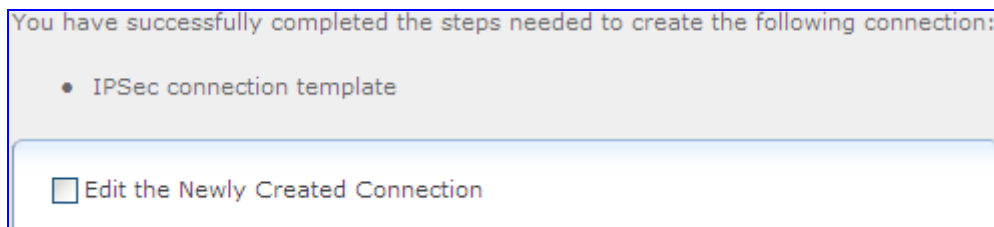
Figure 3-277: IPSec Shared Secret Key



Shared Secret:

5. Enter the IPSec shared secret, which is the encryption key jointly decided upon with the network you are trying to access, and then click **Next**; the following is displayed if successfully configured:

Figure 3-278: IPSec Connection Added Successfully



You have successfully completed the steps needed to create the following connection:

- IPSec connection template

☐ Edit the Newly Created Connection

6. Select the 'Edit the Newly Created Connection' check box if you want to edit the new connection after clicking **Finish**.
7. Click **Finish** to save the settings; the new IPSec Server is added to the network connections list.

3.3.3.9.12 Internet Protocol over Internet Protocol (IPIP)

The device allows you to create an IPIP tunnel to another router, by encapsulating IP packets in IP. This tunnel can be managed as any other network connection. Supported by many routers, this protocol enables using multiple network schemes. Note, however, that IPIP tunnels are not secured.

➤ **To create an IPIP tunnel:**


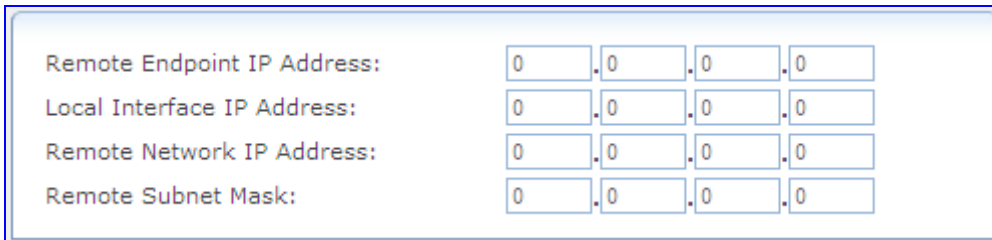
1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Advanced Connection' option, and then click **Next**; the 'Advanced Connection' page appears.
3. Select the 'Internet Protocol over Internet Protocol (IPIP)' option, and then click **Next**; the following page appears.

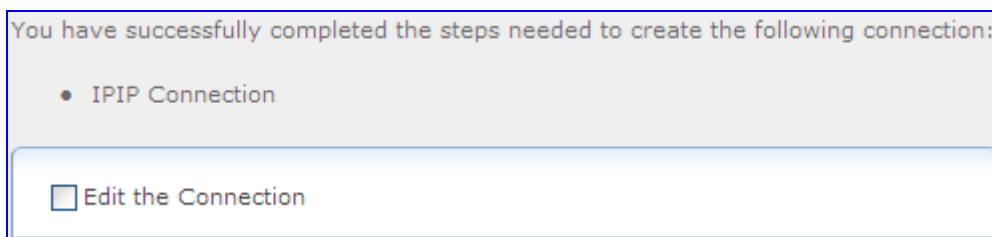
Figure 3-279: Configuring General IPIP Parameters



Remote Endpoint IP Address:	0	0	0	0
Local Interface IP Address:	0	0	0	0
Remote Network IP Address:	0	0	0	0
Remote Subnet Mask:	0	0	0	0

4. In the 'Remote Endpoint IP Address' field, enter the tunnel's remote endpoint IP address.
5. In the 'Local Interface IP Address' field, enter the local IP address for the interface.
6. In the 'Remote Network IP Address' and 'Remote Subnet Address' fields, enter the IP address and subnet mask (respectively) of the remote network that is to be accessed via the tunnel, and then click **Next**; the following message is displayed if successfully configured:

Figure 3-280: IPIP Added Successfully



You have successfully completed the steps needed to create the following connection:

- IPIP Connection

☐ Edit the Connection

7. Select the 'Edit the Connection' check box if you want to edit the new connection after clicking **Finish**.
8. Click **Finish** to save the settings; the new IPIP tunnel is added to the network connections list.

➤ **To edit the IPIP tunnel connection:**

1. In the 'Connections' page, click the "WAN IPIP" link; the **General** tab appears displaying general properties.
2. Select the **Settings** tab to edit various settings (see "Editing Existing Connections" on page 328).

3. Select the **Routing** tab to edit the routing parameters (see "Editing Existing Connections" on page 328).
4. Select the **IPIP** tab to define the tunnels's remote endpoint IP address.

Figure 3-281: IPIP Tab

5. Select the **Advanced** tab to enable the firewall for this network connection (see "Editing Existing Connections" on page 328).

3.3.3.9.13 General Routing Encapsulation (GRE)

The device allows you to create a GRE tunnel to transport multicast traffic and IPv6, in addition to other existing tunneling capabilities (e.g. IPIP, L2TP, and PPTP).

➤ **To create a new GRE tunnel:**


1. In the 'Connections' page, click the **New**  icon; the Connection Wizard opens.
2. Select the 'Advanced Connection' option, and then click **Next**; the 'Advanced Connection' page appears.
3. Select the 'General Routing Encapsulation (GRE)' option, and then click **Next**; the following page appears.

Figure 3-282: Configuring General IPIP Parameters

4. In the 'Remote Endpoint IP Address' field, enter the tunnel's remote endpoint IP address.
5. In the 'Local Interface IP Address' field, enter the local IP address for the interface.
6. In the 'Remote Network IP Address' and 'Remote Subnet Address' fields, enter the IP address and subnet mask (respectively) of the remote network that is to be accessed via the tunnel, and then click **Next**; the following GRE connection message is displayed if successfully configured:

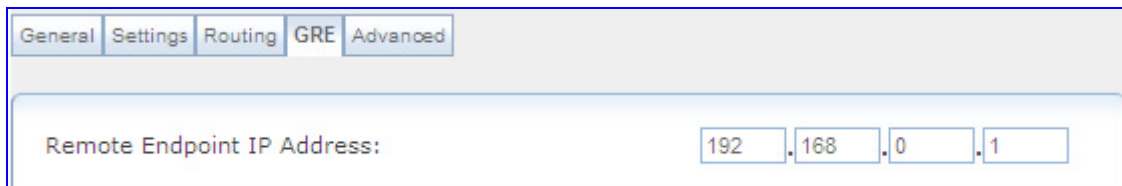
Figure 3-283: GRE Connection Successfully Added

7. Select the 'Edit the Connection' check box if you want to edit the new connection after clicking **Finish**.
8. Click **Finish** to save the settings; the new GRE tunnel is added to the network connections list.

➤ **To edit the GRE tunnel connection:**

1. In the 'Connections' page, click the "WAN GRE" link; the **General** tab appears displaying general properties.
2. Select the **Settings** tab to edit various settings (see "Editing Existing Connections" on page 328).
3. Select the **Routing** tab to edit the routing parameters (see "Editing Existing Connections" on page 328).
4. Select the **GRE** tab to define the tunnel's remote endpoint IP address.

Figure 3-284: Editing GRE Remote Endpoint IP Address



The screenshot shows a configuration window with five tabs: General, Settings, Routing, GRE, and Advanced. The GRE tab is selected. Below the tabs, there is a label 'Remote Endpoint IP Address:' followed by four input fields containing the values 192, 168, 0, and 1, separated by dots.

5. Select the **Advanced** tab to enable the firewall for this network connection (see "Editing Existing Connections" on page 328).

3.3.3.9.13.1 GRE Example Scenario

The following example demonstrates the usage of a GRE interface to communicate between two hosts located on different LANs, behind separate MSBG devices.



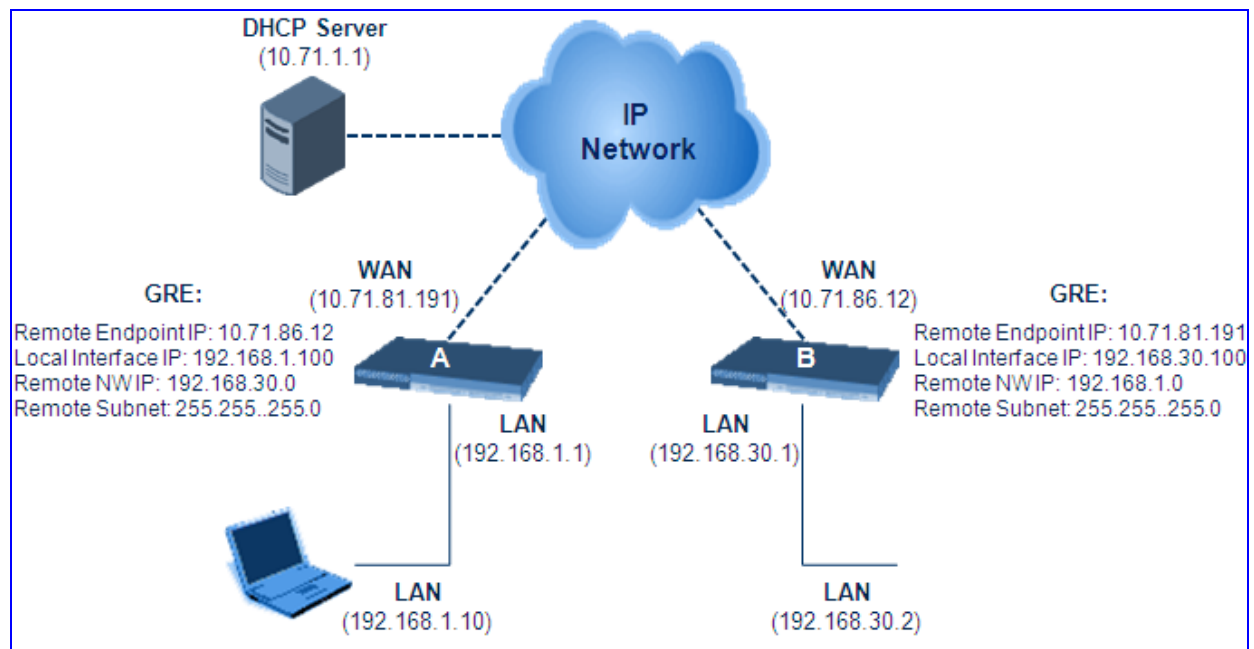
Note: A GRE tunnel is an unsecured (unencrypted) tunnel. Safety measures must be taken when setting up such a tunnel.

This example includes the following setup:

- Two devices:
 - "A" - WAN IP address is 10.71.81.191; LAN IP address is 192.168.1.1
 - "B" - WAN IP address is 10.71.86.12; LAN IP address is 192.168.30.1
- Two LAN hosts
- A WAN host serving as a DHCP server
- Each LAN host is connected to a LAN port on a different device

- The devices' WAN ports are connected to the WAN (where the DHCP server is available)

Figure 3-285: Example Scenario Setup



To create a tunnel, each MSBG device must be made aware of the other's WAN IP address (the information must be exchanged).

➤ **To configure a GRE tunnel:**


1. Create a GRE tunnel for device "A":
 - a. In the 'Connections' page, click the **New**  icon.
 - b. Select the 'Advanced Connection' option, and then click **Next**.
 - c. Select the 'General Routing Encapsulation (GRE)' option, and then click **Next**.

Figure 3-286: Defining GRE Tunnel for Device A

Remote Endpoint IP Address:	10	71	86	12
Local Interface IP Address:	192	168	1	100
Remote Network IP Address:	192	168	30	0
Remote Subnet Mask:	255	255	255	0

- d. Enter 10.71.86.12 as the tunnel's remote endpoint IP address.
- e. Enter 192.168.1.100 as the local interface IP address.
- f. Enter 192.168.30.0 as the IP address of the remote network that will be accessed via the tunnel, and 255.255.255.0 as the subnet mask.
- g. Click **Next**, and then click **Finish**.


2. Create a GRE tunnel for device "B":
 - a. In the 'Connections' page, click the **New**  icon.
 - b. Select the 'Advanced Connection' option, and then click **Next**.
 - c. Select the 'General Routing Encapsulation (GRE)' option, and then click **Next**.

Figure 3-287: Defining GRE Tunnel for Device B

Remote Endpoint IP Address:	10	71	81	191
Local Interface IP Address:	192	168	30	100
Remote Network IP Address:	192	168	1	0
Remote Subnet Mask:	255	255	255	0

- d. Enter 10.71.81.191 as the tunnel's remote endpoint IP address.
 - e. Enter 192.168.30.100 as the local interface IP address.
 - f. Enter 192.168.1.0 as the IP address of the remote network that will be accessed via the tunnel, and 255.255.255.0 as the subnet mask.
 - g. Click **Next**, and then click **Finish**.
3. Running the Scenario: After verifying that each host has properly received an IP address in the subnet of its respective device, send a ping from host "A" (192.168.1.10) to host "B" (192.168.30.2). If the GRE connection is successful, host "B" should reply.

3.3.3.9.14 Editing Existing Connections

As many of the configuration parameters for the different connection types are similar, the basic procedure for editing the connections is described in summary below. Editing connections allows you to configure additional parameters that do not appear when initially creating new connections.



Note: Tabs specific to the connection type are described in later sections relevant to that connection type.

➤ **To edit connections:**

1. Access the configuration tabs:


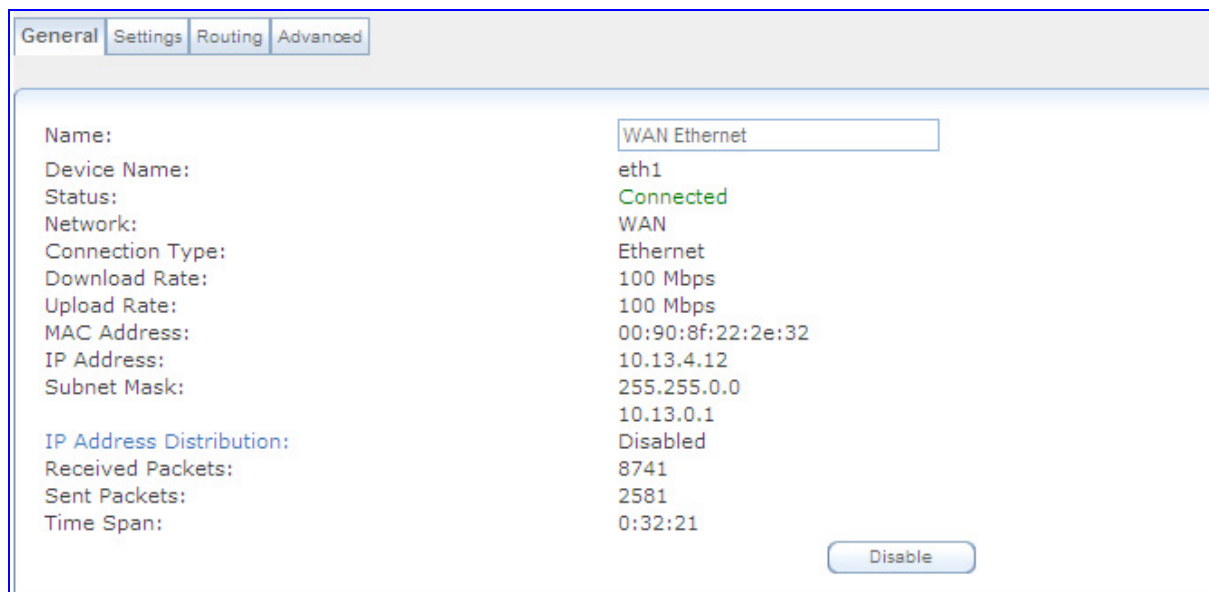
- In the 'Connections' page, click the **Edit**  icon corresponding to the network connection that you want to edit; the **General** tab is displayed, showing general properties of the connection type (e.g., WAN Ethernet connection).
- From the WAN Access page (see "WAN Access Settings" on page 224), click the **Click here for Advanced Settings** link.

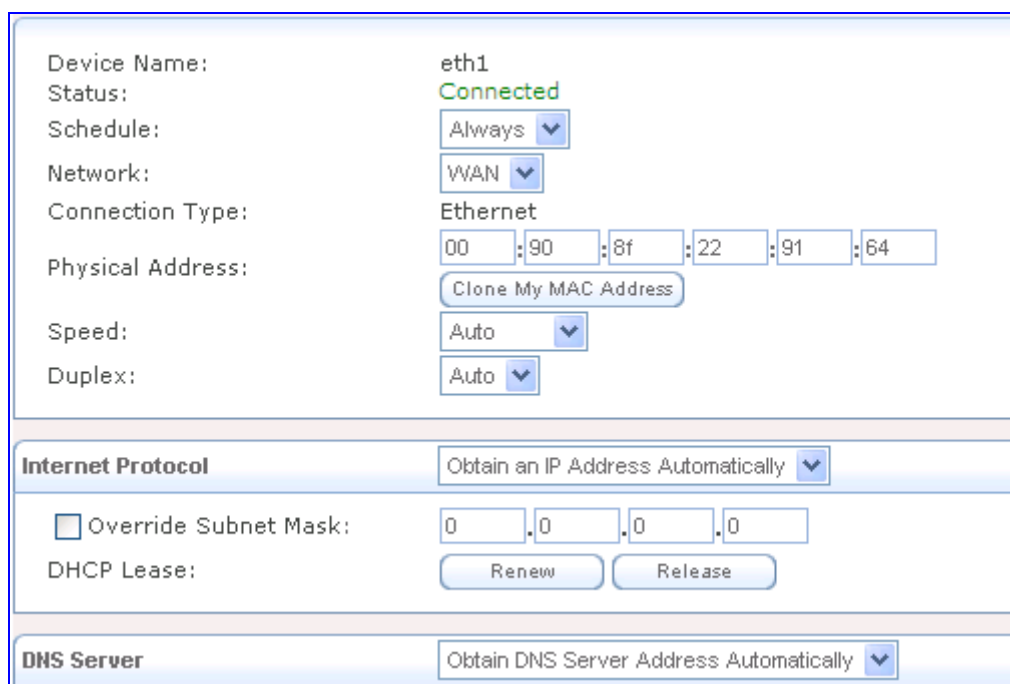
Figure 3-288: Editing Network Connection - General Tab



General Settings Routing Advanced	
Name:	WAN Ethernet
Device Name:	eth1
Status:	Connected
Network:	WAN
Connection Type:	Ethernet
Download Rate:	100 Mbps
Upload Rate:	100 Mbps
MAC Address:	00:90:8f:22:2e:32
IP Address:	10.13.4.12
Subnet Mask:	255.255.0.0
IP Address Distribution:	Disabled
Received Packets:	8741
Sent Packets:	2581
Time Span:	0:32:21
Disable	

2. Select the **Settings** tab:

Figure 3-289: Editing Network Connection - Settings Tab



Device Name:	eth1
Status:	Connected
Schedule:	Always
Network:	WAN
Connection Type:	Ethernet
Physical Address:	00:90:8f:22:2e:32
Speed:	Auto
Duplex:	Auto
Internet Protocol: Obtain an IP Address Automatically	
<input type="checkbox"/> Override Subnet Mask:	0.0.0.0
DHCP Lease:	Renew Release
DNS Server: Obtain DNS Server Address Automatically	

- **Schedule:** by default, the connection is always active. However, if you have defined scheduler rules (see "Configuring Scheduler Rules" on page 285), you can select one of these (time segments during which the connection is active).
 - **Network:** select whether the parameters you are configuring relate to a WAN, LAN or DMZ connection.
 - **Physical Address:** physical address of the network card used for your network. Some cards allow you to change this address.
 - **Speed:** select the transmission speed of the network interface (10Base-T, 100Base-T, 1000Base-T, or autonegotiation).
Note: This is applicable only to the WAN Ethernet port.
 - **Duplex:** select the duplex mode (half-duplex, full-duplex, or autonegotiation).
Note: This is applicable only to the WAN Ethernet port.
 - **MTU:** Maximum Transmission Unit - specifies the largest packet size permitted for Internet transmission. By default ('Automatic'), the device selects the best MTU for your Internet connection. Select 'Automatic by DHCP' to have the DHCP determine the MTU. If you select 'Manual', it is recommended to enter a value in the 1200 to 1500 range.
 - **Internet Protocol:** select one of the following Internet protocol options from the 'Internet'
 - ◆ No IP Address - select this option if you require that your device have no IP address. This can be useful if you are working in an environment where you are not connected to other networks, such as the Internet.
 - ◆ Obtain an IP Address Automatically - your connection is configured by default to act as a DHCP client. You should keep this configuration in case your service provider supports DHCP, or if you are connecting using a dynamic IP address. The server that assigns the device with an IP address, also assigns a subnet mask. You can override the dynamically assigned subnet mask by selecting the 'Override Subnet Mask' check box and specifying your own mask instead. You can click the **Release** button to release the current leased IP address. Once the address has been released, the button text changes to **Renew**. Use this button to renew the leased IP address.
 - ◆ Use the Following IP Address - your connection can be configured using a permanent (static) IP address. Your service provider should provide you with such an IP address and subnet mask.
 - **DNS Server:** Domain Name System (DNS) is the method by which Web site domain names are translated into IP addresses:
 - ◆ Obtain DNS Server Address Automatically - configure the connection to automatically obtain a DNS server address, or specify such an address manually, according to the information provided by your ISP.
 - ◆ Use the Following DNS Server Addresses - manually configure DNS server addresses. You can specify up to two different DNS server addresses, one primary, another secondary.
3. Click **OK** to save the settings.

4. Select the **Routing** tab:

Figure 3-290: Editing Network Connection - Routing Tab

Routing Mode: Route

Device Metric: 4

☐ Default Route

☒ Multicast - IGMP Proxy Internal

IGMP Query Version: IGMPv3

☐ Routing Information Protocol (RIP)

Routing Table

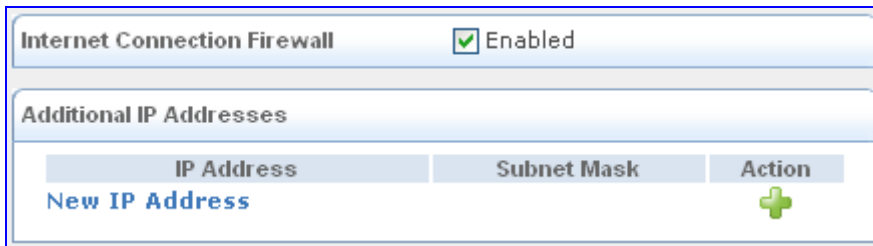
Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						


You can choose to setup your device to use static or dynamic routing. Dynamic routing automatically adjusts how packets travel on the network, whereas static routing specifies a fixed routing path to destinations.

- **Routing Mode:** select one of the following routing modes:
 - ◆ Route: the device functions as a router between two networks.
 - ◆ NAPT: Network Address and Port Translation (NAPT) refers to network address translation involving the mapping of port numbers, allowing multiple hosts to share a single IP address. Use NAPT if your LAN encompasses multiple devices, a topology that necessitates port translation in addition to address translation.
- **Device Metric:** a value used by the device to determine whether one route is superior to another, considering parameters such as bandwidth and delay.
- **Default Route:** defines this device as a the default route.
- **Multicast – IGMP Proxy Internal:** the device serves as an IGMP proxy, issuing IGMP host messages on behalf of its LAN hosts. This check box is enabled on LAN connections by default, meaning that if a LAN multicast server is available, other LAN hosts asking to join multicast groups (by sending IGMP requests) are able to join its multicast group. However, this check box is disabled on the WAN connection by default, meaning that LAN hosts are unable to join multicast groups of WAN multicast servers.
 - ◆ IGMP Query Version - the device supports all three versions of IGMP. Select the version you would like to use. Note that this drop-down list appears for LAN connections only.
- **Routing Information Protocol (RIP):** enables the Routing Information Protocol (RIP). RIP determines a route based on the smallest hop count between source and destination. When RIP is enabled, select the following:
 - ◆ Listen to RIP Messages - select 'None', 'RIPv1', 'RIPv2' or 'RIPv1/2'.
 - ◆ Send RIP Messages - select 'None', 'RIPv1', 'RIPv2 - Broadcast' or 'RIPv2 - Multicast'.
- **Routing Table:** allows you to add or modify routes when this host is active. Use the **New Route** link to add a route or edit existing routes. To learn more about this feature, see "Routing Settings" on page 276.

5. Click **OK** to save the settings.
6. Select the **Advanced** tab:

Figure 3-291: Editing Network Connection - Advanced Tab



Internet Connection Firewall		<input checked="" type="checkbox"/> Enabled
Additional IP Addresses		
IP Address	Subnet Mask	Action
New IP Address		

- **Internet Connection Firewall:** Your device's firewall helps protect your computer by preventing unauthorized users from gaining access to it through a network such as the Internet. The firewall can be activated per network connection. To enable the firewall on this network connection, select the 'Enabled' check box.
 - **Additional IP Addresses:** You can add alias names (additional IP addresses) to the device by clicking the **New IP Address** link. This enables you to access the device using these aliases (in addition to the default 192.168.1.1).
7. Click **OK** to save the settings.

3.4 Maintenance Tab

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

- Maintenance (see "Maintenance" on page 333)
- Software Update (see "Software Update" on page 337)

3.4.1 Maintenance

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

- Maintenance Actions (see "Maintenance Actions" on page 333)

3.4.1.1 Maintenance Actions

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

- Reset the device (see "Resetting the Device" on page 334)
- Lock and unlock the device (see "Locking and Unlocking the Device" on page 335)
- Save configuration to the device's flash memory (see "Saving Configuration" on page 336)

➤ To access the 'Maintenance Actions' page:

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

Figure 3-292: 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"/>

3.4.1.1.1 Resetting the Device

The 'Maintenance Actions' page allows you to remotely reset the device. In addition, before resetting the device, you can choose the following options:

- Save the device's current configuration to the device's flash memory (non-volatile).
- Perform a graceful shutdown, i.e., device reset starts only after a user-defined time (i.e., timeout) or after no more active traffic exists (the earliest thereof).



Notes:

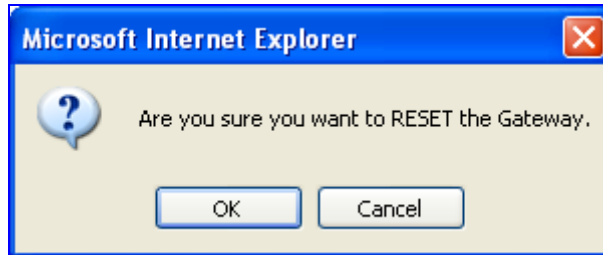
- Throughout the Web interface, parameters preceded by the lightning ⚡ symbol are not applied on-the-fly and require that you reset the device for them to take effect.
- When you modify parameters that require a device reset, once you click the **Submit** button in the relevant page, the toolbar displays the word "Reset" (see "Toolbar" on page 44) to indicate that a device reset is required.
- Upon reboot, the device restores the settings from its configuration file. However, if reboot attempts fail three times consecutively, the device resets the configuration file by restoring factory defaults before attempting to reboot.

➤ To reset the device:

1. Open the 'Maintenance Actions' page (see "Maintenance Actions" on page 333).
2. Under the 'Reset Configuration' group, from the 'Burn To FLASH' drop-down list, select one of the following options:
 - 'Yes': The device's current configuration is saved (*burned*) to the flash memory prior to reset (default).
 - 'No': Resets the device without saving the current configuration to flash (discards all unsaved modifications).
3. Under the 'Reset Configuration' group, from the 'Graceful Option' drop-down list, select one of the following options:
 - 'Yes': Reset starts only after the user-defined time in the 'Shutdown Timeout' field (see Step 4) expires or after no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
 - 'No': Reset starts regardless of traffic, and any existing traffic is terminated at once.
4. In the 'Shutdown Timeout' field (relevant only if the 'Graceful Option' in the previous step is set to 'Yes'), enter the time after which the device resets. Note that if no traffic exists and the time has not yet expired, the device resets.

5. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.

Figure 3-293: Reset Confirmation Message Box



6. Click **OK** to confirm device reset; if the parameter 'Graceful Option' is set to 'Yes' (in Step 3), the reset is delayed and a screen displaying the number of remaining calls and time is displayed. When the device begins to reset, a message appears notifying you of this.

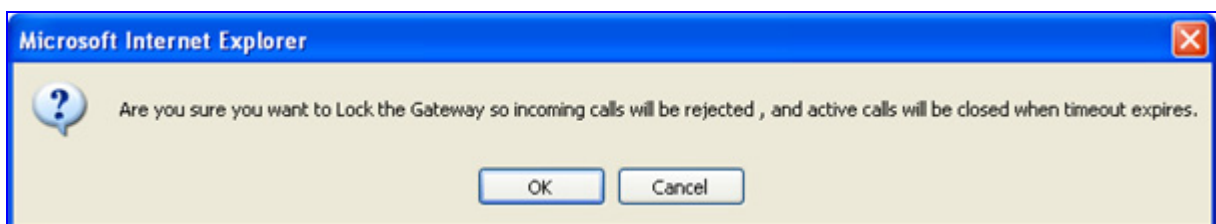
3.4.1.1.2 Locking and Unlocking the Device

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

➤ To lock the device:

1. Open the 'Maintenance Actions' page (see "Maintenance Actions" on page 333).
 2. Under the 'LOCK / UNLOCK' group, from the 'Graceful Option' drop-down list, select one of the following options:
 - 'Yes': The device is 'locked' only after the user-defined time in the 'Lock Timeout' field (see Step 3) expires or no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
 - 'No': The device is 'locked' regardless of traffic. Any existing traffic is terminated immediately.
- Note:** These options are only available if the current status of the device is in the Unlock state.
3. In the 'Lock Timeout' field (relevant only if the parameter 'Graceful Option' in the previous step is set to 'Yes'), enter the time (in seconds) after which the device locks. Note that if no traffic exists and the time has not yet expired, the device locks.
 4. Click the **LOCK** button; a confirmation message box appears requesting you to confirm device Lock.

Figure 3-294: 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 333).
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).

3.4.1.1.3 Saving Configuration

The 'Maintenance Actions' page allows you to save (*burn*) the current parameter configuration (including loaded auxiliary files) to the device's *non-volatile* memory (i.e., flash). The parameter modifications that you make throughout the Web interface's pages are temporarily saved (to the *volatile* memory - RAM) when you click the **Submit** button on these pages. Parameter settings that are saved only to the device's RAM, revert to their previous settings after a hardware/software reset (or power failure). Therefore, to ensure that your configuration changes are retained, you must save them to the device's flash memory using the burn option described below.

➤ **To save the changes to the non-volatile flash memory :**

1. Open the 'Maintenance Actions' page (see "Maintenance Actions" on page 333).
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 335).
- 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 334).
- The Home page's General Information pane displays whether the device is currently "burning" the configuration (see "Using the Home Page" on page 59).

3.4.2 Software Update

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

- Load Auxiliary Files (see "Loading Auxiliary Files" on page [337](#))
- Software Upgrade Key (see "Loading Software Upgrade Key" on page [339](#))
- Software Upgrade Wizard (see "Software Upgrade Wizard" on page [341](#))
- Configuration File (see "Backing Up and Loading Configuration File" on page [344](#))

3.4.2.1 Loading Auxiliary Files

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

Table 3-41: Auxiliary Files Descriptions

File	Description
INI	Provisions the device's parameters. The Web interface enables practically full device provisioning, but customers may occasionally require new feature configuration parameters in which case this file is loaded. Note: Loading this file only provisions those parameters that are included in the <i>ini</i> file. For a detailed description on the <i>ini</i> file, see "INI File-Based Management" on page 367 .
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 a detailed description on CAS files, see CAS Files on page 399 .
Call Progress Tones	This is a region-specific, telephone exchange-dependent file that contains the Call Progress Tones (CPT) levels and frequencies for the device. The default CPT file is U.S.A. For a detailed description of the CPT file, see "Call Progress Tones File" on page 393 .
Prerecorded Tones	The Prerecorded Tones (PRT) file enhances the device's capabilities of playing a wide range of telephone exchange tones that cannot be defined in the CPT file. For a detailed description of the PRT file, see "Prerecorded Tones File" on page 399 .
Dial Plan	This file contains dialing plans, used by the device, for example, to know when to stop collecting the dialed digits and start sending them on. For a detailed description of the Dial Plan file, see Dial Plan File on page 400 .
User Info	The User Information file maps PBX extensions to IP numbers. This file can be used to represent PBX extensions as IP phones in the global 'IP world'. For a detailed description of the User Info file, see "User Information File" on page 402 .


Notes:

- You can schedule automatic loading of updated auxiliary files using HTTP/HTTPS (for more details, refer to the *Product Reference Manual*).
- For a detailed description on auxiliary files, see "Auxiliary Configuration Files" on page 393.
- 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 335).
- For deleting auxiliary files, see "Viewing Device Information" on page 346.


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

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

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

Figure 3-295: Load Auxiliary Files Page



INI file (incremental)	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Load File"/>
Voice Prompts file	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Load File"/>
 Call Progress Tones file	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Load File"/>
Prerecorded Tones file	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Load File"/>
Dial Plan file	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Load File"/>
User Info file	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Load 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 336 and reset the device (if you have loaded a Call Progress Tones file), see "Resetting the Device" on page 334.

3.4.2.2 Loading Software Upgrade Key

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

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

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

- Web interface
- AudioCodes' EMS (refer to *EMS User's Manual* or *EMS Product Description*)



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

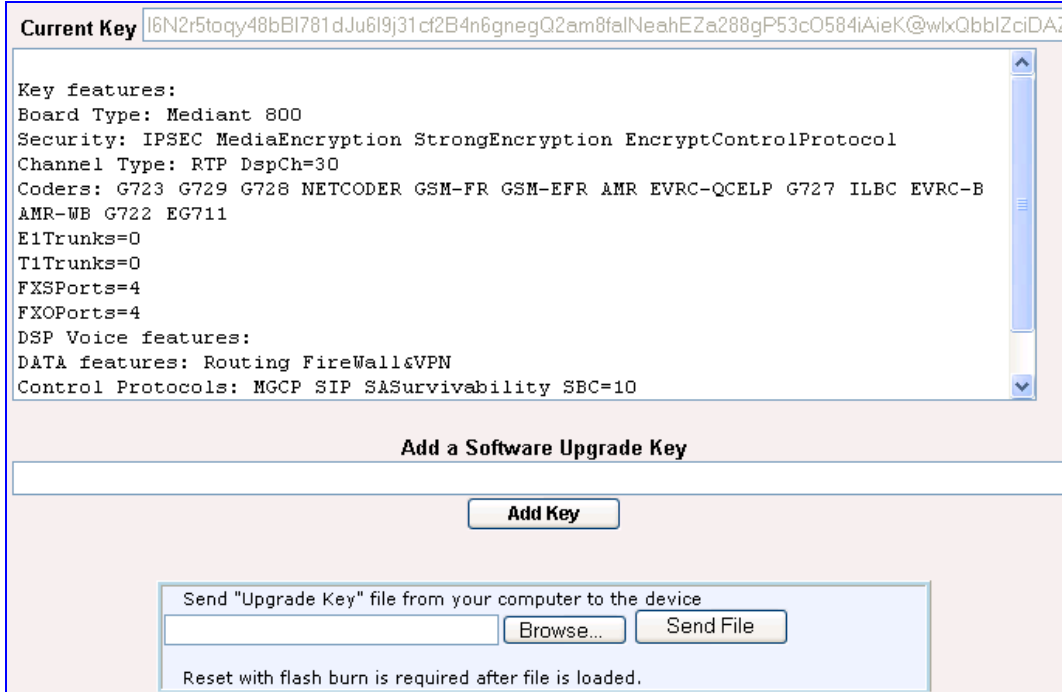


Note: The Software Upgrade Key is an encrypted key.

➤ **To load a Software Upgrade Key:**

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

Figure 3-296: Software Upgrade Key Status Page



Current Key |6N2r5toqy48bBI781dJu6I9j31cf2B4n6gnegQ2am8falNeahEZa288gP53cO584iAieK@wIxQbbIzciDAz|

Key features:
Board Type: Mediant 800
Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
Channel Type: RTP DspCh=30
Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B
AMR-WB G722 EG711
E1Trunks=0
T1Trunks=0
FXSPorts=4
FXOPorts=4
DSP Voice features:
DATA features: Routing FireWall&VPN
Control Protocols: MGCP SIP SASurvivability SBC=10

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 346).
4. Follow one of the following procedures, depending on whether you are loading a single or multiple key S/N lines:
 - **Single key S/N line:**
 - a. Open the Software Upgrade Key text file (using, for example, Microsoft® Notepad).
 - b. Select and copy the key string and paste it into the field 'Add a Software Upgrade Key'.
 - c. Click the **Add Key** button.

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

Figure 3-297: Software Upgrade Key with Multiple S/N Lines



```
sample.ini - Notepad
File Edit Format Help
[LicenseKeys]
.Board Type 29
S/N241182 =
okRTr5topwYMBIZd4NN2a3Qhm4NjIidaagUyehso94APbBF85hF4by0cmQZf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF894Zx
S/N242519 = tmxTr5to0mIMbIZdoPd2a3Qh9zJlIdafilyehsogOQPbBF8pi4by0c9pdl2B8eOoze7JQgywSa5h6o391aOkeTlIAAddF8c6Fx
S/N226403 = tmxTr5to0lsmBIZdoOB2a3Qh9yJlIdafilyehsogN4PbBF8piZ4by0c9pdl2B8eOoze7JQgxgSa5h6o2x1aOkeTlIAAddF8c6Fx
S/N226417 = r6xTr5to25sMBIZdfiB2a3Qh5OJlIda92lyehsoix4PbBF8eOZ4by0c52df2B88yoze7JQlNgSa5h6fyx1aOkeXZlIAAddF8amFx
.Board Type 24
S/N241182 =
okRTr5topwYMBIZd4NN2a3wkm4NjIidaagUyehso94APbBF85hF4by0cmQZf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF8938s
S/N242519 = tmxTr5to0mIMbIZdoPd2a3wk9zJlIdafilyehsogOQPbBF8pi4by0c9pdl2B8eOoze7JQgywSa5h6o391aOkeTlIAAddF8c1ss
S/N226403 = tmxTr5to0lsmBIZdoOB2a3wk9yJlIdafilyehsogN4PbBF8piZ4by0c9pdl2B8eOoze7JQgxgSa5h6o2x1aOkeTlIAAddF8c1ss
S/N226417 = r6xTr5to25sMBIZdfiB2a3wk5OJlIda92lyehsoix4PbBF8eOZ4by0c52df2B88yoze7JQlNgSa5h6fyx1aOkeXZlIAAddF8ahss
```

- In the 'Send Upgrade Key file' field, click the **Browse** button and navigate to the folder in which the Software Upgrade Key text file is located on your PC.
 - Click the **Send File** button; the new key is loaded to the device and validated. If the key is valid, it is burned to memory and displayed in the 'Current Key' field.
- 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.

3.4.2.3 Software Upgrade Wizard

The Software Upgrade Wizard allows you to upgrade the device's firmware (compressed *cmp* file) as well as load an *ini* file and/or auxiliary files (typically loaded using the 'Load Auxiliary File' page described in "Loading Auxiliary Files" on page 337). However, it is mandatory when using the wizard to first load a *cmp* file to the device. You can then choose to also load an *ini* file and/or auxiliary files, but this cannot be done without first loading a *cmp* file. For the *ini* and each auxiliary file type, you can choose to load a new file or not load a file but use the existing file (i.e., maintain existing configuration) running on the device.



Warning: The Software Upgrade Wizard requires the device to be reset at the end of the process, which may disrupt traffic. To avoid this, disable all traffic on the device before initiating the wizard, by performing a graceful lock (see Saving and Resetting the Device).



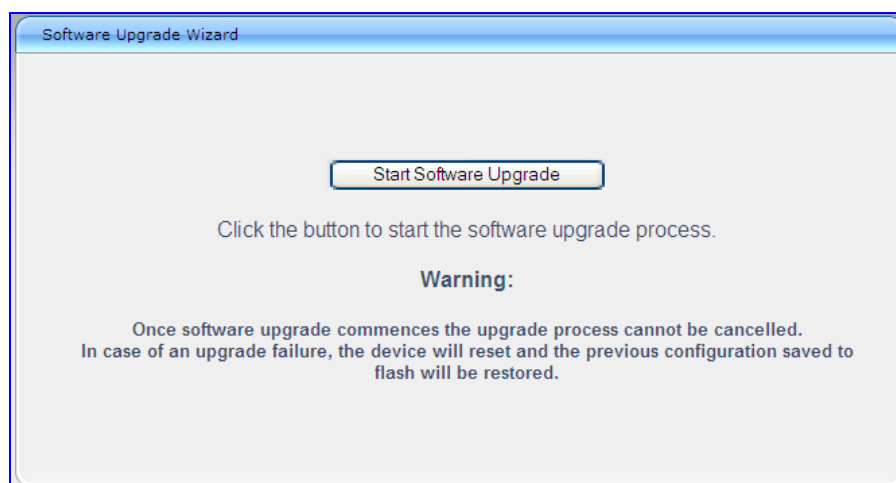
Notes:

- Before upgrading the device, it is recommended that you save a copy of the device's configuration settings (i.e., *ini* file and data 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 344.
- Before you can load an *ini* or auxiliary file, you must first load a *cmp* file.
- When you activate the wizard, the rest of the Web interface is unavailable. After the files are successfully loaded, access to the full Web interface is restored.
- If you upgraded your *cmp* and the "SW version mismatch" message appears in the Syslog or Web interface, then your Software Upgrade Key does not support the new *cmp* version. Contact AudioCodes support for assistance.
- If you use the wizard to load an *ini* file, parameters excluded from the *ini* file are assigned default values (according to the *cmp* file running on the device), thereby, overriding values previously defined for these parameters.
- You can schedule automatic loading of these files using HTTP/HTTPS (refer to the *Product Reference Manual*).

➤ **To load files using the Software Upgrade Wizard:**


1. Stop all traffic on the device using the Graceful Lock feature (refer to the warning bulletin above).
2. Open the 'Software Upgrade Wizard' (**Maintenance** tab > **Software Update** menu > **Software Upgrade Wizard**); the 'Software Upgrade Wizard' page appears.


Figure 3-298: Start Software Upgrade Wizard Screen



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








Note: At this stage, you can quit the Software Update Wizard, by clicking **Cancel** , without requiring a device reset. However, once you start uploading a cmp file, the process must be completed with a device reset. If you choose to quit the process in any of the subsequent pages, the device resets.

- Click the **Browse** button, navigate to the *cmp* file, and then click **Send File**; a progress bar appears displaying the status of the loading process. When the cmp file is successfully loaded to the device, a message appears notifying you of this.
- 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).

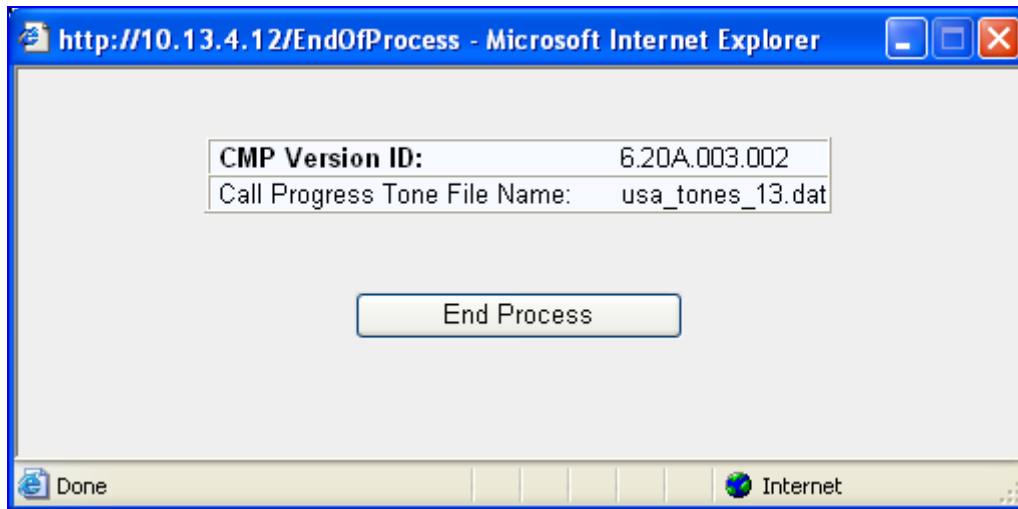
- Click the **Next**  button; the wizard page for loading an *ini* file appears. You can now perform one of the following:
 - Load a new *ini* file: Click **Browse**, navigate to the *ini* file, and then click **Send File**; the *ini* file is loaded to the device and you're notified as to a successful 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.
- 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.
- 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).
- Click the **Reset**  button to complete the upgrade process; the device 'burns' the newly loaded files to flash memory and then resets the device.



Note: Device reset may take a few minutes (depending on cmp file version, this may even take up to 30 minutes).

After the device resets, the 'End Process' screen appears displaying the burned configuration files:

Figure 3-299: End Process Wizard Page



10. Click **End Process** to close the wizard; the Web Login dialog box appears.
11. Enter your login user name and password, and then click **OK**; a message box appears informing you of the new cmp file.
12. Click **OK**; the Web interface becomes active, reflecting the upgraded device.

3.4.2.4 Backing Up and Loading Configuration File

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



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

➤ **To save the ini / data file:**

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

Figure 3-300: Configuration File Page

Configuration File

Save the **INI** file to the PC.

Send the **INI** file to the device.

The device will perform a reset after sending the **INI** file.

Save the **Data configuration** file to the PC.

Send the **Data configuration** file to the device.

2. To save the Voice *ini* file to a folder on your PC, perform the following:
 - a. Click the **Save INI File** button; the 'File Download' dialog box appears.
 - b. Click the **Save** button, navigate to the folder in which you want to save the *ini* file on your PC, and then click **Save**; the device copies the *ini* file to the selected folder.
3. To save the Data configuration ini file to a folder on your PC, perform the following:
 - a. Under the 'Save the Data configuration file to the PC' group, click the **Save File** button; the 'File Download' dialog box appears.
 - b. Click the **Save** button, navigate to the folder in which you want to save the file on your PC, and then click **Save**; the device saves the Data ini file to the selected folder.

➤ **To load the ini / data file:**

1. To load the Voice *ini* file to the device, perform the following:
 - a. Click the **Browse** button, navigate to the folder in which the *ini* file is located, select the file, and then click **Open**; the name and path of the file appear in the field beside the **Browse** button.
 - b. Click the **Send INI File** button, and then at the prompt, click **OK**; the device uploads the *ini* file and then resets (from the *cmp* version stored on the flash memory). Once complete, the Login screen appears, requesting you to enter your user name and password.

2. To load the Data configuration ini file to the device, perform the following:
 - a. Under the 'Send the Data Configuration file to the device' group, click the **Browse** button, navigate to the folder in which the file is located, select the file, and then click **Open**; the name and path of the file appear in the field beside the **Browse** button.
 - b. Click the **Send File** button, and then at the prompt, click **OK**; the device uploads the file and then resets (from the cmp version stored on the flash memory). Once complete, the Login screen appears, requesting you to enter your user name and password.

3.5 Status & Diagnostics Tab

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

- System Status (see "System Status" on page [346](#))
- VoIP Status (see "VoIP Status" on page [350](#))
- Data Status (see Data Status on page [358](#))

3.5.1 System Status

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

- Device Information (see "Viewing Device Information" on page [346](#))
- Ethernet Port Information (see "Viewing Ethernet Port Information" on page [348](#))
- WAN Port Information (see Viewing WAN Port Information on page [348](#))
- Active Alarms (see "Viewing Active Alarms" on page [349](#))

3.5.1.1 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**).

Figure 3-301: Device Information Page

▼ General Settings	
MAC Address:	00908f229162
Serial Number:	2265442
Board Type:	Mediant 800
Device Up Time:	0d:0h:9m:50s:55th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [bytes]:	67108864
RAM Size [bytes]:	388866048
CPU Speed [MHz]:	500
▼ Versions	
Version ID:	6.20A.003.013
DSP Type:	1
DSP Software Version:	62017
DSP Software Name:	5014AE3_R
Flash Version:	580
▼ Loaded Files	
Call Progress Tones File Name:	usa_precedence_tones3_nohold_cid.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 334).

3.5.1.2 Viewing Ethernet Port Information

The 'Ethernet Port Information' page displays read-only information on the device's Ethernet connection. This includes indicating the active port, duplex mode, and speed. You can also access this page from the 'Home' page (see "Using the Home Page" on page 59).

For detailed information on the Ethernet interface configuration, see Ethernet Interface Configuration.

➤ **To view Ethernet port information:**

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

Figure 3-302: Ethernet Port Information Page

Ethernet Information				
	Active	Speed	Duplex Mode	Power Over Ethernet
1	Yes	100 Mbps	Half Duplex	Disabled
2	No	10 Mbps	Half Duplex	Disabled
3	No	10 Mbps	Half Duplex	Disabled
4	No	10 Mbps	Half Duplex	Disabled
5	No	10 Mbps	Half Duplex	Disabled
6	No	10 Mbps	Half Duplex	Disabled
7	No	10 Mbps	Half Duplex	Disabled
8	No	10 Mbps	Half Duplex	Disabled
9	No	10 Mbps	Half Duplex	Disabled
10	No	10 Mbps	Half Duplex	Disabled
11	No	10 Mbps	Half Duplex	Disabled
12	No	10 Mbps	Half Duplex	Disabled

Table 3-42: Ethernet Port Information Parameters

Parameter	Description
Active	Displays whether the port is active or not.
Speed	Displays the speed (in Mbps) of the Ethernet port.
Duplex Mode	Displays the whether the port is half- or full-duplex mode.
Power Over Ethernet	Displays whether Power over Ethernet is active on the port.

3.5.1.3 Viewing WAN Port Information

The 'WAN Port Information' page displays read-only information on the device's WAN connection. This information includes the type of WAN port (e.g., T1 or SHDSL) and whether it is active or not.

➤ **To view WAN port information:**

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

Figure 3-303: WAN Port Information Page

	Port Type	Is Port Active?
1	Ethernet	No

3.5.1.4 Carrier-Grade Alarms

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

- Active Alarms (see "Viewing Active Alarms" on page 349)

3.5.1.4.1 Viewing Active Alarms

The 'Active Alarms' page displays a list of currently active alarms. You can also access this page from the 'Home' page (see "Using the Home Page" on page 59).

➤ **To view the list of alarms:**

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

Figure 3-304: Active Alarms Page

Severity	Source	Description	Date
Major	Board#1/EthernetLink#0	Ethernet link alarm. WAN port is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#3	Ethernet link alarm. LAN port number 3 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#4	Ethernet link alarm. LAN port number 4 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#5	Ethernet link alarm. LAN port number 5 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#6	Ethernet link alarm. LAN port number 6 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#7	Ethernet link alarm. LAN port number 7 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#8	Ethernet link alarm. LAN port number 8 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#9	Ethernet link alarm. LAN port number 9 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#10	Ethernet link alarm. LAN port number 10 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#11	Ethernet link alarm. LAN port number 11 is down.	1.1.2000, 0:0:51.0
Minor	Board#1/EthernetLink#12	Ethernet link alarm. LAN port number 12 is down.	1.1.2000, 0:0:51.0

For each alarm, the following information is provided:

- **Severity:** severity level of the alarm:
 - Critical - alarm displayed in red
 - Major - alarm displayed in orange
 - Minor - alarm displayed in yellow
- **Source:** unit from which the alarm was raised
- **Description:** brief explanation of the alarm
- **Date:** date and time that the alarm was generated

You can view the next 30 alarms (if exist), by pressing the F5 key.

3.5.2 VoIP Status

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

- IP Interface Status (see "Viewing Active IP Interfaces" on page 350)
- Performance Statistics (see "Viewing Performance Statistics" on page 350)
- IP to Tel Calls Count (see "Viewing Call Counters" on page 351)
- Tel to IP Calls Count (see "Viewing Call Counters" on page 351)
- SAS/SBC Registered Users (see Viewing SAS/SBC Registered Users on page 353)
- Call Routing Status (see "Viewing Call Routing Status" on page 354)
- Registration Status (see Viewing Registration Status on page 354)
- IP Connectivity (see "Viewing IP Connectivity" on page 356)

3.5.2.1 Viewing Active IP Interfaces

The 'IP Interface Status' page displays the device's active IP interfaces, which are configured in the 'Multiple Interface Table' page (see "Configuring IP Interface Settings" on page 83).

➤ To view the 'Active IP Interfaces' page:

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

Figure 3-305: IP Interface Status Page

Index	Application Type	Address Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	O+M+C	IPv4	IPv4 Manual	10.13.4.12	16	10.13.0.1	1	Voice
NA	Internal	IPv4	IPv4 Manual	169.254.254.254	30	169.254.254.253	4001	InternalIF

3.5.2.2 Viewing Performance Statistics

The 'Basic Statistics' page provides read-only, device performance statistics. This page is refreshed every 60 seconds. The duration that the currently displayed statistics has been collected is displayed above the statistics table.

➤ **To view performance statistics:**

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

Figure 3-306: 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.

3.5.2.3 Viewing Call Counters

The 'IP to Tel Calls Count' and 'Tel to IP Calls Count' pages provide you with statistical information on incoming (IP-to-Tel) and outgoing (Tel-to-IP) calls. The statistical information is updated according to the release reason that is received after a call is terminated (during the same time as the end-of-call Call Detail Record or CDR message is sent). The release reason can be viewed in the 'Termination Reason' field in the CDR message.

You can reset the statistical data displayed on the page (i.e., refresh the display), by clicking the **Reset Counters** button located on the page.

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

- Open the Call Counters page that you want to view (**Status & Diagnostics** tab > **VoIP Status** menu > **IP to Tel Calls Count** or **Tel to IP Calls Count**); the figure below shows the 'IP to Tel Calls Count' page.

Figure 3-307: Calls Count Page

▼	
Number of Attempted Calls	19
Number of Established Calls	14
Percentage of Successful Calls(ASR)	73.684211
Number of Calls Terminated due to a Busy Line	2
Number of Calls Terminated due to No Answer	0
Number of Calls Terminated due to Forward	0
Number of Failed Calls due to No Route	0
Number of Failed Calls due to No Matched Capabilities	0
Number of Failed Calls due to No Resources	0
Number of Failed Calls due to Other Failures	0
Average Call Duration(ACD)[sec]	25
Attempted Fax Calls Counter	0
Successful Fax Calls Counter	0

Table 3-43: 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 Calls due to No Answer' counter. The rest of the release reasons increment the 'Number of Failed Calls due to Other Failures' counter.</p>
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.

Counter	Description
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.

3.5.2.4 Viewing SAS/SBC Registered Users

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

➤ **To view the registered users:**

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

Figure 3-308: SAS/SBC Registered Users Page

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

Table 3-44: SAS/SBC Registered Users Parameters

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

3.5.2.5 Viewing Call Routing Status

The 'Call Routing Status' page provides you with information on the current routing method used by the device. This information includes the IP address and FQDN (if used) of the Proxy server with which the device currently operates.

➤ **To view the call routing status:**

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

Figure 3-309: 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 3-45: 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.

3.5.2.6 Viewing Registration Status

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

➤ **To view Registration status:**

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

Figure 3-310: 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 133):

- **Group Type:** type of served group - Hunt Group or IP Group
- **Group Name:** name of the served group, if applicable
- **Status:** indicates whether or not the group is registered ('Registered' or 'Unregistered')

- **BRI Phone Number Status:**

- **Phone Number:** phone number of BRI endpoint
- **Module/Port:** module/port number of BRI endpoint
- **Status:** indicates whether or not the BRI endpoint is registered ('Registered' or 'Unregistered')



Note: The registration mode (i.e., per device, endpoint, account. or no registration) is configured in the 'Hunt Group Settings' table (see "Configuring Hunt Group Settings" on page 148) or using the TrunkGroupSettings *ini* file parameter.

3.5.2.7 Viewing IP Connectivity

The 'IP Connectivity' page displays online, read-only network diagnostic connectivity information on all destination IP addresses configured in the 'Outbound IP Routing Table' page (see "Configuring Outbound IP Routing Table" on page 165).



Notes:

- This information is available only if the parameter 'Enable Alt Routing Tel to IP'/'AltRoutingTel2IPMode' (see "Configuring General Routing Parameters" on page 164) is set to 1 (Enable) or 2 (Status Only).
- The information in columns 'Quality Status' and 'Quality Info' (per IP address) is reset if two minutes elapse without a call to that destination.

➤ To view IP connectivity information:

1. In the 'Routing General Parameters' page, set the parameter 'Enable Alt Routing Tel to IP' (or *ini* file parameter *AltRoutingTel2IPEnable*) to Enable [1] or Status Only [2].
2. Open the 'IP Connectivity' page (**Status & Diagnostics** tab > **VoIP Status** menu > **IP Connectivity**).

Figure 3-311: IP Connectivity Page

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

Table 3-46: 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.

Column Name	Description
	<ul style="list-style-type: none"> 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	<p>Determines the QoS (according to packet loss and delay) of the IP address.</p> <ul style="list-style-type: none"> Unknown = Recent quality information isn't available. OK Poor <p>Notes:</p> <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.	<p>Displays QoS information: delay and packet loss, calculated according to previous calls.</p> <p>Notes:</p> <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	<p>DNS status can be one of the following:</p> <ul style="list-style-type: none"> DNS Disable DNS Resolved DNS Unresolved

3.5.3 Data Status

The **Data Status** menu is used to view and monitor the device's data routing functionality. This menu includes the following page items:

- WAN Status (see "Viewing WAN Status" on page 358)
- Connection Statistics (see "Viewing Network Connection Statistics" on page 359)
- Security Log (see "Viewing Logged Security Events" on page 360)
- QoS Queues Statistics (see "Viewing QoS Queues Statistics" on page 362)
- Data Log (see "Viewing Logged Data Events" on page 363)
- Diagnostics (see "Running Diagnostic Tests" on page 365)

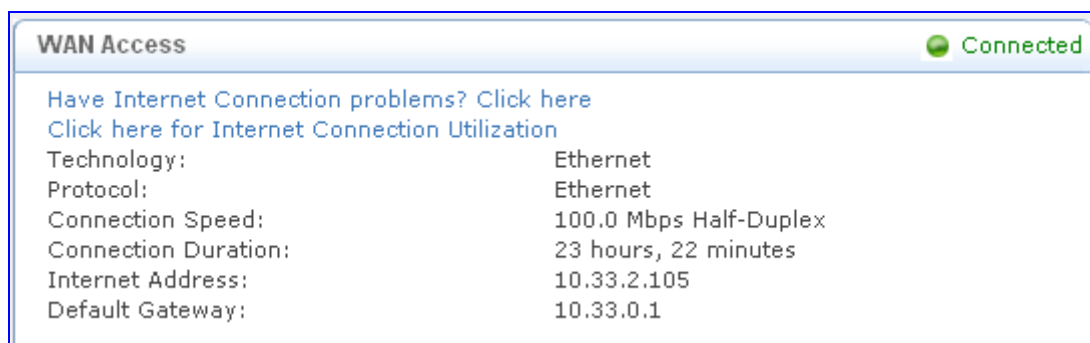
3.5.3.1 Viewing WAN Status

The **WAN Status** item allows you to view the WAN access status and provides a series of diagnostic tests to validate your device's Internet connection. For the diagnostic tests, see "Running Internet Connectivity Diagnostic Tests" on page 358.

➤ **To view the status of the WAN connection:**

- Click the **WAN Status** item (**Status & Diagnostics** tab > **Data Status** menu > **WAN Status**); the following page appears:

Figure 3-312: WAN Status



The status of the WAN interface is depicted by the ball-shaped icon located in the top-right corner:

- Green - "Connected": indicates a valid connection to the WAN network.
- Red - "Cable Disconnected": Green: indicates that there is no connection to the WAN network (cable disconnected).

3.5.3.1.1 Running Internet Connectivity Diagnostic Tests

The procedure below describes how to run a series of tests to validate your device's Internet connection. These tests diagnose and resolve Internet connectivity problems.

➤ **To run Internet connectivity tests:**

1. Click the **WAN Status** item (**Status & Diagnostics** tab > **Data Status** menu > **WAN Status**), and then click the **Have Internet Connection problems? Click here** link; the following page appears:

Figure 3-313: Running Internet Connectivity Diagnostics Tests

Physical Link	Not Tested
Internet Connection Type	Not Tested
Internet Provider	Not Tested
Internet Connectivity	Not Tested

2. Click the **Run** button. While testing is in progress, you may abort the diagnostics process by clicking the **Abort** button.
3. Should a failure message appear, click **Repair** to initiate the Diagnostics Wizard procedure. The device performs the following consecutive diagnostic tests:
 - a. **Test Ethernet Link** - tests the physical integrity of the WAN connection (e.g., Ethernet cable is plugged).
 - b. **Analyze Internet Connection Type** - checks whether the Internet connection type is correctly configured (if not, change the connection type, e.g., to 'Automatic IP Address Ethernet Connection').
 - c. **Setup Internet Connection** - performed if your Internet connection requires login details provided by your ISP, e.g. when using PPPoE (if the test fails, re-enter the login user name and password).
 - d. **Test Service Provider Connection** - tests the connectivity to your ISP.
 - e. **Test Internet Connection** - tests the connectivity to the Internet.
4. When the Diagnostics Wizard completes all the tests, it provides a summary of all the above test results:
5. Click **Finish** to end the Wizard Diagnostics.

3.5.3.2 Viewing Network Connection Statistics

The 'Network Connections' page displays a table summarizing the monitored connection data. The device constantly monitors traffic within the local network and between the local network and the Internet. You can view statistical information about data received from and transmitted to the Internet (WAN) and to computers in the local network (LAN).

➤ To view data on network connections:

- Click the **Connection Statistics** item (**Status & Diagnostics** tab > **Data Status** menu > **Connection Statistics**); the following page appears:

Figure 3-314: Connection Statistics Page

Name	LAN switch	WAN Ethernet	LAN switch VLAN 4001
Device Name	eth0	eth1	eth0.4001
Status	1 Ports Connected	Cable Disconnected	Connected
Network	LAN	WAN	LAN
Underlying Device			LAN switch
Connection Type	Hardware Ethernet Switch	Ethernet	Ethernet
Download Rate	100 Mbps		100 Mbps
Upload Rate	100 Mbps		100 Mbps
MAC Address	00:90:8f:22:2e:31	00:90:8f:22:2e:32	00:90:8f:22:2e:31
IP Address			169.254.254.253
Subnet Mask			255.255.255.252
IP Address Distribution	Disabled	Disabled	Disabled
Received Packets	46098		13666
Sent Packets	10659		10514
Received Bytes	5331977		1284110
Sent Bytes	3147792		3113910
Receive Errors	0		0
Receive Drops	0		0
Time Span	2:15:13		2:15:00

To update the display, click the **Refresh** button, or click the **Automatic Refresh On** button to constantly update the displayed parameters.

3.5.3.3 Viewing Logged Security Events

The **Security Log** item displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate through an administrative interface (Web or Telnet terminal), firewall configuration and system start-up.

➤ To view logs of firewall-related events:

1. Click the **Security Log** item (**Status & Diagnostics** tab > **Data Status** menu > **Security Log**); the following page appears:

Figure 3-315: Firewall - Log Page

Time	Event	Event-Type	Details
Jan 1 17:25:25 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 1 17:25:25 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 1 17:25:25 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 1 17:25:25 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 1 00:00:07 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded

The log table displays the following details:

- **Time:** time the event occurred.
- **Event:** there are five kinds of events:
 - ◆ **Inbound Traffic:** event is a result of an incoming packet.
 - ◆ **Outbound Traffic:** event is a result of outgoing packet.
 - ◆ **Firewall Setup:** configuration message
 - ◆ **WBM Login:** indicates that a user has logged in to the Web interface.
 - ◆ **CLI Login:** indicates that a user has logged in to CLI (via Telnet).
- **Event-Type:** textual description of the event:
 - ◆ **Blocked:** packet was blocked (message is colored red).
 - ◆ **Accepted:** packet was accepted (message is colored green).
- **Details:** additional details about the packet or the event such as protocol, IP addresses, ports, etc.

The page also provides you with the following buttons:

- **Clear Log:** clears currently displayed log messages from the table.
- **Refresh:** updates the log display with the latest log messages.
- **Settings:** allows you to select the types of activities for which you want to have a log message generated, as shown below:

Figure 3-316: Log Settings Page

Accepted Events		
<input type="checkbox"/> Accepted Incoming Connections <input type="checkbox"/> Accepted Outgoing Connections		
Blocked Events		
<input type="checkbox"/> All Blocked Connection Attempts <input type="checkbox"/> Winnuke <input type="checkbox"/> Defragmentation Error <input type="checkbox"/> Blocked Fragments <input type="checkbox"/> Syn Flood <input type="checkbox"/> Echo Chargen	<input type="checkbox"/> Multicast/Broadcast <input type="checkbox"/> Spoofed Connection <input type="checkbox"/> Packet Illegal Options <input type="checkbox"/> UDP Flood	<input type="checkbox"/> ICMP Replay <input type="checkbox"/> ICMP Redirect <input type="checkbox"/> ICMP Multicast <input type="checkbox"/> ICMP Flood
Other Events		
<input type="checkbox"/> Remote Administration Attempts <input type="checkbox"/> Connection States		
Log Buffer		
<input type="checkbox"/> Prevent Log Overrun		

- Accepted Events group:
 - ◆ **Accepted Incoming Connections:** generates a log message for each successful attempt to establish an inbound connection to the home network.
 - ◆ **Accepted Outgoing Connections:** generates a log message for each successful attempt to establish an outgoing connection to the public network.

- Blocked Events group:
 - ◆ **All Blocked Connection Attempts:** generates a log message for each blocked attempt to establish an inbound connection to the home network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options listed below it.
 - ◆ Generate a log message for specific events that are blocked such as SynFlood. A log message is generated if either the corresponding check box is checked, or the 'All Blocked Connection Attempts' check box is selected.
- Other Events group:
 - ◆ **Remote Administration Attempts:** generates a log message for each remote administration connection attempt, whether successful or not.
 - ◆ **Connection States:** provide additional information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application Level Gateways (ALGs).
- Log Buffer group:
 - ◆ **Prevent Log Overrun:** stops logging firewall activities when the memory allocated for the log fills up.

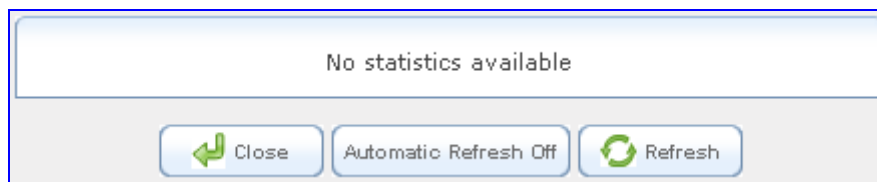
3.5.3.4 Viewing QoS Queues Statistics

You can view an accurate, real-time information on the traffic moving through your defined device classes. For example, the amount of packets sent, dropped or delayed are just a few of the parameters that you can monitor per shaping class.

➤ To view your class statistics:

- Click the **QoS Class Statistics** item (**Status & Diagnostics** tab > **Data Status** menu > **QoS Queues Statistics**); the following page appears:

Figure 3-317: QoS Queues Statistics Page



Note: Class statistics are only available after defining at least one class; otherwise, the page does not display any information.

3.5.3.5 Viewing Logged Data Events

The **Data Log** item displays a list of recent events occurred on the device.

➤ **To view logged messages:**

- Click the **Log** item (**Status & Diagnostics** tab > **Data Status** menu > **Data Log**); the following page appears:

Figure 3-318: System Log Page

Close Clear Log Refresh

Press the **Refresh** button to update the data.

Filters

Component	Severity	Action
All	Information	
New Filter		+
Apply Filters		Reset Filters


Time	Component	Severity	Details
Jan 1 17:25:25 2003	DHCP	Information	Activated Server for dev eth0
Jan 1 00:00:15 2003	IPSec	Information	pluto[57]: RATELIMIT: 1 messages of type IPSec IKE packet reported 11 second(s) ago
Jan 1 00:00:07 2003	Main Task	Information	eth1: link up, device will be up

By default, all log messages are displayed one after another, sorted by their order of posting by the device (latest on top). You can sort the messages according to the column titles 'Time', 'Component', or 'Severity', by clicking the column header. You can also filter the log messages by the component that generated them or by their severity, providing a more refined list. By default, the page displays log messages with 'debug' severity level and higher, for all components. You may change the severity level for this filter.

➤ **To add a new log display filter:**

1. In the 'Filters' group, click the **New Filter** link; the 'Filters' group displays a new Component entry.

Figure 3-319: Adding a New Filter



Component	Severity	Action
All	Information	
Other	Information	✖

[New Filter](#)

2. Using the drop-down lists, select the component and severity level by which to sort the log messages.
3. Click **Apply Filters** to display the messages in your specified criteria.

You can also delete filters using their respective action icons. Clicking **Reset Filters** deletes all the defined filters. Defined filters override the default filter that displays all messages.

You can use the buttons located at the top of the page to perform the following:

- **Close:** closes the 'Log' page and returns to the device's Home page.
- **Clear Log:** clears all currently displayed log messages.
- **Refresh:** refreshes the page to display the latest log messages.

3.5.3.6 Running Diagnostic Tests

The **Diagnostics** item can assist you in testing network connectivity and viewing statistics such as the number of packets transmitted and received, round-trip time and success status. This page allows you to run network connectivity tests (ping), query the physical address (MAC) of a host, and run a trace route test.

➤ **To run diagnostic tests:**

1. Click the **Diagnostics** item (**Status & Diagnostics** tab > **Data Status** menu > **Diagnostics**); the following page appears:

Figure 3-320: System - Diagnostics Page

The screenshot displays the 'System - Diagnostics Page' with three main sections, each with a 'Go' button:

- Ping (ICMP Echo)**: Contains fields for 'Destination:', 'Number of pings:' (set to 4), and 'Status:'.
- ARP**: Contains a 'Destination:' field with four sub-inputs (each containing '0') and a 'Status:' field.
- Traceroute**: Contains a 'Destination:' field and a 'Status:' field.

2. To diagnose network connectivity, under the 'Ping (ICMP Echo)' group, perform the following:
 - a. In the 'Destination' field, enter the IP address or URL to be tested.
 - b. In the 'Number of Pings', enter the number of pings you would like to run.
 - c. Click **Go**; in a few moments, diagnostic statistics are displayed. If no new information appears, click **Refresh**.
3. To query the physical address (MAC) of a host, under the 'ARP' group, perform the following:
 - a. In the 'Destination' field, enter an IP address of the target host.
 - b. Click **Go**; in a few moments, diagnostic statistics are displayed. If no new information is displayed, click **Refresh**.
4. To run a traceroute test, under the Traceroute group, perform the following:
 - a. In the 'Destination' field, enter the IP address or URL to be tested.
 - b. Click **Go**; the traceroute test commences, constantly refreshing the page.
 - c. To stop the test and view the results, click **Cancel**.

Reader's Notes

4 INI File-Based Management

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

- Web interface (see "Backing Up and Loading Configuration File" on page 344)

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

- 'Load Auxiliary Files' page (see "Loading Auxiliary Files" on page 337): 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 653.
- Some parameters are configurable only through the *ini* file (and not the Web interface).
- To restore the device to default settings using the *ini* file, see "Restoring Factory Default Settings" on page 391.

4.1 INI File Format

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

- Individual parameters (see "Configuring Individual ini File Parameters" on page 367)
- Table parameters (see "Configuring ini File Table Parameters" on page 368)

4.1.1 Configuring Individual ini File Parameters

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

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

For general *ini* file formatting rules, see "General ini File Formatting Rules" on page 370.

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

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

[Web Parameters]
LogoWidth = '339'
WebLogoText = 'My Device'
UseWeblogo = 1
; these are a few of the Web-related parameters.

[Files]
CallProgressTonesFileName = 'cpusa.dat'
```

4.1.2 Configuring ini File Table Parameters

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

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

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

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

```
[Table Title]
; This is the title of the table.
FORMAT Index = Column Name1, Column Name2, Column Name3;
; This is the Format line.
Index 0 = value1, value2, value3;
Index 1 = value1, $$, value3;
; These are the Data lines.
[\\Table Title]
; This is the end-of-the-table-mark.
```

The *ini* file table parameter formatting rules are listed below:

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

For general *ini* file formatting rules, see "General ini File Formatting Rules" on page [370](#).

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

```
[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = g711Alaw64k, 20, 0, 255, 0;
CodersGroup0 1 = eg711Ulaw, 10, 0, 71, 0;
CodersGroup0 2 = eg711Ulaw, 10, 0, 71, 0;
[ \\CodersGroup0 ]
```



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

4.1.3 General ini File Formatting Rules

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

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

4.2 Modifying an ini File

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

➤ To modify an *ini* file:

1. Save the current *ini* file from the device to your PC, using the Web interface (see "Backing Up and Loading Configuration File" on page 344).
2. Open the *ini* file (using a text file editor such as Microsoft Notepad), and then modify the *ini* file parameters according to your requirements.
3. Save the modified *ini* file, and then close the file.
4. Load the modified *ini* file to the device, using the Web interface (see "Backing Up and Loading Configuration File" on page 344).



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

4.3 Secured Encoded ini File

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

**Notes:**

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

Reader's Notes

5 EMS-Based Management

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

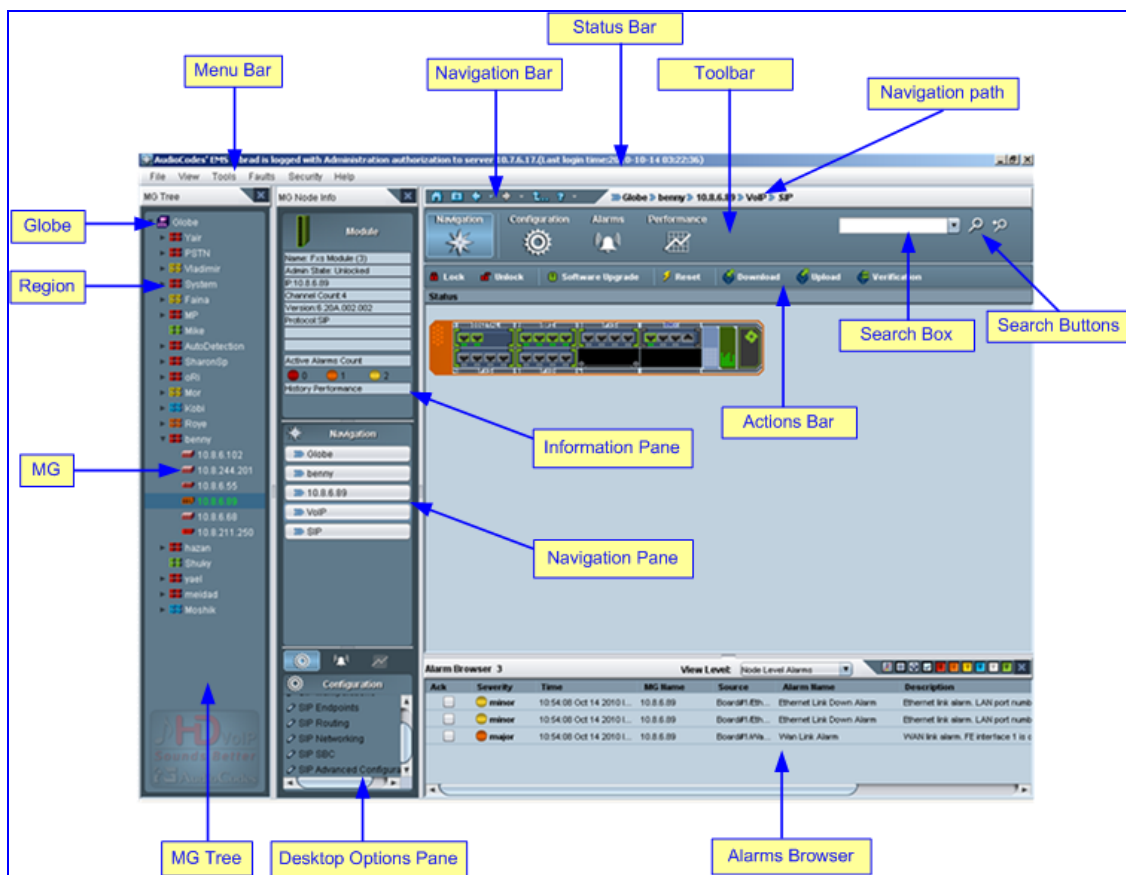


Note: For a detailed description of using the EMS tool, refer to the *EMS User's Manual* and *EMS Server IOM Manual*.




5.1 Familiarizing yourself with EMS GUI

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

Figure 5-1: Areas of the EMS GUI



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

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

5.2 Adding the Device in EMS

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

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

- a. Adding a Region
- b. Defining the device's IP address (and other initial settings)

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


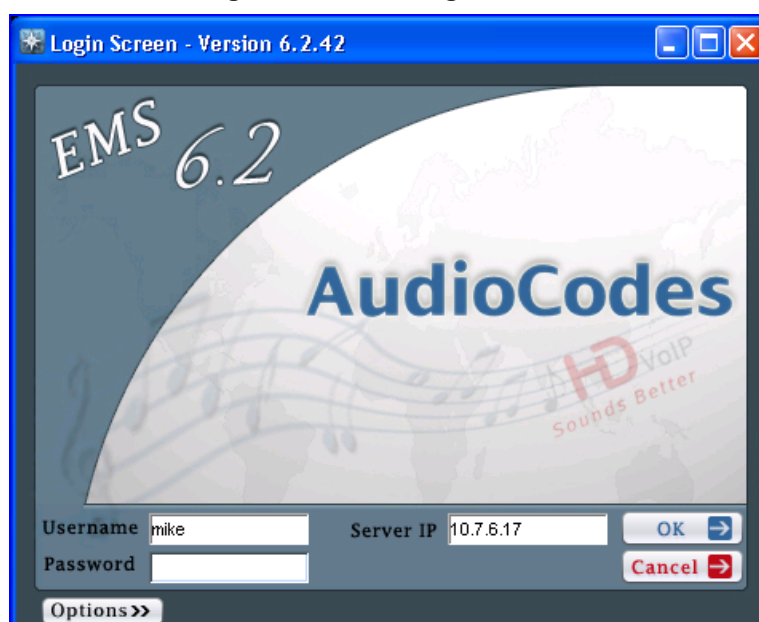
1. Start the EMS by double-clicking the shortcut icon  on your desktop, or from the **Start** menu, point to **Programs**, point to **EMS Client**, and then click **EMS Client**; the Login Screen appears:

Figure 5-2: EMS Login Screen



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


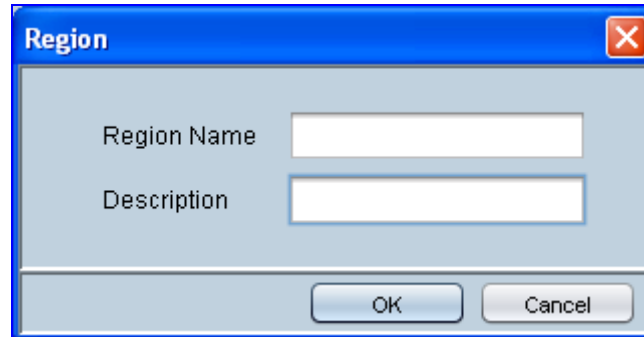
3. Add a Region for your deployed device, by performing the following:
 - a. In the MG Tree, right-click the **Globe**  icon, and then click **Add Region**; the Region dialog box appears.

Figure 5-3: Adding a Region


 A dialog box titled "Region" with a blue header bar and a red close button. It contains two text input fields: "Region Name" and "Description". At the bottom, there are "OK" and "Cancel" buttons.


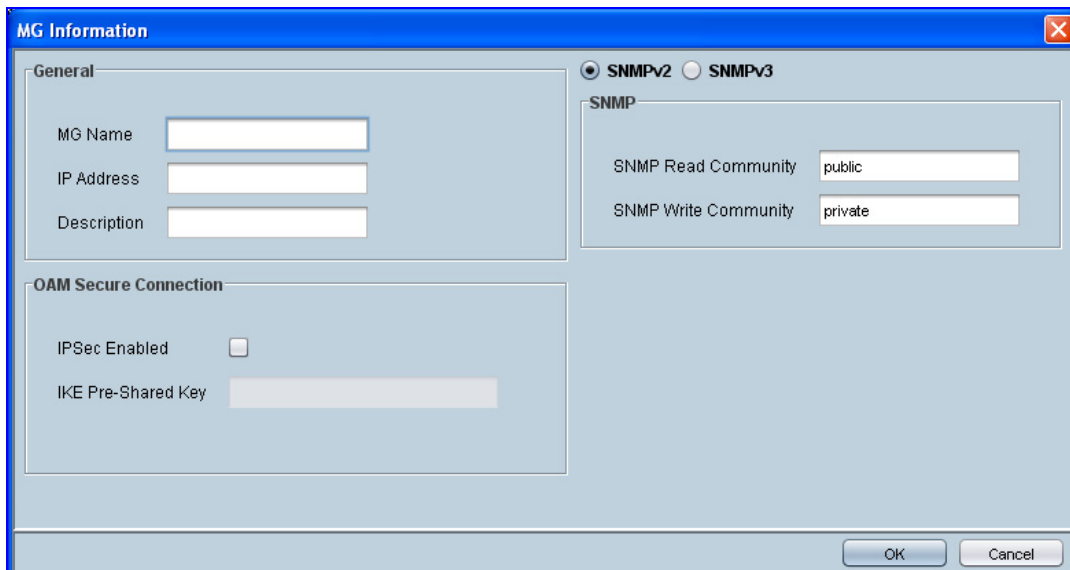
- b. In the 'Region Name' field, enter a name for the Region (e.g., a geographical name), and then click **OK**; the Region is added to the MG Tree list.
4. Verify that the device is up and running (by performing a ping to its IP address).
5. Add the device to the Region, by performing the following:
 - a. Right-click the added Region  icon, and then from the shortcut menu, choose **Add MG**; the MG Information dialog box appears.

Figure 5-4: Defining the IP Address


 A dialog box titled "MG Information" with a blue header bar and a red close button. It has two main sections: "General" and "OAM Secure Connection". The "General" section contains fields for "MG Name", "IP Address", and "Description". The "OAM Secure Connection" section contains a checkbox for "IPSec Enabled" and a text field for "IKE Pre-Shared Key". To the right of these sections, there are radio buttons for "SNMPv2" (selected) and "SNMPv3", and a section for "SNMP" with fields for "SNMP Read Community" (set to "public") and "SNMP Write Community" (set to "private"). At the bottom, there are "OK" and "Cancel" buttons.

- b. Enter an arbitrary name for the device, and then in the 'IP Address' field, enter the device's IP address
 - c. Click **OK**; the device is added to the Region and appears listed in the MGs List.



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

5.3 Configuring Trunks

This section describes the provisioning of trunks:

- E1/T1 Trunk configuration (see "General Trunk Configuration" on page 376)
- ISDN NFAS (see "Configuring ISDN NFAS" on page 377)

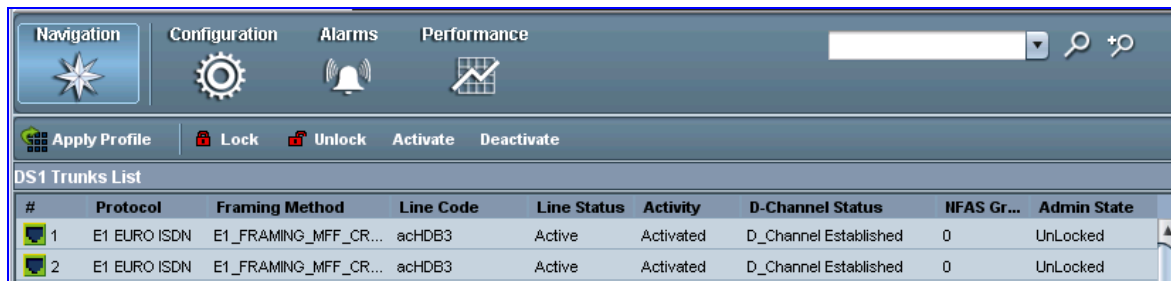
5.3.1 General Trunk Configuration

This section describes how to provision a PSTN trunk.

➤ **To provision a trunk:**

1. In the **Navigation** pane, select **VoIP > PSTN > DS1 Trunks**; the DS1 Trunks List appears.

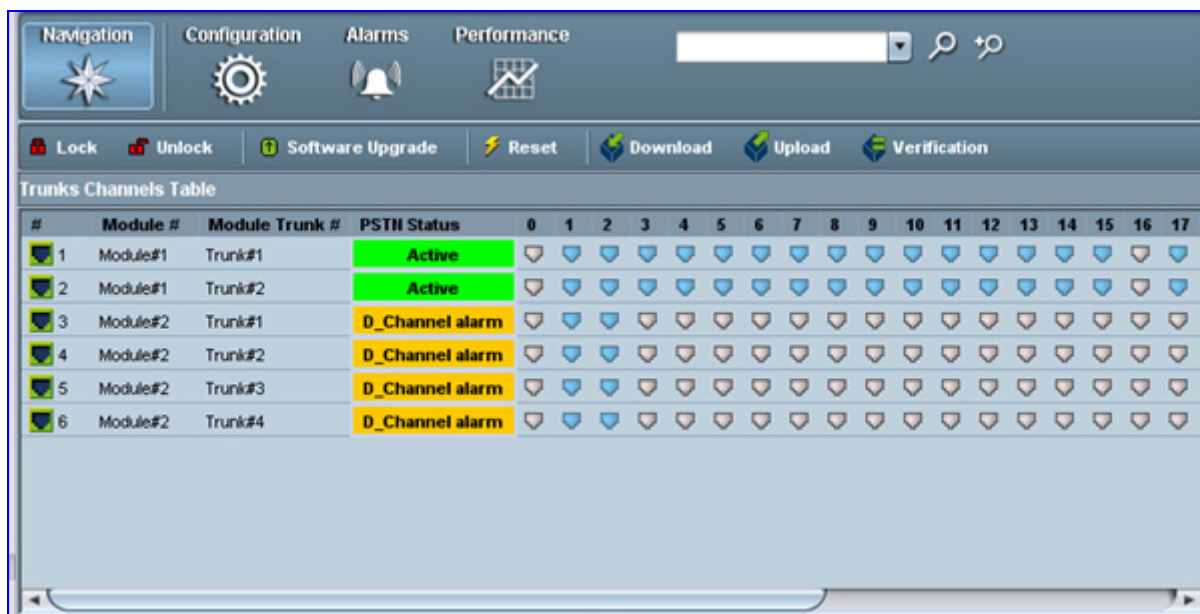
Figure 5-5: DS1 Trunks List Table



#	Protocol	Framing Method	Line Code	Line Status	Activity	D-Channel Status	NFAS Gr...	Admin State
1	E1 EURO ISDN	E1_FRAMING_MFF_CR...	achDB3	Active	Activated	D_Channel Established	0	UnLocked
2	E1 EURO ISDN	E1_FRAMING_MFF_CR...	achDB3	Active	Activated	D_Channel Established	0	UnLocked

2. Select a trunk, and then in the **Navigation** pane, click **VoIP > PSTN > Trunks Channels**; the Trunks Channels Table appears in the Main pane.

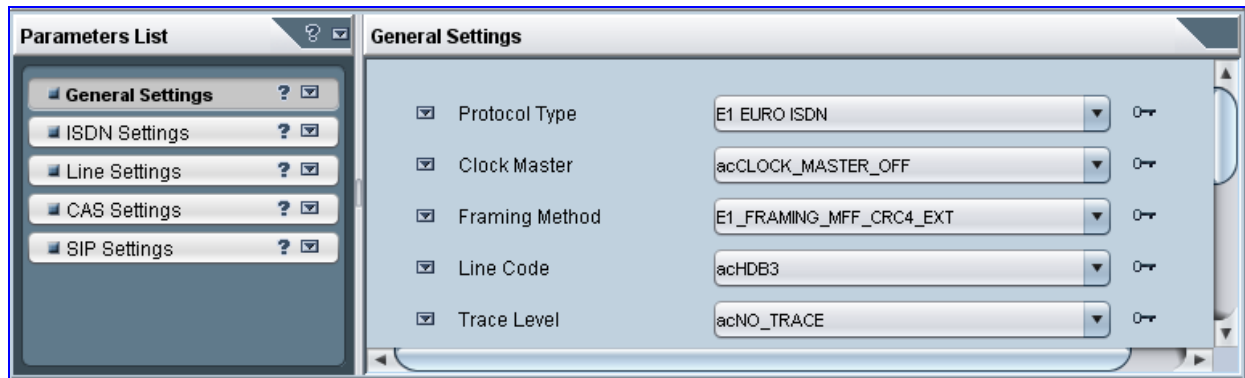
Figure 5-6: Trunks Channels Table



#	Module #	Module Trunk #	PSTN Status	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	Module#1	Trunk#1	Active																		
2	Module#1	Trunk#2	Active																		
3	Module#2	Trunk#1	D_Channel alarm																		
4	Module#2	Trunk#2	D_Channel alarm																		
5	Module#2	Trunk#3	D_Channel alarm																		
6	Module#2	Trunk#4	D_Channel alarm																		

3. Select a trunk, and then in the **Configuration** pane, click **Trunk SIP Frame**; the Trunk SIP Provisioning screen is displayed with the General Settings tab selected.

Figure 5-7: General Settings Screen



4. From the 'Protocol Type' drop-down list, select the required protocol.
5. From the 'Framing Method' drop-down list, select the required framing method. For E1, always set this parameter to Extended Super Frame.
6. From the 'Clock Master' drop-down list, set the Clock Master to one of the following values:
 - Clock Master OFF: the Clock Source is recovered from the Trunk line.
 - Clock Master ON: the Clock Source is provided by the internal TDM bus clock source, according to the parameter TDM Bus Clock Source.
7. Select the other tabs to continue configuring the PSTN trunks.



Notes:

- When changing 'Protocol Type' from 'None' to any other protocol, reset the device. You're not required to reset the device when making subsequent changes to 'Protocol Type'.
- Most Trunk provisioning parameters require that a Trunk Lock / Unlock be performed before / after configuring them. When performing a Lock action, all active calls are dropped and users cannot make new calls. This is Trunk Out Of Service mode.
- Upon initial configuration, do not change the Admin State of the trunks to unlock (it is changed automatically after the device is reset in EMS).

5.3.2 Configuring ISDN NFAS

This section describes how to configure ISDN-NFAS trunks as an initial configuration.

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 NFAS group can comprise up to 10 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.

ISDN-NFAS Trunks can be configured offline or on-the-fly.

➤ **To configure ISDN-NFAS Trunks offline:**

1. Access the Trunks Channels Table (as described in "General Trunk Configuration" on page 376).
2. Select a trunk, and then in the **Configuration** pane, click **Trunk SIP Frame**; the Trunk SIP Provisioning screen is displayed with the General Settings tab selected.
3. Select the **ISDN Settings** tab; the 'ISDN Settings' screen appears.

Figure 5-8: EMS ISDN Settings Screen



4. Perform the following configurations:
 - a. Configure each trunk in the group with the same values for the 'Termination Side' parameter.
 - b. Select the 'EXPLICIT INTERFACE ID' check box to configure the Interface ID (see Step d) of a NFAS Trunk. If this field is not set, only the Trunk ID is recognized.
 - c. From the 'D-Channel Configuration' drop-down list, select 'Primary NFAS Trunk' for the T1 trunk whose D-channel is used for signaling or 'Backup NFAS Trunk' for the T1 trunk whose D-channel is used for backup signaling. The primary and backup trunks each carry 23 B-channels while all other NFAS trunks each carry 24 B-channels.
 - d. In the 'ISDN NFAS Interface ID' field, enter the Interface ID (0 - 255) of the trunk in the NFAS group.
 - e. In the 'Group Number' field, enter the device's NFAS Group Number. If this field is set to 0, the trunk is not an NFAS trunk.
 - f. Click **Apply**.
 - g. To apply the configured fields to multiple trunks, use the Profiles that appear on the lower part of the screen.

5. Select the **General Settings** tab, and then configure each trunk in the group with the same values for the following parameters:
 - Protocol Type
 - Framing Method
 - Line Code
6. Burn and reset the device after all the trunks have been configured.



Note: All trunks in the group must be configured with the same values for trunk parameters TerminationSide, ProtocolType, FramingMethod and LineCode.

The procedure below describes how to configure ISDN-NFAS trunks on-the-fly. The configuration process is the same as the initial Offline configuration, but the sequence of configuring or locking the trunks is important.

➤ **To configure ISDN-NFAS Trunks on-the-fly:**

- Unlocking an NFAS Group:
 - a. If there is a Backup trunk for this group, it must be unlocked first.
 - b. The Primary trunk must be unlocked before unlocking any NFAS trunks.
 - c. NFAS trunks should then be unlocked.
- Locking and Removing an NFAS Group:
 - a. Lock all NFAS trunks, change their Protocol Type to NONE and then unlock them.
 - b. Lock the Backup trunk if it exists. Change its Protocol Type to NONE and then unlock it.
 - c. Lock the Primary trunk, change its Protocol Type to NONE and then unlock it.



Note: You cannot re-configure an NFAS group after locking it. You must first set all trunks to Protocol Type NONE and then start configuration again.

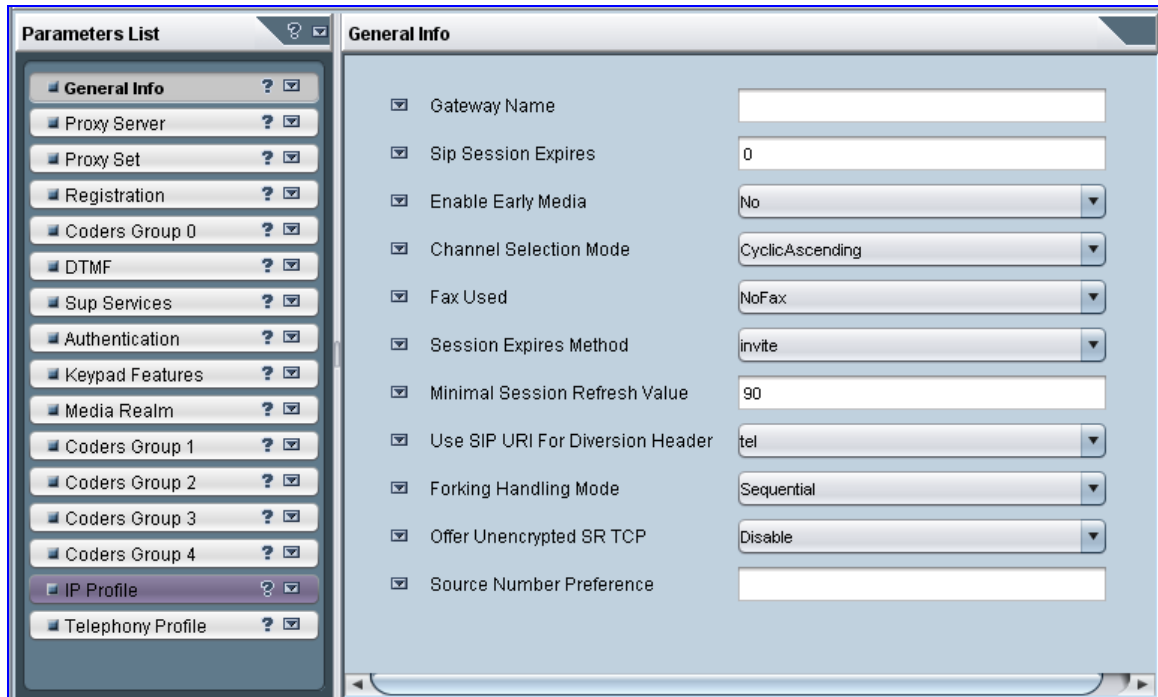
5.4 Configuring Basic SIP Parameters

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


➤ To configure basic SIP parameters:

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

Figure 5-9: SIP Protocol Definitions Frame




2. Select the **Coders Group 0** tab; the Coders screen is displayed.
 - a. Click the **+** button to add a new Coder entry, and then click **Yes** to confirm.
 - b. Double-click each field to enter values.
 - c. Right-click the new entry, and then choose **Unlock Rows**.
3. Select the **Proxy Server** tab.
 - a. Set 'Proxy Used' to Yes.
 - b. (Optional) In the 'Proxy Name' field, enter the Proxy's name. The Proxy name replaces the Proxy IP address in all SIP messages. This means that messages are still sent to the physical Proxy IP address, but the SIP URI contains the Proxy name instead. When no Proxy is used, the internal routing table is used to route the calls.
 - c. Click the **+** button, and then click **Yes** to confirm.
 - d. Enter the IP address of the Proxy Server.
 - e. Right-click the new entry, and then choose **Unlock Rows**.

4. Select the **Registration** tab.
 - a. Configure 'Is Register Needed' field:
 - ◆ No = the device doesn't register to a Proxy/Registrar server (default).
 - ◆ Yes = the device registers to a Proxy/Registrar server at power up and every user-defined interval ('Registration Time' parameter).
 - b. Click **Apply** and close the active window.
5. Open the 'SIP EndPoints' frame (**Configuration** pane > **SIP Endpoints** menu).
 - a. Click the  button to add a new entry, and then click **Yes** to confirm; the 'Phones' screen is displayed.
 - b. Double-click each field to enter values.
 - c. Right-click the new entry, and then select **Unlock Rows**.
 - d. Click **Apply** and close the active window.



Note: For T1 ISDN spans, configure 1-23 (and not 1-24) for B-channels. Channel 24 is a signaling ISDN channel.

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

5.5 Provisioning SIP SRTP Crypto Offered Suites

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

➤ To configure SRTP crypto offered suites:

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

Figure 5-10: Authentication & Security Screen



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

5.6 Provisioning SIP MLPP Parameters

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

➤ To configure the MLPP parameters:

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

2. Select the **MLPP** tab; the 'MLPP' screen appears.

Figure 5-11: MLPP Screen

Parameter	Value
Call Priority Mode	Disable
Default Name Space	DSN
Default Call Priority	0
Diff Serv	50
Preemption Tone Duration	3
Default Service Domain	111111
Normalized Service Domain	000000
RTP DSCP for MLPP Routine	-1
RTP DSCP for MLPP Priority	-1
RTP DSCP for MLPP Immediate	-1

3. Configure the MLPP parameters as required.



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

5.7 Configuring the Device to Operate with SNMPv3

This section describes the SNMPv3 configuration process:

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



Note: After configuring SNMPv3, ensure that you disable IPSec.

5.7.1 Configuring SNMPv3 using SSH

The procedure below describes how to configure SNMPv3 using SSH. This is a more secure way of configuring the SNMPv3 connection between the EMS and the device, i.e., before you have a secure SNMP connection, there could be eavesdropping.

➤ **To configure the device to operate with SNMPv3 via SSH:**

1. Open an SSH Client session (e.g. PuTTY), and then connect, using the default user name and password ("Admin" - case sensitive) to the device. If a message appears with the RSA host key, click "Yes" to continue. Verify that the shell prompt appears (">").

2. Type **Conf**, and then press Enter.

```
/CONFiguration>
```

3. Type **cf set**, and then press Enter; the following prompt is displayed:

```
Enter data below. Type a period (.) on an empty line to finish.
```

The configuration session is now active and all data entered at the terminal is parsed as configuration text (formatted as an *ini* file).

4. Type the following text at the configuration session:

```
[ SNMPUsers ]
FORMAT SNMPUsers_Index = SNMPUsers_Username,
SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol,
SNMPUsers_AuthKey, SNMPUsers_PrivKey, SNMPUsers_Group;
SNMPUsers 0 = v3user, 2, 1,<auth password>,<priv password>, 1;
[ \SNMPUsers ]
```

where:

- <auth password> is the password for the authentication protocol
- <priv password> is the password for the privacy protocol

Possible values for AuthProtocol:

- 0 – none
- 1 - MD5
- 2 - SHA-1

Possible values for PrivProtocol:

- 0 – none
- 1 – DES
- 3 - AES128

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

```
INI File replaced
```

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

5.7.2 Configuring EMS to Operate with a Pre-configured SNMPv3 System

The procedure below describes how to configure the device with a pre-configured SNMPv3.

➤ To configure EMS to operate with a pre-configured SNMPv3 system:

1. In the MG Tree, select the required Region to which the device belongs, and then right-click the device.
2. From the shortcut menu, choose **Details**; the 'MG Information' screen appears.

Figure 5-12: MG Information Screen

The figure shows a dialog box titled "MG Information" with a close button in the top right corner. The dialog is divided into three main sections:

- General:** Contains text boxes for "MG Name" (filled with "Device"), "IP Address" (filled with "10.13.4.13"), and "Description".
- OAM Secure Connection:** Contains checkboxes for "IPSec Enabled" and "HTTPS Enabled" (both unchecked), and a text box for "IKE Pre-Shared Key".
- SNMP:** At the top of this section are two radio buttons: "SNMPv2" (unselected) and "SNMPv3" (selected). Below them are several fields:
 - Engine ID:** An empty text box.
 - Security Name:** A text box filled with "snmpv3user1".
 - Security Level:** A dropdown menu showing "Authentication & Privacy".
 - Authentication Protocol:** A dropdown menu showing "SHA".
 - Authentication Key:** A text box filled with "*****".
 - Privacy Protocol:** A dropdown menu showing "AES_128".
 - Privacy Key:** A text box filled with "*****".

At the bottom right of the dialog are "OK" and "Cancel" buttons.

3. Select the **SNMPv3** option, configure the SNMP fields, and then click **OK**.
4. Open the 'SNMPv3 Users' screen (**Navigation** pane > **System** > **Management** > **SNMP Frame** > **SNMPv3 Users** tab).
5. From the **SNMPv3 Users** tab's drop-down list, choose **Unit value**; the 'SNMPv3 Users' table is refreshed with the values that you entered in Step 3.
6. Click the **Save** button; the EMS and the device are now synchronized.

5.7.3 Configuring SNMPv3 to Operate with Non-Configured SNMPv3 System

The procedure below describes how to configure SNMPv3 using the EMS.

- **To configure the device to operate with SNMPv3 via EMS (to a non-configured System):**
 1. In the MG Tree, select the required Region to which the device belongs; the device is displayed in the Main pane.
 2. Right-click the device, and then from the shortcut menu, point to **Configuration**, and then click **SNMP Configuration**; the 'SNMP Configuration' window appears.

Figure 5-13: SNMP Configuration Screen




The screenshot shows the 'SNMP Configuration' dialog box. At the top, there are two radio buttons: 'SNMPv2' and 'SNMPv3'. The 'SNMPv3' option is selected. Below this, the 'SNMP' section contains several fields: 'Engine ID' (empty), 'Security Name' (filled with 'snmpv3user'), 'Security Level' (dropdown menu showing 'Authentication & Privacy'), 'Authentication Protocol' (dropdown menu showing 'SHA'), 'Authentication Key' (filled with '***'), 'Privacy Protocol' (dropdown menu showing 'AES_128'), and 'Privacy Key' (filled with '*****'). At the bottom of the dialog, there is a checked checkbox labeled 'Update Media Gateway SNMP Settings'. The 'OK' and 'Cancel' buttons are at the bottom right.

3. Select the **SNMPv3** option.
4. Configure the SNMPv3 fields, and then select the **Update Media Gateway SNMP Settings** check box.
5. Click **OK**; the update progress is displayed.
6. Click **Done** when complete.
7. Open the 'SNMPv3 Users' screen (**Navigation** pane > **System** > **Management** > **SNMP Frame** > **SNMPv3 Users** tab).
8. From the **SNMPv3 Users** tab's drop-down list, choose **Unit value**; the 'SNMPv3 Users' table is refreshed with the values that you entered in Step 4.
9. Click the **Save** button; the EMS and the device are now synchronized.

5.7.4 Cloning SNMPv3 Users

According to the SNMPv3 standard, SNMPv3 users on the SNMP Agent (on the device) cannot be added via the SNMP protocol, e.g. SNMP Manager (i.e., the EMS). Instead, new users must be defined by User Cloning. The SNMP Manager creates a new user according to the original user permission levels.

➤ **To clone SNMPv3 Users:**

1. Open the 'SNMPv3 Users' screen (**Navigation** pane > **System** > **Management** > **SNMP Frame** > **SNMPv3 Users** tab).
2. Select the user with which you wish to clone permission levels.
3. Click the  button; the 'New SNMPv3 User' window appears.
4. Provide a new user name, old passwords of the user you clone permissions from and new user passwords.
5. Select a User permission group.
6. If the new user wishes to receive traps to the user-defined destination, select the **Use SNMPv3 User Security Profile for Trap Forwarding** option to provision Trap destination IP and Port. EMS adds this new user to the SNMP Trap Managers Table. It is also possible to define an additional trap destination after a new user is defined.

5.8 Resetting the Device

When you have completed configuring the device, you need to save your settings to the device's flash memory and reset the device.

➤ **To save configuration and reset the device:**


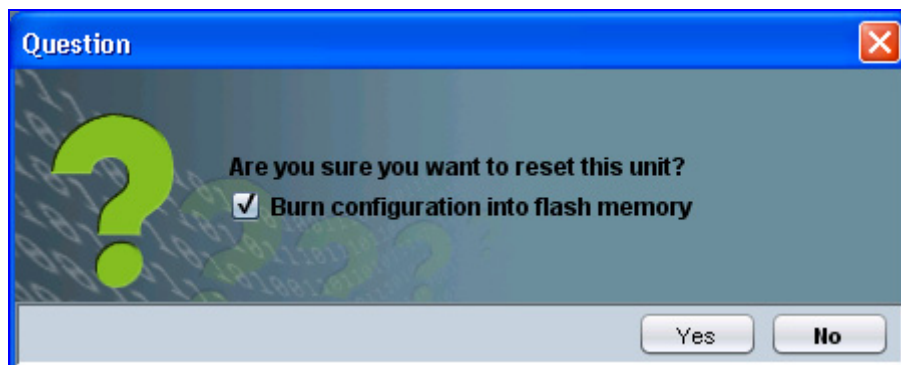
1. In the MG Tree, select the device that you want to reset.
2. On the Actions bar, click the **Reset**  button.

Figure 5-14: Confirmation for Saving Configuration and Resetting Device



3. Ensure that the option **Burn Configuration into flash memory** is selected.
4. Click **Yes**; the progress of the reset process is displayed.
5. Click **Done** when complete.

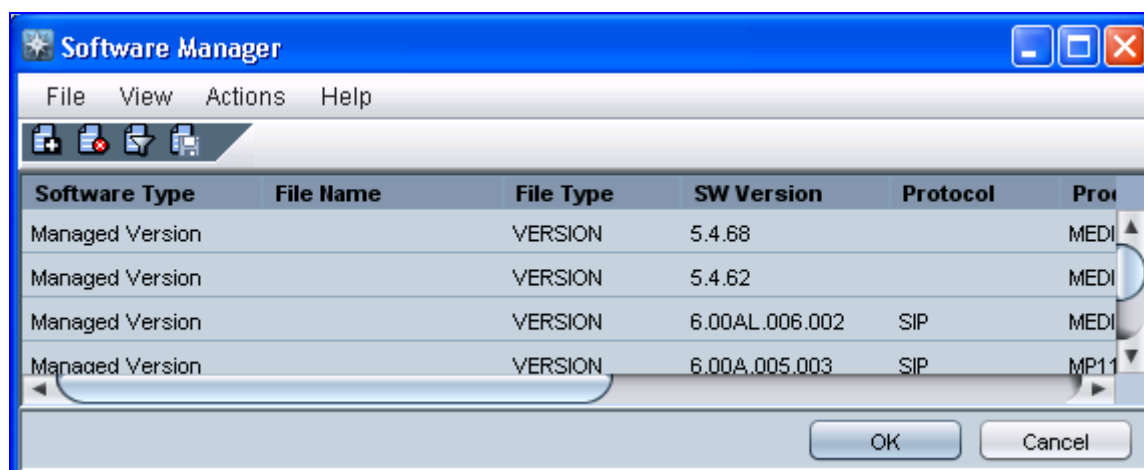
5.9 Upgrading the Device's Software

The procedure below describes how to upgrade the devices software (i.e., cmp file) using the EMS.

➤ To upgrade the device's cmp file:

1. From the **Tools** menu, choose **Software Manager**; the 'Software Manager' screen appears.

Figure 5-15: Software Manager Screen




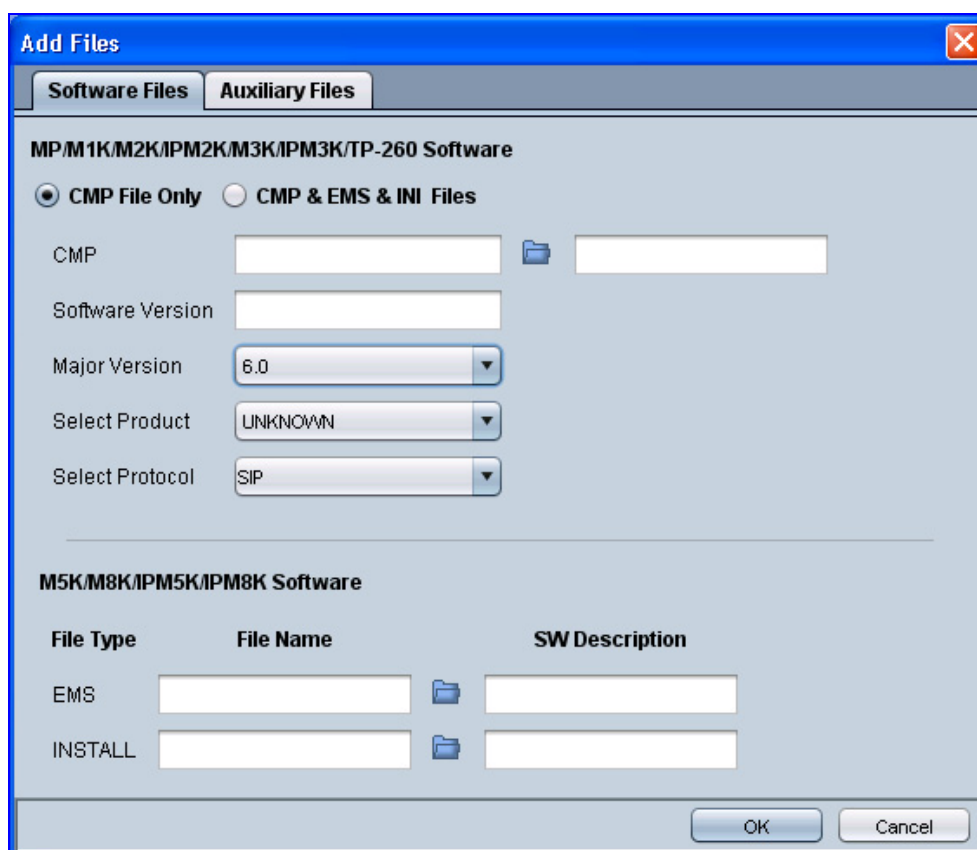
2. Click the **Add File**  icon; the 'Add Files' dialog box appears.

Figure 5-16: Add Files Screen




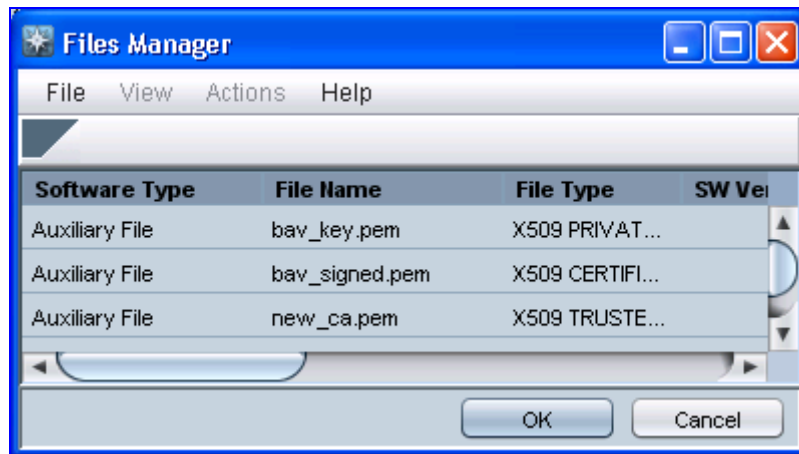
3. Select the cmp file, by performing the following:
 - a. Ensure that the **CMP File Only** option is selected.
 - b. In the 'CMP' field, click the browse button and navigate to the required cmp file; the software version number of the selected file appears in the 'Software Version' field.
 - c. From the 'Major Version' drop-down list, select the version number of the cmp file.
 - d. From the 'Select Product' drop-down list, select the type of device.
 - e. From the 'Select Protocol' drop-down list, select the control protocol (i.e., SIP).
4. Click **OK**.
5. In the MG Tree, select the device that you want to upgrade.
6. On the Actions bar, click the **Software Upgrade**  button; the 'Files Manager' screen appears.

Figure 5-17: Files Manager Screen



7. Select the file that you want to download to the device, and then click **OK**; a confirmation box appears.
8. Click **Yes** to confirm download; the 'Software Download' screen appears, displaying the download progress.
9. Click **Done** when download is completed successfully.

Reader's Notes

6 Restoring Factory Default Settings

You can restore the device's configuration to factory defaults using one of the following methods:

- Using the CLI (see "Restoring Defaults using CLI" on page 391)
- Loading an empty *ini* file (see "Restoring Defaults using an ini File" on page 392)
- Using the hardware Reset button (see Restoring Defaults using Hardware Reset Button on page 392)

6.1 Restoring Defaults using CLI

The device can be restored to factory defaults using CLI, as described in the procedure below.

➤ **To restore factory defaults using CLI:**

1. Access the device's CLI:
 - a. Connect the device's RS-232 port (refer to the *Installation Manual*) to COM1 or COM2 communication port on your PC.
 - b. Establish serial communication with the device, using a serial communication program (such as HyperTerminal™) with the following communication port settings:
 - ◆ **Baud Rate:** 115,200 bps
 - ◆ **Data Bits:** 8
 - ◆ **Parity:** None
 - ◆ **Stop Bits:** 1
 - ◆ **Flow Control:** None
2. At the initial CLI prompt, type the username (default is 'Admin'), and then press the Enter key.
3. At the Password prompt, type the password (default is 'Admin'), and then press the Enter key.
4. At the prompt, type the following, and then press the Enter key:

```
enable
```

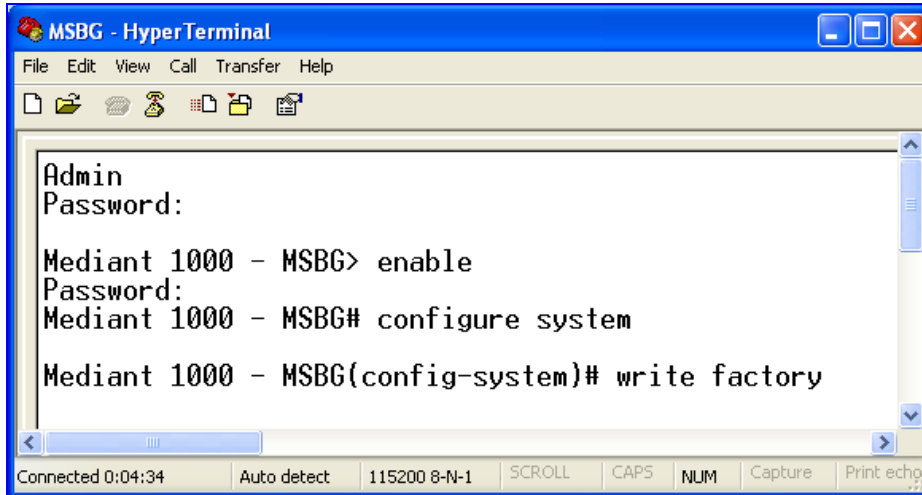
5. At the Password prompt, type the password (default is 'Admin'), and then press the Enter key.
6. At the prompt, type the following, and then press the Enter key:

```
configure system
```

7. At the prompt, type the following command to reset the device to default settings, and then press the Enter key:

```
write factory
```

The CLI commands are shown in the terminal emulation program (e.g., HyperTerminal) below:



```

MSBG - HyperTerminal
File Edit View Call Transfer Help
[Icons]
Admin
Password:
Mediant 1000 - MSBG> enable
Password:
Mediant 1000 - MSBG# configure system
Mediant 1000 - MSBG(config-system)# write factory
[Scroll bar]
Connected 0:04:34 Auto detect 115200 8-N-1 SCROLL CAPS NUM Capture Print echo

```

6.2 Restoring Defaults using an ini File

You can restore the device to factory default settings by loading an empty *ini* file to the device, using the Web interface's 'Configuration File' page (see "Backing Up and Loading Configuration File" on page 344). The only settings that are not restored to default are the management (OAMP) LAN IP address and the Web interface's login user name and password. The loaded *ini* file must be empty (i.e., contain no parameters), or include only comment signs (i.e., semicolons ";") preceding lines (parameters). The default values assigned to the parameters are according to the *cmp* file running on the device.

6.3 Restoring Defaults using Hardware Reset Button

The device's hardware Reset pinhole button can be used to reset the device to default settings. For a detailed description, refer to the *Installation Manual*.

7 Auxiliary Configuration Files

This section describes the auxiliary files that can be loaded to the device:

- Call Progress Tones (see "Call Progress Tones File" on page 393)
- Distinctive Ringing in the ini file (see Distinctive Ringing on page 396)
- Prerecorded Tones (see "Prerecorded Tones File" on page 399)
- CAS (see CAS Files on page 399)
- Dial Plan (see Dial Plan File on page 400)
- User Information (see "User Information File" on page 402)

You can load these auxiliary files to the device using one of the following methods:

- Loading the files directly to the device using the device's Web interface (see "Loading Auxiliary Files" on page 337).
- Specifying the auxiliary file name in the *ini* file (see "Auxiliary and Configuration Files Parameters" on page 881) and then loading the *ini* file to the device. The Auxiliary files listed in the *ini* file are then uploaded to the device through TFTP during device startup. If the *ini* file does not contain a specific auxiliary file type, the device uses the last auxiliary file of that type that was stored on its non-volatile memory.

7.1 Call Progress Tones File

The Call Progress Tones (CPT) and Distinctive Ringing (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 396).

You can use one of the supplied auxiliary files (*.dat file format) or create your own file. To create your own file, it's recommended to modify the supplied *usa_tone.ini* file (in any standard text editor) to suit your specific requirements and then convert the modified *ini* file into binary format using the TrunkPack Downloadable Conversion Utility (DConvert). For a description on converting a CPT *ini* file into a binary *dat* file, refer to the *Product Reference Manual*.



Note: Only the *dat* file format can be loaded to the device.

You can create up to 32 different Call Progress Tones, each with frequency and format attributes. The frequency attribute can be single or dual-frequency (in the range of 300 to 1980 Hz) or an Amplitude Modulated (AM). Up to 64 different frequencies are supported. Only eight AM tones, in the range of 1 to 128 kHz, can be configured (the detection range is limited to 1 to 50 kHz). Note that when a tone is composed of a single frequency, the second frequency field must be set to zero.

The format attribute can be one of the following:

- **Continuous:** A steady non-interrupted sound (e.g., a dial tone). Only the 'First Signal On time' should be specified. All other on and off periods must be set to zero. In this case, the parameter specifies the detection period. For example, if it equals 300, the tone is detected after 3 seconds (300 x 10 msec). The minimum detection time is 100 msec.
- **Cadence:** A repeating sequence of on and off sounds. Up to four different sets of on/off periods can be specified.
- **Burst:** A single sound followed by silence. Only the 'First Signal On time' and 'First Signal Off time' should be specified. All other on and off periods must be set to zero. The burst tone is detected after the off time is completed.

You can specify several tones of the same type. These additional tones are used only for tone detection. Generation of a specific tone conforms to the first definition of the specific tone. For example, you can define an additional dial tone by appending the second dial tone's definition lines to the first tone definition in the *ini* file. The device reports dial tone detection if either of the two tones is detected.

The Call Progress Tones section of the *ini* file comprises the following segments:

- **[NUMBER OF CALL PROGRESS TONES]:** Contains the following key:
'Number of Call Progress Tones' defining the number of Call Progress Tones that are defined in the file.
- **[CALL PROGRESS TONE #X]:** containing the Xth tone definition, starting from 0 and not exceeding the number of Call Progress Tones less 1 defined in the first section (e.g., if 10 tones, then it is 0 to 9), using the following keys:
 - **Tone Type:** Call Progress Tone types:
 - ◆ **[1]** Dial Tone
 - ◆ **[2]** Ringback Tone
 - ◆ **[3]** Busy Tone
 - ◆ **[7]** Reorder Tone
 - ◆ **[8]** Confirmation Tone
 - ◆ **[9]** Call Waiting Tone - heard by the called party
 - ◆ **[15]** Stutter Dial Tone
 - ◆ **[16]** Off Hook Warning Tone
 - ◆ **[17]** Call Waiting Ringback Tone - heard by the calling party
 - ◆ **[18]** Comfort Tone
 - ◆ **[23]** Hold Tone
 - ◆ **[46]** Beep Tone
 - **Tone Modulation Type:** Amplitude Modulated (1) or regular (0)
 - **Tone Form:** The tone's format can be one of the following:
 - ◆ Continuous (1)
 - ◆ Cadence (2)
 - ◆ Burst (3)
 - **Low Freq [Hz]:** Frequency (in Hz) of the lower tone component in case of dual frequency tone, or the frequency of the tone in case of single tone. This is not relevant to AM tones.

- **High Freq [Hz]:** Frequency (in Hz) of the higher tone component in case of dual frequency tone, or zero (0) in case of single tone (not relevant to AM tones).
- **Low Freq Level [-dBm]:** Generation level 0 dBm to -31 dBm in dBm (not relevant to AM tones).
- **High Freq Level:** Generation level of 0 to -31 dBm. The value should be set to 32 in the case of a single tone (not relevant to AM tones).
- **First Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the first cadence on-off cycle. For continuous tones, this parameter defines the detection period. For burst tones, it defines the tone's duration.
- **First Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the first cadence on-off cycle (for cadence tones). For burst tones, this parameter defines the off time required after the burst tone ends and the tone detection is reported. For continuous tones, this parameter is ignored.
- **Second Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the second cadence on-off cycle. Can be omitted if there isn't a second cadence.
- **Second Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the second cadence on-off cycle. Can be omitted if there isn't a second cadence.
- **Third Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the third cadence on-off cycle. Can be omitted if there isn't a third cadence.
- **Third Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the third cadence on-off cycle. Can be omitted if there isn't a third cadence.
- **Fourth Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the fourth cadence on-off cycle. Can be omitted if there isn't a fourth cadence.
- **Fourth Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the fourth cadence on-off cycle. Can be omitted if there isn't a fourth cadence.
- **Carrier Freq [Hz]:** Frequency of the carrier signal for AM tones.
- **Modulation Freq [Hz]:** Frequency of the modulated signal for AM tones (valid range from 1 to 128 Hz).
- **Signal Level [-dBm]:** Level of the tone for AM tones.
- **AM Factor [steps of 0.02]:** Amplitude modulation factor (valid range from 1 to 50). Recommended values from 10 to 25.

**Notes:**

- When the same frequency is used for a continuous tone and a cadence tone, the 'Signal On Time' parameter of the continuous tone must have a value that is greater than the 'Signal On Time' parameter of the cadence tone. Otherwise, the continuous tone is detected instead of the cadence tone.
- The tones frequency must differ by at least 40 Hz between defined tones.

For example, to configure the dial tone to 440 Hz only, enter the following text:

```
[NUMBER OF CALL PROGRESS TONES]
Number of Call Progress Tones=1
#Dial Tone
[CALL PROGRESS TONE #0]
Tone Type=1
Tone Form =1 (continuous)
Low Freq [Hz]=440
High Freq [Hz]=0
Low Freq Level [-dBm]=10 (-10 dBm)
High Freq Level [-dBm]=32 (use 32 only if a single tone is
required)
First Signal On Time [10msec]=300; the dial tone is detected after
3 sec
First Signal Off Time [10msec]=0
Second Signal On Time [10msec]=0
Second Signal Off Time [10msec]=0
```

7.1.1 Distinctive Ringing

Distinctive Ringing is applicable only to FXS interfaces. Using the Distinctive Ringing section of the Call Progress Tones auxiliary file, you can create up to 16 Distinctive Ringing patterns. Each ringing pattern configures the ringing tone frequency and up to four ringing cadences. The same ringing frequency is used for all the ringing pattern cadences. The ringing frequency can be configured in the range of 10 to 200 Hz with a 5 Hz resolution.

Each of the ringing pattern cadences is specified by the following parameters:

- **Burst Ring On Time:** Configures the cadence to be a burst cadence in the entire ringing pattern. The burst relates to On time and the Off time of the same cadence. It must appear between 'First/Second/Third/Fourth' string and the 'Ring On/Off Time'. This cadence rings once during the ringing pattern. Otherwise, the cadence is interpreted as cyclic: it repeats for every ringing cycle.
- **Ring On Time:** Specifies the duration of the ringing signal.
- **Ring Off Time:** Specifies the silence period of the cadence.

The Distinctive Ringing section of the *ini* file format contains the following strings:

- **[NUMBER OF DISTINCTIVE RINGING PATTERNS]:** Contains the following key:
 - 'Number of Distinctive Ringing Patterns' defining the number of Distinctive Ringing signals that are defined in the file.
- **[Ringing Pattern #X]:** Contains the Xth ringing pattern definition (starting from 0 and not exceeding the number of Distinctive Ringing patterns defined in the first section minus 1) using the following keys:
 - **Ring Type:** Must be equal to the Ringing Pattern number.
 - **Freq [Hz]:** Frequency in hertz of the ringing tone.
 - **First (Burst) Ring On Time [10 msec]:** 'Ring On' period (in 10 msec units) for the first cadence on-off cycle.

- **First (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the first cadence on-off cycle.
- **Second (Burst) Ring On Time [10 msec]:** 'Ring On' period (in 10 msec units) for the second cadence on-off cycle.
- **Second (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the second cadence on-off cycle.
- **Third (Burst) Ring On Time [10 msec]:** 'Ring On' period (in 10 msec units) for the third cadence on-off cycle.
- **Third (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the third cadence on-off cycle.
- **Fourth (Burst) Ring On Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the fourth cadence on-off cycle.
- **Fourth (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the fourth cadence on-off cycle.



Note: In SIP, the Distinctive Ringing pattern is selected according to the Alert-Info header in the INVITE message. For example:
Alert-Info:<Bellcore-dr2>, or Alert-Info:<http://.../Bellcore-dr2>
'dr2' defines ringing pattern #2. If the Alert-Info header is missing, the default ringing tone (0) is played.

An example of a **ringing burst** definition is shown below:

```
#Three ringing bursts followed by repeated ringing of 1 sec on and
3 sec off.
[NUMBER OF DISTINCTIVE RINGING PATTERNS]
Number of Ringing Patterns=1
[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
[Ringing Pattern #2]
Ring Type=2
Freq [Hz]=20
First Ring On Time [10msec]=80
First Ring Off Time [10msec]=40
Second Ring On Time [10msec]=80
Second Ring Off Time [10msec]=400
```

7.1.2 FXS Distinctive Ringing and Call Waiting Tones per Source/Destination Number

The device supports the configuration of a Distinctive Ringing tone and Call Waiting Tone per calling (source) and/or called (destination) number (or prefix) for IP-to-Tel calls. This feature can be configured per FXS endpoint or for a range of FXS endpoints. Therefore, different tones can be played per FXS endpoint/s depending on the source and/or destination number of the received call. This configuration is performed using the `ToneIndex` *ini* file table parameter, which maps Ringing and/or Call Waiting tones to source and/or destination number prefixes per FXS endpoint/s.

Typically, the Ringing and/or Call Waiting tone played is indicated in the SIP Alert-info header field of the received INVITE message. If this header is not present in the received INVITE, then this feature is used and the tone played is according to the settings in this table.

For example, to configure Distinctive Ringing and Call Waiting tones of Index #9 in the CPT file for FXS endpoints 1 to 4 when a call is received from a source number with prefix 2, configure the following in the *ini* file:

```
[ToneIndex]
FORMAT ToneIndex_Index = ToneIndex_FXSPort_First,
ToneIndex_FXSPort_Last, ToneIndex_SourcePrefix,
ToneIndex_DestinationPrefix, ToneIndex_PriorityIndex;
ToneIndex_Index 0 = 0, 3, 2, , 1;
[\\ToneIndex]
FirstCallWaitingToneID=8
```

Note that the Call Waiting tone index equals to the priority index plus `FirstCallWaitingToneID(*)`. For example, if you want to select the Call Waiting tone defined in the CPT file at Index #9, then you can enter 1 as the priority index and the value 8 for `FirstCallWaitingToneID`. The summation of these values equals 9, i.e., index #9.

7.2 Prerecorded Tones File

The CPT file mechanism has several limitations such as a limited number of predefined tones and a limited number of frequency integrations in one tone. To overcome these limitations and provide tone generation capability that is more flexible, the Prerecorded Tones (PRT) file can be used. If a specific prerecorded tone exists in the PRT file, it takes precedence over the same tone that exists in the CPT file and is played instead of it.



Note: The PRT are used only for generation of tones. Detection of tones is performed according to the CPT file.

The PRT is a *.dat file containing a set of prerecorded tones that can be played by the device. Up to 40 tones (totaling approximately 10 minutes) can be stored in a single PRT file on the device's flash memory. The prerecorded tones are prepared offline using standard recording utilities (such as CoolEdit™) and combined into a single file using the DConvert utility (refer to the *Product Reference Manual*).

The raw data files must be recorded with the following characteristics:

- **Coders:** G.711 A-law or G.711 μ -law
- **Rate:** 8 kHz
- **Resolution:** 8-bit
- **Channels:** mono

Once created, the PRT file can then be loaded to the device using the Web interface (see "Loading Auxiliary Files" on page 337).

The prerecorded tones are played repeatedly. This allows you to record only part of the tone and then play the tone for the full duration. For example, if a tone has a cadence of 2 seconds on and 4 seconds off, the recorded file should contain only these 6 seconds. The PRT module repeatedly plays this cadence for the configured duration. Similarly, a continuous tone can be played by repeating only part of it.

7.3 CAS Files

The CAS auxiliary files contain the CAS Protocol definitions that are used for CAS-terminated trunks. You can use the supplied files or construct your own files. Up to eight files can be loaded to the device. Different files can be assigned to different trunks (CASTableIndex_x) and different CAS tables can be assigned to different B-channels (CASChannelIndex).

The CAS files can be loaded to the device using the Web interface or *ini* file (see "Loading Auxiliary Files" on page 337).



Note: All CAS files loaded together must belong to the same Trunk Type (i.e., either E1 or T1).

7.4 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 a detailed description, see [Dial Plan Prefix Tags for IP-to-Tel Routing](#) on page 418.

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 337).

The Dial Plan file must be prepared in a textual *ini* file with the following syntax:

- Every line in the file defines a known dialing prefix and the number of digits expected to follow that prefix. The prefix must be separated from the number of additional digits by a comma (',').
- Empty lines are ignored.
- Lines beginning with a semicolon (;) are ignored.
- Multiple dial plans may be specified in one file; a name in square brackets on a separate line indicates the beginning of a new dial plan. Up to eight dial plans can be defined.
- Asterisks (**) and number-signs (#) can be specified as part of the prefix.
- Numeric ranges are allowed in the prefix.
- A numeric range is allowed in the number of additional digits.



Notes:

- The prefixes must not overlap. Attempting to process an overlapping configuration by the DConvert utility results in an error message specifying the problematic line.
- For a detailed description on working with Dial Plan files, see "External Dial Plan File" on page 415.

An example of a Dial Plan file in *ini*-file format (i.e., before converted to *.dat) that contains two dial plans is shown below:

```
; Example of dial-plan configuration.
; This file contains two dial plans:
[ PLAN1 ]
; Defines cellular/VoIP area codes 052, 054, and 050.
; In these area codes, phone numbers have 8 digits.
052,8
054,8
050,8
; Defines International prefixes 00, 012, 014.
; The number following these prefixes may
; be 7 to 14 digits in length.
00,7-14
012,7-14
014,7-14
; Defines emergency number 911.
; No additional digits are expected.
911,0
[ PLAN2 ]
; Defines area codes 02, 03, 04.
; In these area codes, phone numbers have 7 digits.
0[2-4],7
; Operator services starting with a star: *41, *42, *43.
; No additional digits are expected.
*4[1-3],0
```

7.5 User Information File

The User Information file is a text file that maps PBX extensions connected to the device to global IP numbers. In this context, a global IP phone number (alphanumeric) 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 7-1: User Information Items

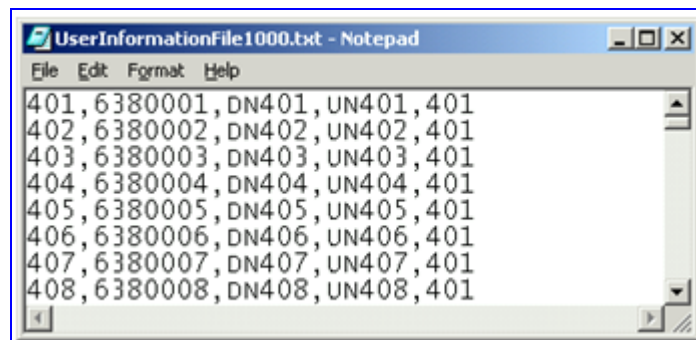
Item	Description	Maximum Size (Characters)
PBX extension #	The relevant PBX extension number.	10
Global phone #	The relevant global phone number.	20
Display name	A string that represents the PBX extensions for the Caller ID.	30
Username	A string that represents the user name for SIP registration.	40
Password	A string that represents the password for SIP registration.	20



Note: For FXS ports, when the device is required to send a new request with the 'Authorization' header (for example, after receiving a SIP 401 reply), it uses the user name and password from the Authentication table. To use the username and password from the User Info file, change the parameter 'Password' from its default value.

An example of a User Information file is shown in the figure below:

Figure 7-1: Example of a User Information File





Note: The last line in the User Information file must end with a carriage return (i.e., by pressing the <Enter> key).

The User Information file can be loaded to the device by using one of the following methods:

- *ini* file, using the parameter `UserInfoFileName` (described in "Auxiliary and Configuration Files Parameters" on page 881)
- Web interface (see "Loading Auxiliary Files" on page 337)
- Automatic update mechanism, using the parameter `UserInfoFileURL` (refer to the *Product Reference Manual*)

Each PBX extension registers separately (a REGISTER message is sent for each entry only if `AuthenticationMode` is set to Per Endpoint) using the "Global phone number" in the From/To headers. The REGISTER messages are sent gradually. Initially, the device sends requests according to the maximum number of allowed SIP dialogs (configured by the parameter `NumberOfActiveDialogs`). After each received response, the subsequent request is sent. Therefore, no more than `NumberOfActiveDialogs` dialogs are active simultaneously. The user name and password are used for SIP Authentication when required.

The calling number of outgoing Tel-to-IP calls is translated to a "Global phone number" only after Tel-to-IP manipulation rules (if defined) are performed. The Display Name is used in the From header in addition to the "Global phone number". The called number of incoming IP-to-Tel calls is translated to a PBX extension only after IP-to-Tel manipulation rules (if defined) are performed.

Reader's Notes

8 IP Telephony Capabilities

This section describes the device's main IP telephony capabilities.

8.1 Multiple SIP Signaling and Media Interfaces

The device supports multiple, logical SIP signaling interfaces and RTP (media) traffic interfaces. This allows you to separate SIP signaling messages and media traffic between different applications (i.e., SAS, Gateway\IP-to-IP, and SBC), and/or between different networks (e.g., when operating with multiple ITSP's). Multiple SIP signaling and RTP interfaces are configured using Signaling Routing Domains (SRD), as described in "Signaling Routing Domains" on page 405.

For an example configuration of multiple SIP signaling and media interfaces, see "Multiple SIP Signaling and Media Configuration Example" on page 408.

8.1.1 Signaling Routing Domains

A Signaling Routing Domain (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:

- **Media Realm:** The Media Realm defines a media port range associated with a Media IP interface (defined in the Multiple Interface table in "Configuring IP Interface Settings" on page 83). Media Realms are defined in the SIP Media Realm table (see "Media Realms" on page 406) and then later assigned to an SRD (in the SRD table).
- **SIP Interface:** A SIP signaling interface is a combination of UDP, TCP, and TLS ports associated with a specific IP address (network interface, configured in the Multiple Interface table). SIP Interfaces are defined in the SIP Signaling Interface table (see "SIP Interfaces" on page 406) where they are also assigned to specific SRDs.

Once configured, you can use an SRD as follows:

- Associate it with a SIP Interface (see "Configuring SIP Interface Table" on page 117)
- Associate it with an IP Group (see Configuring IP Groups on page 119)
- Associate it with a Proxy Set (see Configuring Proxy Sets Table on page 126)
- Apply an Admission Control rule to it (see Configuring Admission Control Table on page 195)
- Define it as a Classification rule for the incoming SIP request (see Configuring Classification Table on page 198)
- Define it as a destination IP-to-IP routing rule (see "Configuring IP-to-IP Routing Table" on page 201)

SRD provides the following capabilities:

- Multiple, different SIP signaling (SRD associated with a SIP Interface, described later) and RTP media (associated with a Media Realm) interfaces for multiple Layer-3 networks. Due to the B2BUA nature of the SBC application, different interfaces can be assigned to each leg of the call, and between the LAN side and the WAN side.
- Ability to 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

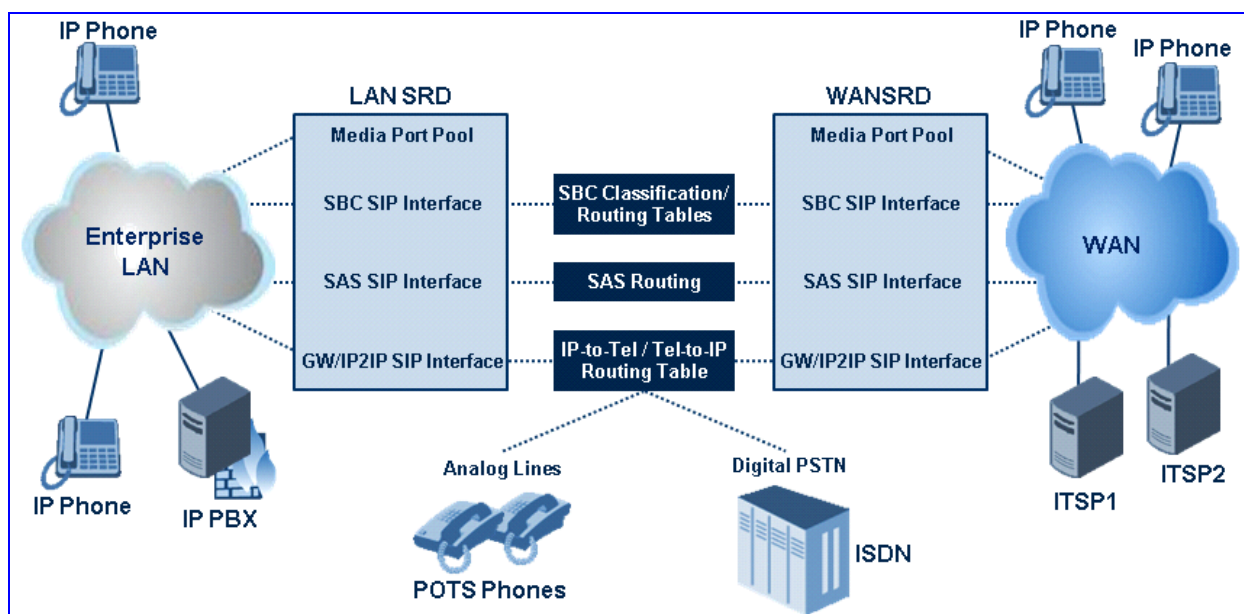
traffic between different customers. In such a scenario, the device is configured with multiple SRD's.

Typically, one SRD is defined per group of SIP User Agents/UA (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). Typically, one SRD is configured for the LAN and one SRD is configured for the WAN.

Routing from one SRD to another is possible, where each routing destination (IP Group or destination address) must indicate the SRD to which it belongs.

The figure below illustrates two SRD's - one for LAN and one for WAN. Each of the applications (i.e., SAS, GatewayIP2IP, and SBC) pertain to the same SRD, but each has its own SIP interface.

Figure 8-1: Example Showing SIP Interfaces per Application within SRD



8.1.1.1 Media Realms

A Media Realm is a range of UDP ports that is associated with a media IP interface/IP address (defined in the Multiple Interface table). Media Realms allow you to divide a media (RTP traffic) IP interface into several realms, where each realm is specified by a UDP port range. The pool of media interfaces (i.e., Media Realms) are defined in the SIP Media Realm table (CpMediaRealm parameter). Once created, the Media Realm can be assigned to other entities for routing (e.g., to an IP Group in the 'IP Group' table and to an SRD in the 'SRD' table). For defining Media Realms, see "Configuring Media Realms" on page 109.

8.1.1.2 SIP Interfaces

A SIP Interface represents one SIP signaling entity, which is a combination of UDP, TCP, and TLS ports relating to one specific IP address (network interface, configured in the Multiple Interface table). SIP Interfaces are configured in the SIP Interface table (see "Configuring SIP Interface Table" on page 117), each associated with an SRD. This allows User Agents on the network to communicate with a specific SRD, using the SIP Interface (signaling interface) associated with it.

Each SRD may be associated with up to three SIP Interfaces (one per application type - SAS, Gateway\IP-to-IP, and SBC). Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no overlapping).

SIP Interfaces are used for the following:

- Defining different SIP signaling ports (listening UDP, TCP, and TLS, and the UDP source ports) for single or multiple interfaces.
- Differentiating between the different application types supported by the device. 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.
- Separating signaling traffic of different customers to use different routing tables, manipulations, SIP definitions, etc.

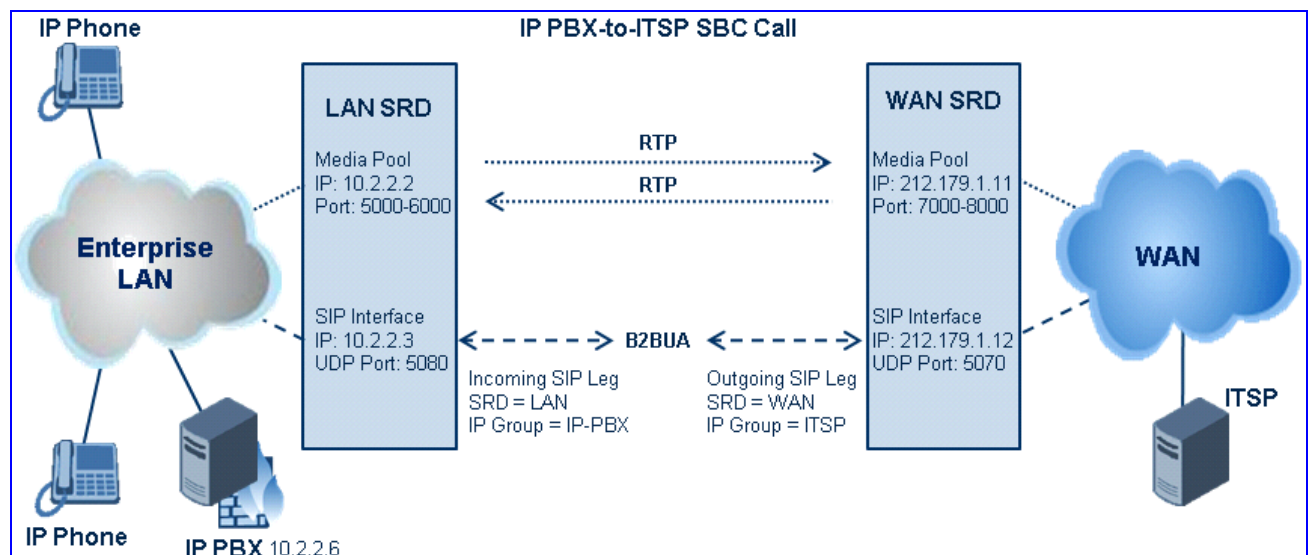
The figure below illustrates the SBC call flow between an enterprises LAN (IP PBX) and an ITSP (WAN) implementing different interfaces (IP addresses and ports) for RTP packets and SIP signaling. In addition, for each leg (LAN and WAN side), different interfaces are used.

The example uses the following IP addresses:

- IP-PBX: 10.2.2.6
- LAN MSBG: 10.2.2.3
- WAN MSBG: 212.179.1.12
- ITSP: 212.179.1.13
- MSBG LAN Media: 10.2.2.2:5000-6000
- MSBG WAN Media: 212.179.1.11:7000-8000

Figure 8-2: Back-to-Back SBC Call Flow (RTP and Signaling)

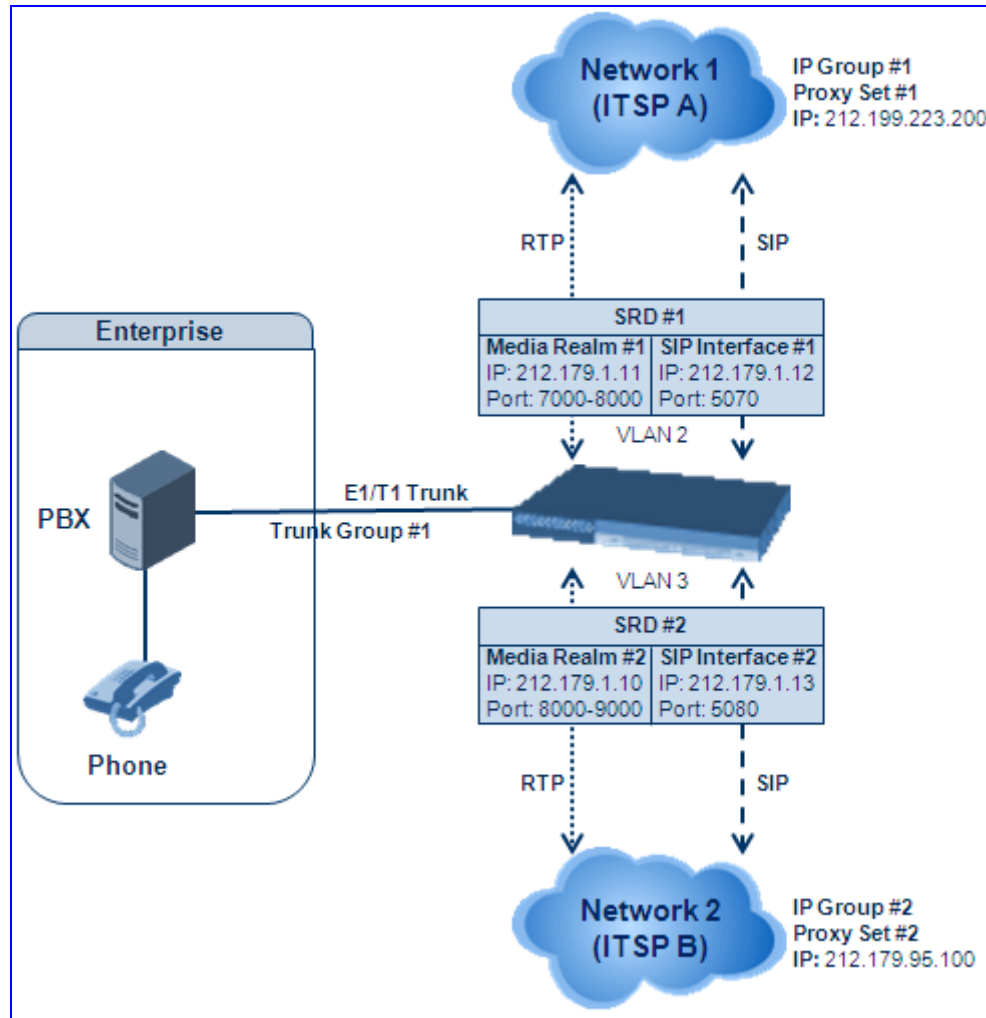
Figure 8-3: Back-to-Back SBC Call Flow (RTP and Signaling)



8.1.2 Multiple SIP Signaling and Media Configuration Example

This section 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 8-4: 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 > **Hunt Group** > **Hunt Group**), as shown in the figure below:

Figure 8-5: Defining a Trunk Group for PSTN

▼							
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 > **Hunt Group** > **Hunt Group Settings**).
3. Configure the IP interfaces in the 'Multiple Interface Table' page (**Configuration** tab > **VoIP** menu > **Network** submenu > **IP Settings**):

Figure 8-6: Defining IP Interfaces

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	<input type="radio"/> QAMP + Media + Control	192.168.0.2	24	192.168.0.1	1	Voice
1	<input type="radio"/> Media	212.179.1.11	16	0.0.0.0	2	Media1
2	<input type="radio"/> Media	212.179.1.10	16	0.0.0.0	3	Media2
3	<input type="radio"/> Control	212.179.1.12	16	0.0.0.0	2	SIP1
4	<input type="radio"/> Control	212.179.1.13	16	0.0.0.0	3	SIP2

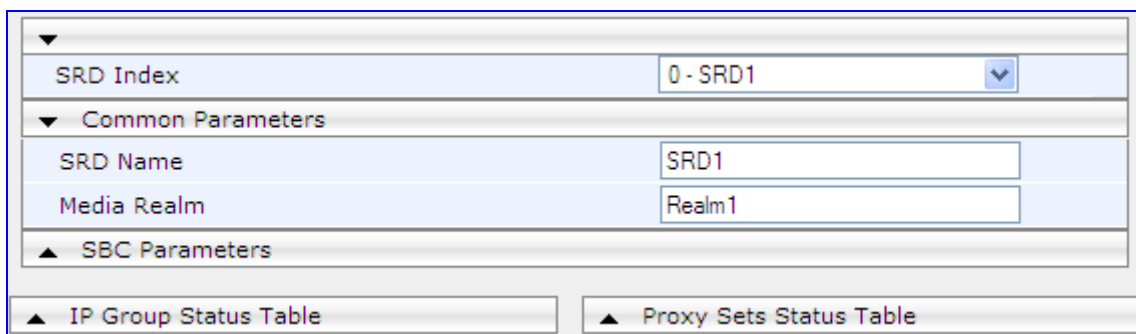
4. Configure SIP Media Realms in the 'SIP Media Realm Table' page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Realm Configuration**):

Figure 8-7: Defining Media Realms

Index	Media Realm Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End
1	<input type="radio"/> Realm1	Media1	7000	101	8000
2	<input type="radio"/> Realm2	Media2	8020	20	8210

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

Figure 8-8: Defining SRDs



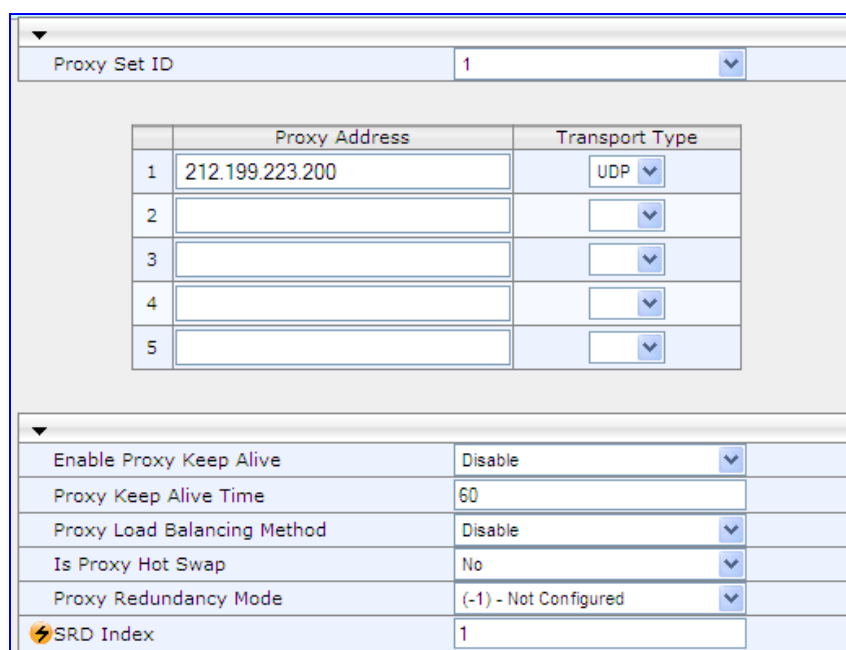
6. Configure the SIP Interfaces in the 'SIP Interface Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SIP Interface Table**):

Figure 8-9: Defining SIP Interfaces

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	<input type="radio"/> SIP1	Gw\IP2IP	5070	5070	5071	1
2	<input type="radio"/> 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 8-10: Defining Proxy Set



8. 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 8-11: 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 ▼

9. 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 8-12: 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							

10. 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 8-13: 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 ▼

8.2 Dynamic Jitter Buffer Operation

Voice frames are transmitted at a fixed rate. If the frames arrive at the other end at the same rate, voice quality is perceived as good. In many cases, however, some frames can arrive slightly faster or slower than the other frames. This is called jitter (delay variation), and degrades the perceived voice quality. To minimize this problem, the device uses a jitter buffer. The jitter buffer collects voice packets, stores them and sends them to the voice processor in evenly spaced intervals.

The device uses a dynamic jitter buffer that can be configured using the following parameters:

- **Minimum delay:** DJBufMinDelay (0 msec to 150 msec)
Defines the starting jitter capacity of the buffer. For example, at 0 msec, there is no buffering at the start. At the default level of 10 msec, the device always buffers incoming packets by at least 10 msec worth of voice frames.
- **Optimization Factor:** DJBufOptFactor (0 to 12, 13)
Defines how the jitter buffer tracks to changing network conditions. When set at its maximum value of 12, the dynamic buffer aggressively tracks changes in delay (based on packet loss statistics) to increase the size of the buffer and doesn't decay back down. This results in the best packet error performance, but at the cost of extra delay. At the minimum value of 0, the buffer tracks delays only to compensate for clock drift and quickly decays back to the minimum level. This optimizes the delay performance but at the expense of a higher error rate.

The default settings of 10 msec Minimum delay and 10 Optimization Factor should provide a good compromise between delay and error rate. The jitter buffer 'holds' incoming packets for 10 msec before making them available for decoding into voice. The coder polls frames from the buffer at regular intervals in order to produce continuous speech. As long as delays in the network do not change (jitter) by more than 10 msec from one packet to the next, there is always a sample in the buffer for the coder to use. If there is more than 10 msec of delay at any time during the call, the packet arrives too late. The coder tries to access a frame and is not able to find one. The coder must produce a voice sample even if a frame is not available. It therefore compensates for the missing packet by adding a Bad-Frame-Interpolation (BFI) packet. This loss is then flagged as the buffer being too small. The dynamic algorithm then causes the size of the buffer to increase for the next voice session. The size of the buffer may decrease again if the device notices that the buffer is not filling up as much as expected. At no time does the buffer decrease to less than the minimum size configured by the Minimum delay parameter.

For certain scenarios, the **Optimization Factor is set to 13**: One of the purposes of the Jitter Buffer mechanism is to compensate for clock drift. If the two sides of the VoIP call are not synchronized to the same clock source, one RTP source generates packets at a lower rate, causing under-runs at the remote Jitter Buffer. In normal operation (optimization factor 0 to 12), the Jitter Buffer mechanism detects and compensates for the clock drift by occasionally dropping a voice packet or by adding a BFI packet.

Fax and modem devices are sensitive to small packet losses or to added BFI packets. Therefore, to achieve better performance during modem and fax calls, the Optimization Factor should be set to 13. In this special mode the clock drift correction is performed less frequently - only when the Jitter Buffer is completely empty or completely full. When such condition occurs, the correction is performed by dropping several voice packets simultaneously or by adding several BFI packets simultaneously, so that the Jitter Buffer returns to its normal condition.

8.3 Gateway and IP-to-IP

This section describes various Gateway and IP-to-IP application features.

8.3.1 Dialing Plan Features

This section discusses various dialing plan features supported by the device:

- Dialing plan notations (see "Dialing Plan Notation for Routing and Manipulation" on page 413)
- Digit mapping (see "Digit Mapping" on page 414)
- External Dial Plan file containing dial plans (see "External Dial Plan File" on page 415)
- Dial plan prefix tags for enhanced IP-to-Tel routing (see Dial Plan Prefix Tags for IP-to-Tel Routing on page 418)

8.3.1.1 Dialing Plan Notation for Routing and Manipulation

The device supports flexible dialing plan notations for representing digits (single or multiple) entered for destination and source prefixes (of phone numbers and SIP URI user names) in the routing and manipulation tables.

Table 8-1: Dialing Plan Notations

Notation	Description	Example
[n-m]	Represents a range of numbers. Note: Range of letters is not supported.	<ul style="list-style-type: none"> ■ [5551200-5551300]#: represents all numbers from 5551200 to 5551300. ■ 123[100-200]: represents all numbers from 123100 to 123200.
[n,m,...]	Represents multiple numbers. Up to three digits can be used to denote each number.	<ul style="list-style-type: none"> ■ [2,3,4,5,6]#: represents a one-digit number starting with 2, 3, 4, 5, or 6. ■ [11,22,33]xxx#: represents a five-digit number that starts with 11, 22, or 33. ■ [111,222]xxx#: represents a six-digit number that starts with 111 or 222.
[n1-m1,n2-m2,a,b,c,n3-m3]	Represents a mixed notation of multiple ranges and single numbers. Note: The ranges and the single numbers must have the same number of digits. For example, each number range and single number in the dialing plan [123-130,455,577,780-790] consists of three digits.	[123-130,455,766,780-790] : represents numbers 123 to 130, 455, 766, and 780 to 790.
x	Represents any single digit.	-

Notation	Description	Example
Pound sign (#) at the end of a number	Represents the end of a number.	54324xx# : represents a 7-digit number that starts with 54324.
A single asterisk (*)	Represents any number.	* : represents any number (i.e., all numbers).

8.3.1.2 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 a detailed description of digit maps for ISDN overlapping, see ISDN Overlap Dialing on page 642. The device collects digits until a match is found in the user-defined digit pattern (e.g., for closed numbering schemes). The device stops collecting digits and starts sending the digits (collected number) when any one of the following scenarios occur:

- Maximum number of digits is received. You can define (using the MaxDigits parameter) the maximum number of collected destination number digits that can be received (i.e., dialed) from the Tel side by the device. When the number of collected digits reaches the maximum (or a digit map pattern is matched), the device uses these digits for the called destination number.
- Inter-digit timeout expires (e.g., for open numbering schemes). This is defined using the TimeBetweenDigits parameter. This is the time that the device waits between each received digit. When this inter-digit timeout expires, the device uses the collected digits to dial the called destination number.
- The phone's pound (#) key is pressed.
- Digit string (i.e., dialed number) matches one of the patterns defined in the digit map.

Digit map (pattern) rules are defined using the DigitMapping parameter. The digit map pattern can contain up to 52 options (rules), each separated by a vertical bar ("|"). The maximum length of the entire digit pattern is 152 characters. The available notations are described in the table below:

Table 8-2: Digit Map Pattern Notations

Notation	Description
[n-m]	Range of numbers (not letters).
.	(single dot) Repeat digits until next notation (e.g., T).
x	Any single digit.
T	Dial timeout (configured by the TimeBetweenDigits parameter).
S	Short timer (configured by the TimeBetweenDigits parameter; default is two seconds) that can be used when a specific rule is defined after a more general rule. For example, if the digit map is 99 998, then the digit collection is terminated after the first two 9 digits are received. Therefore, the second rule of 998 can never be matched. But when the digit map is 99s 998, then after dialing the first two 9 digits, the device waits another two seconds within which the caller can enter the digit 8.

Below is an example of a digit map pattern containing eight rules:

```
DigitMapping = 11xS|00[1-7]xxx|8xxxxxxx|#xxxxxxx|*xx|91xxxxxxxxxxxx|9011x|xx.T
```

In the example, the rule "00[1-7]xxx" denotes dialed numbers that begin with 00, and then any digit from 1 through 7, followed by three digits (of any number). Once the device receives these digits, it does not wait for additional digits, but starts sending the collected digits (dialed number) immediately.



Notes:

- If you want the device to accept/dial any number, ensure that the digit map contains the rule "xx.T"; otherwise, dialed numbers not defined in the digit map are rejected.
- If you are using an external Dial Plan file for dialing plans (see "External Dial Plan File" on page 415), the device first attempts to locate a matching digit pattern in the Dial Plan file, and if not found, then attempts to locate a matching digit pattern in the Digit Map (configured by the DigitMapping parameter).
- It may be useful to configure both Dial Plan file and Digit Maps. For example, the Digit Map can be used for complex digit patterns (which are not supported by the Dial Plan) and the Dial Plan can be used for long lists of relatively simple digit patterns. In addition, as timeout between digits is not supported by the Dial Plan, the Digit Map can be used to define digit patterns (MaxDigits parameter) that are shorter than those defined in the Dial Plan, or left at default. For example, "xx.T" Digit Map instructs the device to use the Dial Plan and if no matching digit pattern, it waits for two more digits and then after a timeout (TimeBetweenDigits parameter), it sends the collected digits. Therefore, this ensures that calls are not rejected as a result of their digit pattern not been completed in the Dial Plan.

8.3.1.3 External Dial Plan File

The device allows you to select a specific Dial Plan (index) defined in an external Dial Plan file. This file is loaded to the device as a *.dat file (binary file), converted from an *ini* file using the DConvert utility. This file can include up to eight Dial Plans (Dial Plan indices), with a total of up to 8,000 dialing rules (lines). The required Dial Plan is selected using the DialPlanIndex parameter. This parameter can use values 0 through 7, where 0 denotes PLAN1, 1 denotes PLAN2, and so on. The Dial Plan index can be configured globally or per Tel Profile.

The format of the Dial Plan index file is as follows:

- A name in square brackets ("[...]") on a separate line indicates the beginning of a new Dial Plan index.
- Every line under the Dial Plan index defines a dialing prefix and the number of digits expected to follow that prefix. The prefix is separated by a comma (",") from the number of additional digits.
- The prefix can include numerical ranges in the format [x-y], as well as multiple numerical ranges [n-m][x-y] (no comma between them).

- The prefix can include asterisks ("*") and number signs ("#").
- The number of additional digits can include a numerical range in the format x-y.
- Empty lines and lines beginning with a semicolon (";") are ignored.

An example of a Dial Plan file with indices (in *ini*-file format before conversion to binary *.dat) is shown below:

```
[ PLAN1 ]
; Area codes 02, 03, - phone numbers include 7 digits.
02,7
03,7
; Cellular/VoIP area codes 052, 054 - phone numbers include 8
digits.
052,8
054,8
; International prefixes 00, 012, 014 - number following
prefix includes 7 to 14 digits.
00,7-14
012,7-14
014,7-14
; Emergency number 911 (no additional digits expected).
911,0
[ PLAN2 ]
; Supplementary services such as Call Camping and Last Calls
(no additional digits expected), by dialing *41, *42, or *43.
*4[1-3],0
```



Notes:

- If you are using an external Dial Plan file for dialing plans (see "External Dial Plan File" on page 415), 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.
- 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.

8.3.1.3.1 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 337), 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.

8.3.1.4 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 Hunt 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 Hunt Group (e.g. Hunt Group ID 1).

- The 'Dest. Phone Prefix' field is set to the value "LONG" and this rule is assigned to a long distance Hunt Group (e.g. Hunt Group ID 2).

Figure 8-14: Configuring Dial Plan File Label for IP-to-Tel Routing

<div> <div>Routing Index</div> <div>1-12</div> </div> <div> <div>IP To Tel Routing Mode</div> <div>Route calls before manipulation</div> </div>						
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	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 8-15: Configuring Manipulation for Removing Label

Index	Destination Prefix	Source Prefix	Source IP Address	Stripped Digits From Left
1	LOCL	*	*	4
2	LONG	*	*	4

8.3.2 Manipulating Number Prefix

The device supports a notation for adding a prefix where part of the prefix is first extracted from a user-defined location in the original destination or source number. This notation is entered in the 'Prefix to Add' field in the Number Manipulation tables (see "Manipulation" on page 151):

$x[n,l]y...$

where,

- x = any number of characters/digits to add at the beginning of the number (i.e. first digits in the prefix).
- $[n,l]$ = defines the location in the original destination or source number where the digits y are added:
 - n = location (number of digits counted from the left of the number) of a specific string in the original destination or source number.
 - l = number of digits that this string includes.
- y = prefix to add at the specified location.

For example, assume that you want to manipulate an incoming IP call with destination number +5492028888888 (area code 202 and phone number 8888888) to the number 0202158888888. To perform such a manipulation, the following configuration is required in the Number Manipulation table:

1. The following notation is used in the 'Prefix to Add' field:
0[5,3]15
where,
 - 0 is the number to add at the beginning of the original destination number.
 - [5,3] denotes a string that is located after (and including) the fifth character (i.e., the first '2' in the example) of the original destination number, and its length being three digits (i.e., the area code 202, in the example).
 - 15 is the number to add immediately after the string denoted by [5,3] - in other words, 15 is added after (i.e. to the right of) the digits 202.
2. The first seven digits from the left are removed from the original number, by entering "7" in the 'Stripped Digits From Left' field.

Figure 8-16: Prefix to Add Field with Notation

Index	Destination Prefix	Source Prefix	Source IP Address	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add
1	+5492028888888	*	*	7	0	0[5,3]15

In this configuration, the following manipulation process occurs: 1) the prefix is calculated, 020215 in the example; 2) the first seven digits from the left are removed from the original number, in the example, the number is changed to 8888888; 3) the prefix that was previously calculated is then added.

8.3.3 Emergency Phone Number Services - E911

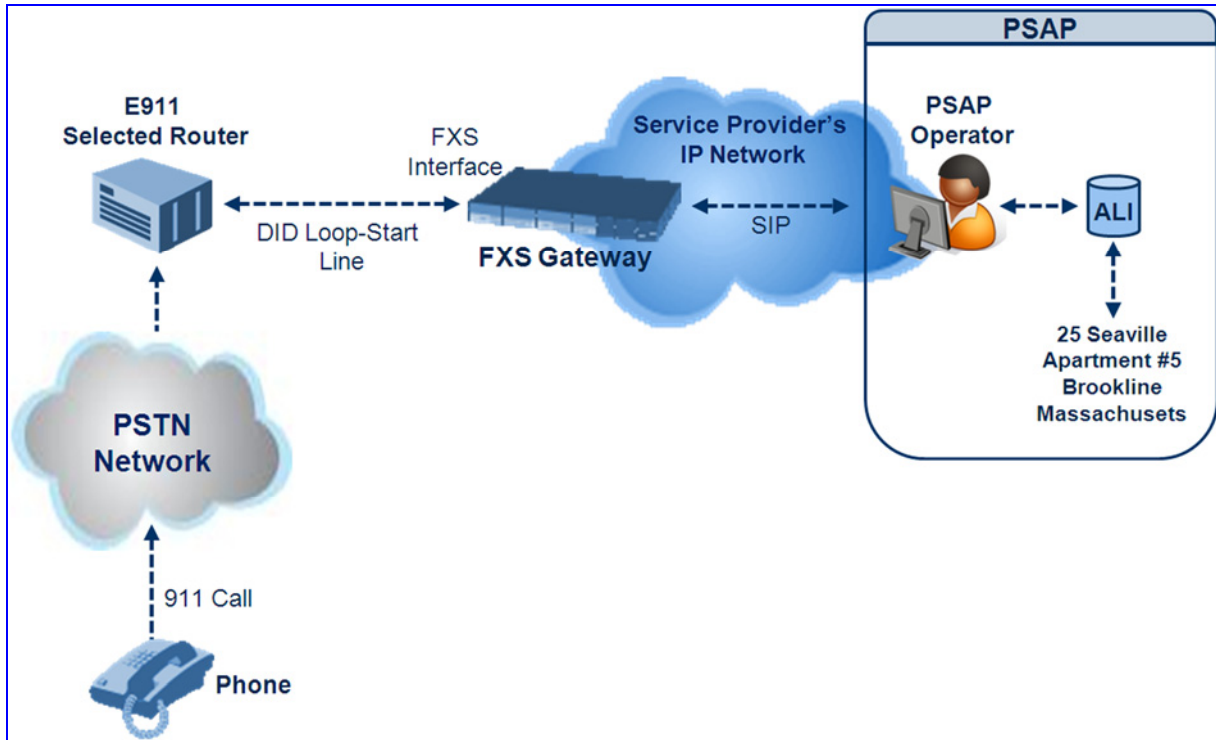
The device supports emergency phone number services. The device supports the North American emergency telephone number system known as Enhanced 911 (E911), according to the TR-TSY-000350 and Bellcore's GR-350-Jun2003 standards. The E911 emergency system automatically associates a physical address with 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).

8.3.3.1 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 8-17: 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 "hookflash" 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 8-3: 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.

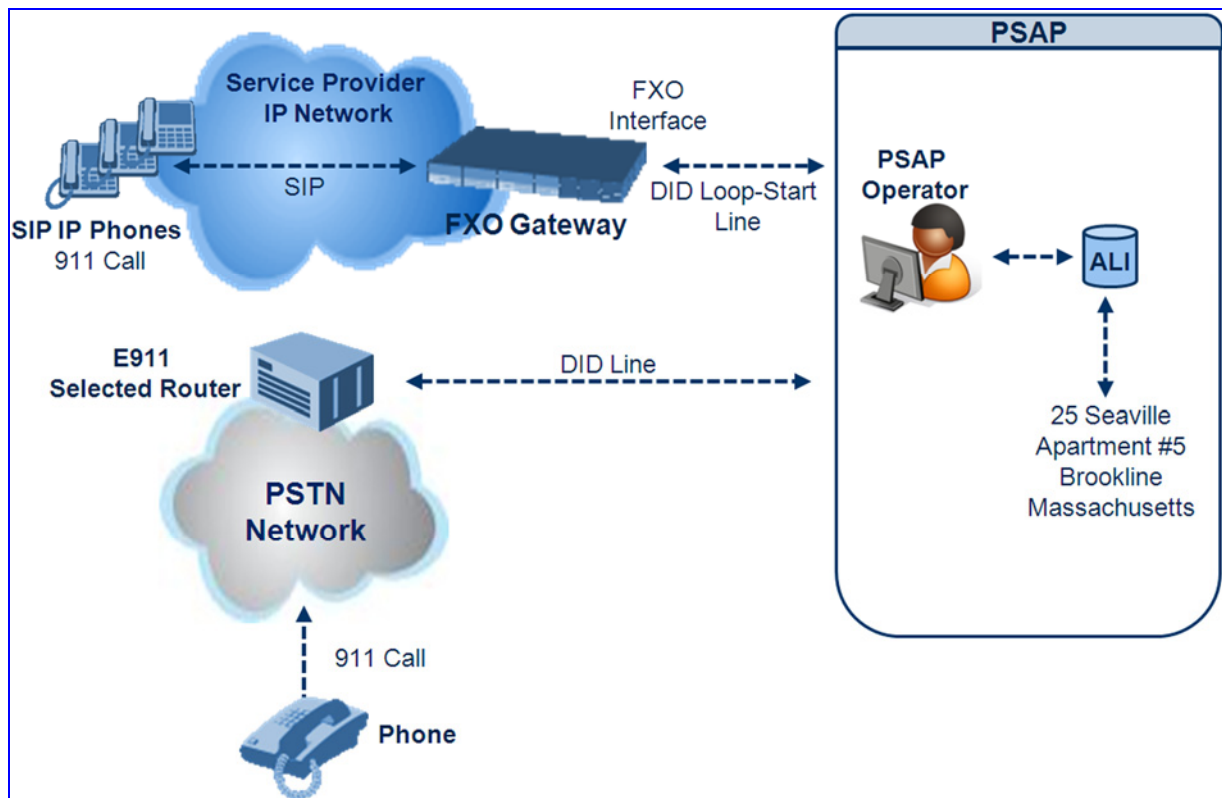
If the device receives the SIP INFO message below, it then generates a "hookflash" mid-call Wink signal:

```
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
```

8.3.3.2 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 8-18: 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 8-4: 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 "00INXXXXXX".
- 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
```

8.3.3.3 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 Hunt Group for which the E911 call was initially destined and if the channel select mode (configured by the ChannelSelectMode parameter) is set to other than "By Dest Number" (0).

The preemption is done only if the incoming IP-to-Tel call is identified as an emergency call. The device identifies emergency calls by one of the following:

- The destination number of the IP call matches one of the numbers defined by the EmergencyNumbers parameter. (For E911, you must 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 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.

8.3.4 Configuring DTMF Transport Types

You can control the way DTMF digits are transported over the IP network to the remote endpoint, by using one of the following modes:

- **Using INFO message according to Nortel IETF draft:** DTMF digits are carried to the remote side in INFO messages. To enable this mode, define the following:

- RxDTMFOption = 0
- TxDTMFOption = 1

Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0).

- **Using INFO message according to Cisco's mode:** DTMF digits are carried to the remote side in INFO messages. To enable this mode, define the following:

- RxDTMFOption = 0
- TxDTMFOption = 3

Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0).

- **Using NOTIFY messages according to IETF Internet-Draft draft-mahy-sipping-signaled-digits-01:** DTMF digits are carried to the remote side using NOTIFY messages. To enable this mode, define the following:

- RxDTMFOption = 0
- TxDTMFOption = 2

Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0).

- **Using RFC 2833 relay with Payload type negotiation:** DTMF digits are carried to the remote side as part of the RTP stream in accordance with RFC 2833 standard. To enable this mode, define the following:

- RxDTMFOption = 3
- TxDTMFOption = 4

Note that to set the RFC 2833 payload type with a different value (other than its default), configure the RFC2833PayloadType parameter. The device negotiates the RFC 2833 payload type using local and remote SDP and sends packets using the payload type from the received SDP. The device expects to receive RFC 2833 packets with the same payload type as configured by the RFC2833PayloadType parameter. If the remote side doesn't include 'telephony-event' in its SDP, the device sends DTMF digits in transparent mode (as part of the voice stream).

- **Sending DTMF digits (in RTP packets) as part of the audio stream (DTMF Relay is disabled):** This method is typically used with G.711 coders; with other low-bit rate (LBR) coders, the quality of the DTMF digits is reduced. To enable this mode, define the following:

- RxDTMFOption = 0 (i.e., disabled)
- TxDTMFOption = 0 (i.e., disabled)
- DTMFTransportType = 2 (i.e., transparent)

- **Using INFO message according to Korea mode:** DTMF digits are carried to the remote side in INFO messages. To enable this mode, define the following:
 - RxDTMFOption = 0 (i.e., disabled)
 - TxDTMFOption = 3

Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0).



Notes:

- The device is always ready to receive DTMF packets over IP in all possible transport modes: INFO messages, NOTIFY, and RFC 2833 (in proper payload type) or as part of the audio stream.
- To exclude RFC 2833 Telephony event parameter from the device's SDP, set RxDTMFOption to 0 in the *ini* file.

The following parameters affect the way the device handles the DTMF digits:

- TxDTMFOption, RxDTMFOption, and RFC2833PayloadType
- MGCPDTMFDetectionPoint, DTMFVolume, DTMFTransportType, DTMFDigitLength, and DTMFInterDigitInterval

8.3.5 FXS and FXO Capabilities

8.3.5.1 FXS/FXO Coefficient Types

The FXS Coefficient and FXO Coefficient types used by the device can be one of the following:

- US line type of 600 ohm AC impedance and 40 V RMS ringing voltage for REN = 2
- European standard (TBR21)

These types can be selected using the *ini* file parameters FXSCountryCoefficients (for FXS) and CountryCoefficients (for FXO), or using the Web interface (see "Configuring Analog Settings" on page 108).

These Coefficient types are used to increase return loss and trans-hybrid loss performance for two telephony line type interfaces (US or European). This adaptation is performed by modifying the telephony interface characteristics. This means, for example, that changing impedance matching or hybrid balance doesn't require hardware modifications, so that a single device is able to meet requirements for different markets. The digital design of the filters and gain stages also ensures high reliability, no drifts (over temperature or time) and simple variations between different line types.

The FXS Coefficient types provide best termination and transmission quality adaptation for two FXS line type interfaces. This parameter affects the following AC and DC interface parameters:

- DC (battery) feed characteristics
- AC impedance matching
- Transmit gain
- Receive gain
- Hybrid balance
- Frequency response in transmit and receive direction
- Hook thresholds
- Ringing generation and detection parameters

8.3.5.2 FXO Operating Modes

This section provides a description of the device's FXO operating modes:

- For IP-to-Tel calls (see "FXO Operations for IP-to-Tel Calls" on page 430)
- For Tel-to-IP calls (see "FXO Operations for Tel-to-IP Calls" on page 433)
- Call termination on FXO devices (see "Call Termination on FXO Devices" on page 436)

8.3.5.2.1 FXO Operations for IP-to-Tel Calls

The FXO device provides the following operating modes for IP-to-Tel calls:

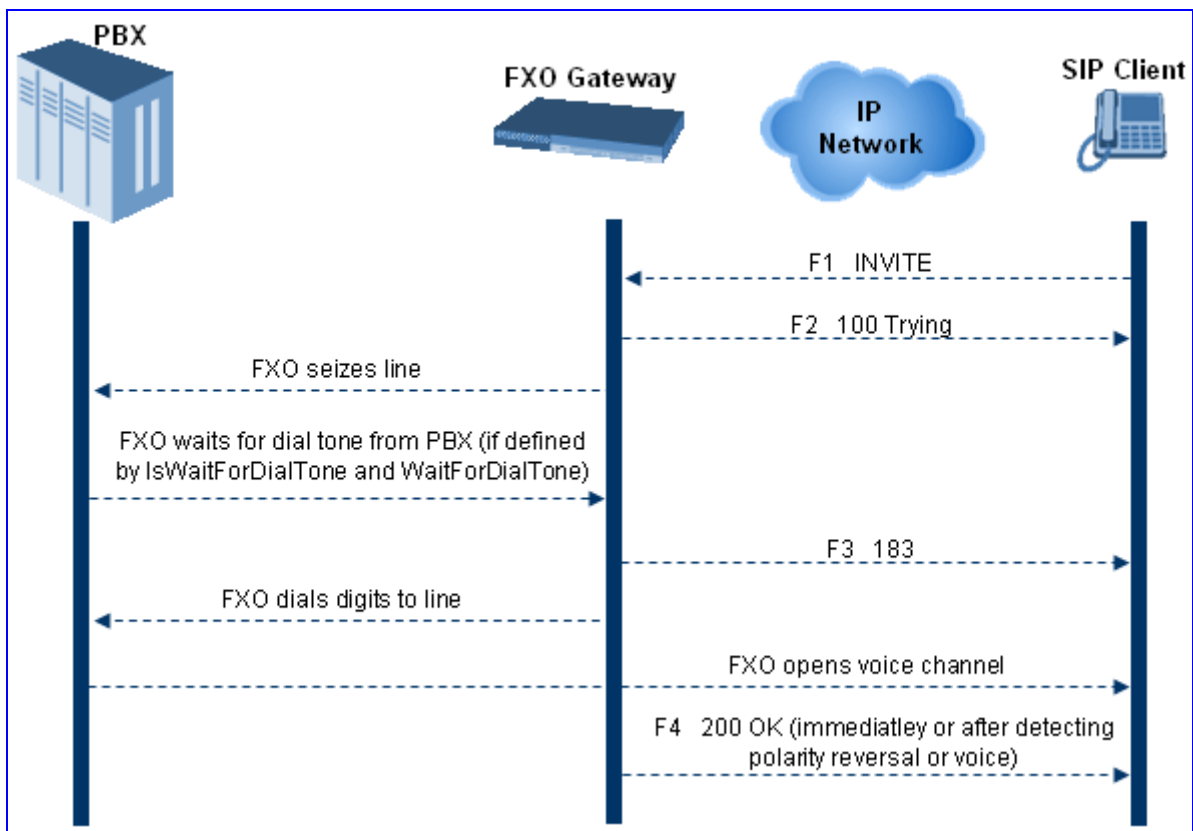
- One-stage dialing (see "One-Stage Dialing" on page 431)
 - Waiting for dial tone (see "Two-Stage Dialing" on page 432)

- Time to wait before dialing
- Answer supervision
- Two-stage dialing (see "Two-Stage Dialing" on page 432)
- Dialing time: DID wink (see "DID Wink" on page 433)

8.3.5.2.1.1 One-Stage Dialing

One-stage dialing is when the FXO device receives an IP-to-Tel call, off-hooks the PBX line connected to the telephone, and then immediately dials the destination telephone number. In other words, the IP caller doesn't dial the PSTN number upon hearing a dial tone.

Figure 8-19: Call Flow for One-Stage Dialing



One-stage dialing incorporates the following FXO functionality:

- **Waiting for Dial Tone:** Enables the device to dial the digits to the Tel side only after detecting a dial tone from the PBX line. The *ini* file parameter *IsWaitForDialTone* is used to configure this operation.
- **Time to Wait Before Dialing:** Defines the time (in msec) between seizing the FXO line and starting to dial the digits. The *ini* file parameter *WaitForDialTime* is used to configure this operation.



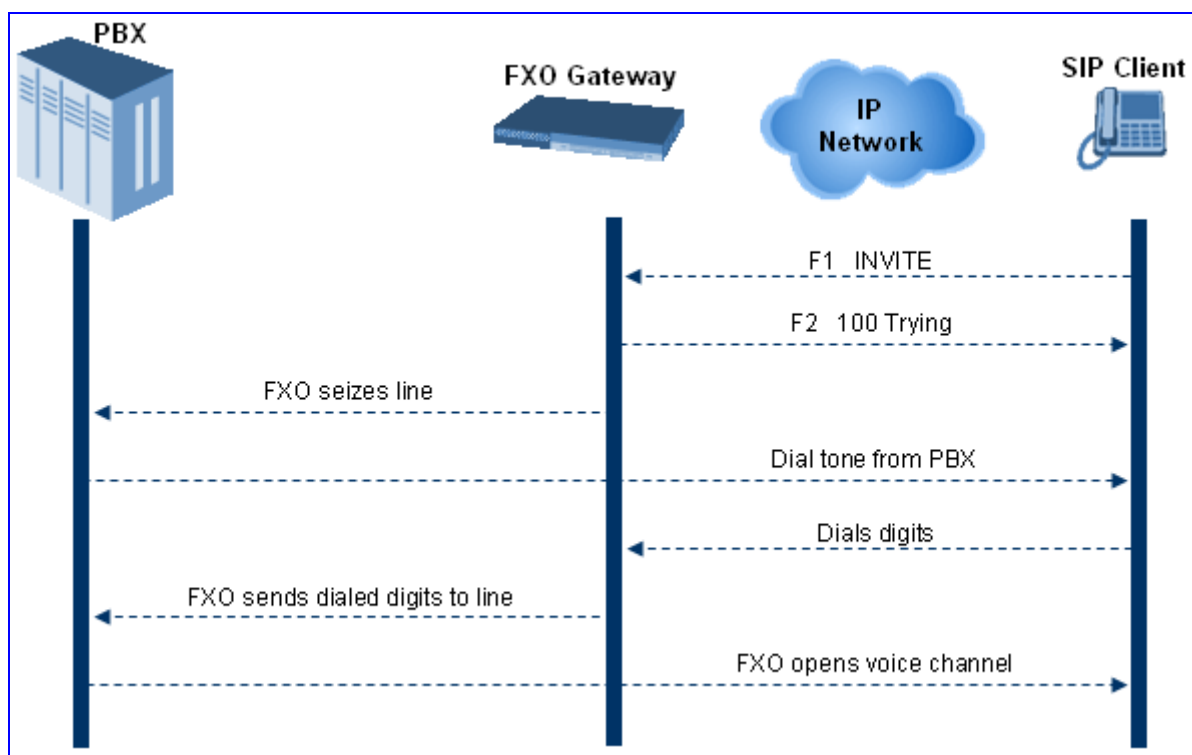
Note: The *ini* file parameter *IsWaitForDialTone* must be disabled for this mode.

- **Answer Supervision:** The Answer Supervision feature enables the FXO device to determine when a call is connected, by using one of the following methods:
 - Polarity Reversal: device sends a 200 OK in response to an INVITE only when it detects a polarity reversal.
 - Voice Detection: device sends a 200 OK in response to an INVITE only when it detects the start of speech (or ringback tone) from the Tel side. (Note that the IPM detectors must be enabled).

8.3.5.2.1.2 Two-Stage Dialing

Two-stage dialing is when the IP caller is required to dial twice. The caller initially dials to the FXO device and only after receiving a dial tone from the PBX (via the FXO device), dials the destination telephone number.

Figure 8-20: Call Flow for Two-Stage Dialing



Two-stage dialing implements the Dialing Time feature. Dialing Time allows you to define the time that each digit can be separately dialed. By default, the overall dialing time per digit is 200 msec. The longer the telephone number, the greater the dialing time.

The relevant parameters for configuring Dialing Time include the following:

- **DTMFDigitLength (100 msec):** time for generating DTMF tones to the PSTN (PBX) side
- **DTMFInterDigitInterval (100 msec):** time between generated DTMF digits to PSTN (PBX) side

8.3.5.2.1.3 DID Wink

The device's FXO ports support Direct Inward Dialing (DID). DID is a service offered by telephone companies that enables callers to dial directly to an extension on a PBX without the assistance of an operator or automated call attendant. This service makes use of DID trunks, which forward only the last three to five digits of a phone number to the PBX. If, for example, a company has a PBX with extensions 555-1000 to 555-1999, and a caller dials 555-1234, the local central office (CO) would forward, for example, only 234 to the PBX. The PBX would then ring extension 234.

DID wink enables the originating end to seize the line by going off-hook. It waits for acknowledgement from the other end before sending digits. This serves as an integrity check that identifies a malfunctioning trunk and allows the network to send a re-order tone to the calling party.

The "start dial" signal is a wink from the PBX to the FXO device. The FXO then sends the last four to five DTMF digits of the called number. The PBX uses these digits to complete the routing directly to an internal station (telephone or equivalent)

- DID Wink can be used for connection to EIA/TIA-464B DID Loop Start lines
- Both FXO (detection) and FXS (generation) are supported

8.3.5.2.2 FXO Operations for Tel-to-IP Calls

The FXO device provides the following FXO operating modes for Tel-to-IP calls:

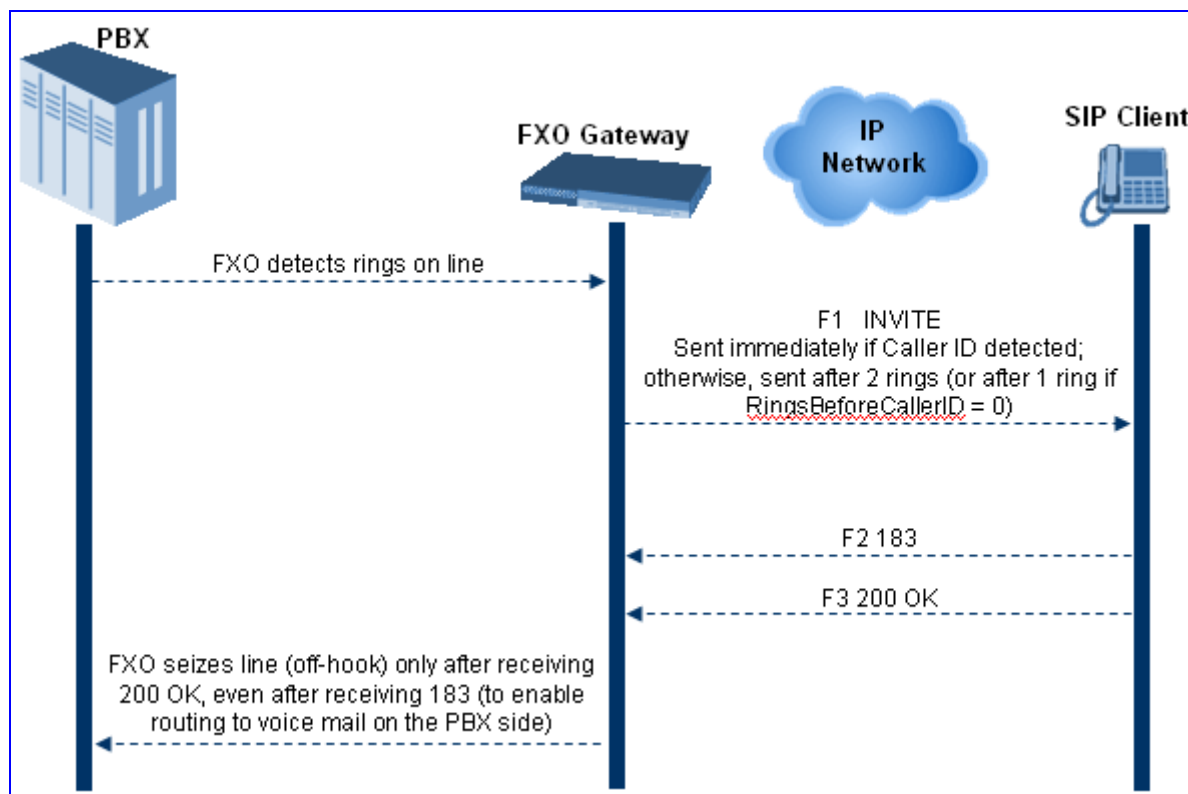
- Automatic Dialing (see "Automatic Dialing" on page [434](#))
- Collecting Digits Mode (see "Collecting Digits Mode" on page [434](#))
- FXO Supplementary Services (see "FXO Supplementary Services" on page [435](#))
 - Hold/Transfer Toward the Tel side
 - Hold/Transfer Toward the IP side
 - Blind Transfer to the Tel side

8.3.5.2.2.1 Automatic Dialing

Automatic dialing is defined using the *ini* file parameter table TargetOfChannel (see Analog Telephony Parameters) or the embedded Web server's 'Automatic Dialing' screen (see "Automatic Dialing" on page 184).

The SIP call flow diagram below illustrates Automatic Dialing.

Figure 8-21: Call Flow for Automatic Dialing

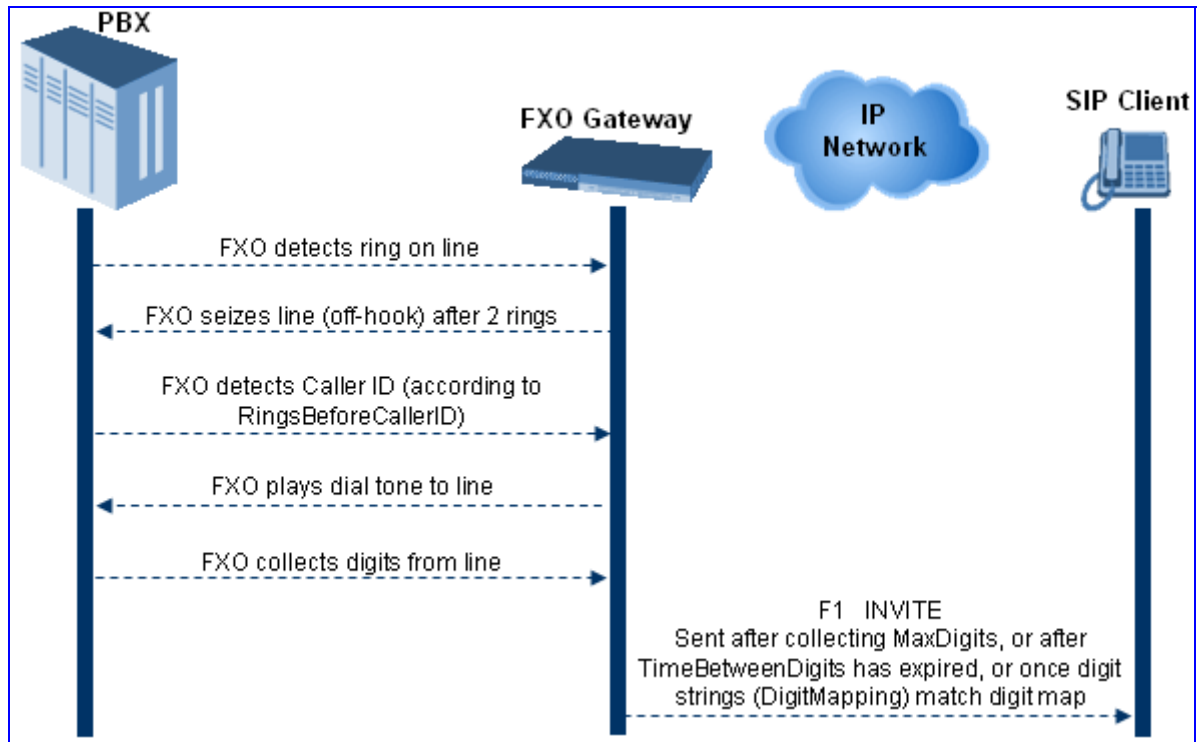


8.3.5.2.2.2 Collecting Digits Mode

When automatic dialing is not defined, the device collects the digits.

The SIP call flow diagram below illustrates the Collecting Digits Mode.

Figure 8-22: Call Flow for Collecting Digits Mode



8.3.5.2.2.3 FXO Supplementary Services

The FXO supplementary services include the following:

- **Hold / Transfer toward the Tel side:** The *ini* file parameter *LineTransferMode* must be set to 0 (default). If the FXO receives a hook-flash from the IP side (using out-of-band or RFC 2833), the device sends the hook-flash to the Tel side by performing one of the following:

- Performing a hook flash (i.e., on-hook and off-hook)
- Sending a hook-flash code (defined by the *ini* file parameter *HookFlashCode*)

The PBX may generate a dial tone that is sent to the IP, and the IP side may dial digits of a new destination.

- **Blind Transfer to the Tel side:** A blind transfer is one in which the transferring phone connects the caller to a destination line before ringback begins. The *ini* file parameter *LineTransferMode* must be set to 1.

The blind transfer call process is as follows:

- FXO receives a REFER request from the IP side
- FXO sends a hook-flash to the PBX, dials the digits (that are received in the Refer-To header), and then drops the line (on-hook). Note that the time between flash to dial is according to the *WaitForDialTime* parameter.
- PBX performs the transfer internally
- **Hold / Transfer toward the IP side:** The FXO device doesn't initiate hold / transfer as a response to input from the Tel side. If the FXO receives a REFER request (with or without replaces), it generates a new INVITE according to the Refer-To header.

8.3.5.2.3 Call Termination on FXO Devices

This section describes the device's call termination capabilities for its FXO interfaces:

- Calls terminated by a PBX (see "Call Termination by PBX" on page 436)
- Calls terminated before call establishment (see "Call Termination before Call Establishment" on page 437)
- Ring detection timeout (see "Ring Detection Timeout" on page 437)

8.3.5.2.3.1 Calls Termination by PBX

The FXO device supports various methods for identifying when a call has been terminated by the PBX.

The PBX doesn't disconnect calls, but instead signals to the device that the call has been disconnected using one of the following methods:

- **Detection of polarity reversal/current disconnect:** The call is immediately disconnected after polarity reversal or current disconnect is detected on the Tel side (assuming the PBX/CO generates this signal). This is the recommended method.

Relevant parameters: EnableReversalPolarity, EnableCurrentDisconnect, CurrentDisconnectDuration, CurrentDisconnectDefaultThreshold, and TimeToSampleAnalogLineVoltage.

- **Detection of Reorder, Busy, Dial, and Special Information Tone (SIT) tones:** The call is immediately disconnected after a Reorder, Busy, Dial, or SIT tone is detected on the Tel side (assuming the PBX / CO generates this tone). This method requires the correct tone frequencies and cadence to be defined in the Call Progress Tones file. If these frequencies are not known, define them in the CPT file (the tone produced by the PBX / CO must be recorded and its frequencies analyzed -- refer to Adding a Reorder Tone to the CPT File in the Reference Manual). This method is slightly less reliable than the previous one. You can use the CPTWizard (described in the *Reference Manual*) to analyze Call Progress Tones generated by any PBX or telephone network.

Relevant parameters: DisconnectOnBusyTone and DisconnectOnDialTone.

- **Detection of silence:** The call is disconnected after silence is detected on both call directions for a specific (configurable) amount of time. The call isn't disconnected immediately; therefore, this method should only be used as a backup option.

Relevant parameters: EnableSilenceDisconnect and FarEndDisconnectSilencePeriod.

- **Special DTMF code:** A digit pattern that when received from the Tel side, indicates to the device to disconnect the call.

Relevant *ini* file parameter: TelDisconnectCode.

- **Interruption of RTP stream:** Relevant parameters: BrokenConnectionEventTimeout and DisconnectOnBrokenConnection.



Note: This method operates correctly only if silence suppression is not used.

- **Protocol-based termination of the call from the IP side**



Note: The implemented disconnect method must be supported by the CO or PBX.

8.3.5.2.3.2 Call Termination before Call Establishment

The device supports the following call termination methods before a call is established:

- **Call termination upon receipt of SIP error response (in Automatic Dialing mode):**
By default, when the FXO device operates in Automatic Dialing mode, there is no method to inform the PBX if a Tel-to-IP call has failed (SIP error response - 4xx, 5xx or 6xx - is received). The reason is that the FXO device does not seize the line until a SIP 200 OK response is received. Use the `FXOAutoDialPlayBusyTone` parameter to allow the device to play a Busy/Reorder tone to the PSTN line if a SIP error response is received. The FXO device seizes the line (off-hook) for the duration defined by the `TimeForReorderTone` parameter. After playing the tone, the line is released (on-hook).
- **Call termination after caller (PBX) on-hooks phone (Ring Detection Timeout feature):** This method operates in one of the following manners:
 - **Automatic Dialing is enabled:** if the remote IP party doesn't answer the call and the ringing signal (from the PBX) stops for a user-defined time (configured by the parameter `FXOBetweenRingTime`), the FXO device releases the IP call.
 - **No automatic dialing and Caller ID is enabled:** the device seizes the line after detection of the second ring signal (allowing detection of caller ID sent between the first and the second rings). If the second ring signal is not received within this timeout, the device doesn't initiate a call to IP.

8.3.5.2.3.3 Ring Detection Timeout

The operation of Ring Detection Timeout depends on the following:

- **Automatic dialing is disabled and Caller ID is enabled:** if the second ring signal is not received for a user-defined time (using the parameter `FXOBetweenRingTime`), the FXO device doesn't initiate a call to the IP.
- **Automatic dialing is enabled:** if the remote party doesn't answer the call and the ringing signal stops for a user-defined time (using the parameter `FXOBetweenRingTime`), the FXO device releases the IP call.

Ring Detection Timeout supports full ring cycle of ring on and ring off (from ring start to ring start).

8.3.5.3 Remote PBX Extension Between FXO and FXS Devices

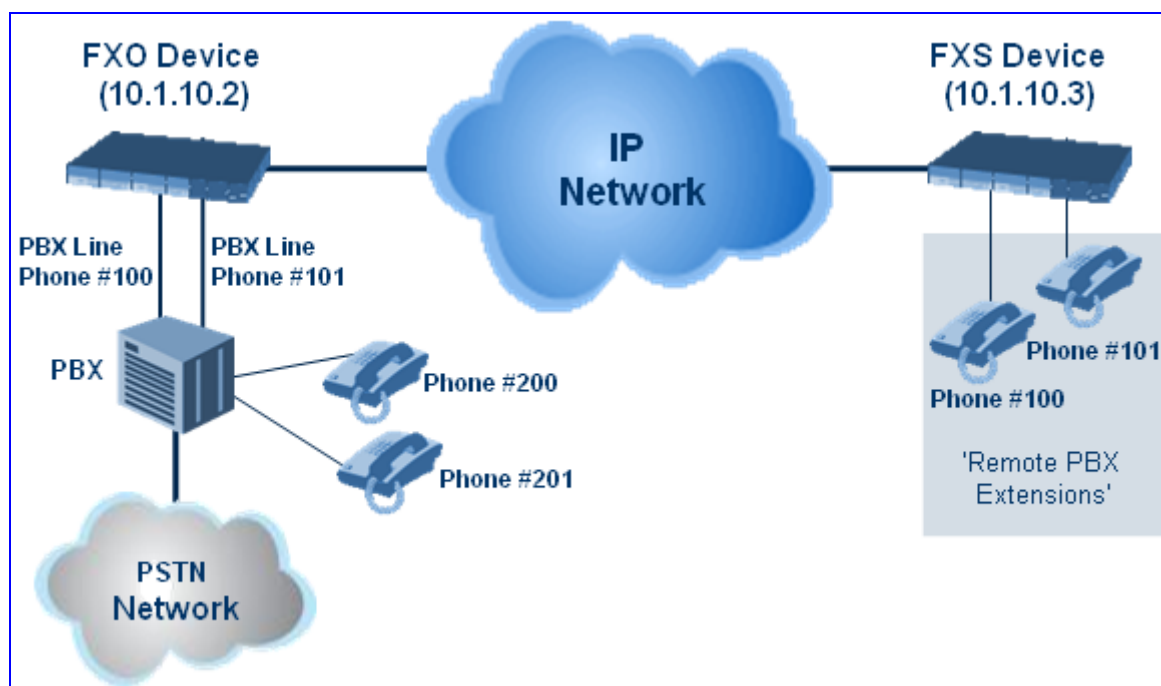
Remote PBX extension offers a company the capability of extending the "power" of its local PBX by allowing remote phones (remote offices) to connect to the company's PBX over the IP network (instead of via PSTN). This is as if the remote office is located in the head office (where the PBX is installed). PBX extensions are connected through FXO ports to the IP network, instead of being connected to individual telephone stations. At the remote office, FXS units connect analog phones to the same IP network. To produce full transparency, each FXO port is mapped to an FXS port (i.e., one-to-one mapping). This allows individual extensions to be extended to remote locations. To call a remote office worker, a PBX user or a PSTN caller simply dials the PBX extension that is mapped to the remote FXS port.

This section provides an example on how to implement a remote telephone extension through the IP network, using 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

Figure 8-23: FXO-FXS Remote PBX Extension (Example)



8.3.5.3.1 Dialing from Remote Extension (Phone at FXS)

The procedure below describes how to dial from the 'remote PBX extension' (i.e., phone connected to the FXS interface).

➤ **To make a call from the FXS interface:**

1. Off-hook the phone and wait for the dial tone from the PBX. This is as if the phone is connected directly to the PBX. The FXS and FXO interfaces establish a voice path connection from the phone to the PBX immediately after the phone is off-hooked.
2. Dial the destination number (e.g., phone number 201). The DTMF digits are sent over IP directly to the PBX. All the audible tones are generated from the PBX (such as ringback, busy, or fast busy tones). One-to-one mapping occurs between the FXS ports and PBX lines.
3. The call disconnects when the phone connected to the FXS goes on-hook.

8.3.5.3.2 Dialing from PBX Line or PSTN

The procedure below describes how to dial from a PBX line (i.e., from a telephone directly connected to the PBX) or from the PSTN to the 'remote PBX extension' (i.e., telephone connected to the FXS interface).

➤ **To dial from a telephone directly connected to the PBX or from the PSTN:**

- Dial the PBX subscriber number (e.g., phone number 101) in the same way as if the user's phone was connected directly to the PBX. As soon as the PBX rings the FXO device, the ring signal is 'sent' to the phone connected to the FXS device. Once the phone connected to the FXS device is off-hooked, the FXO device seizes the PBX line and the voice path is established between the phone and PBX.

There is one-to-one mapping between PBX lines and FXS device ports. Each PBX line is routed to the same phone (connected to the FXS device). The call disconnects when the phone connected to the FXS device is on-hooked.

8.3.5.3.3 Message Waiting Indication for Remote Extensions

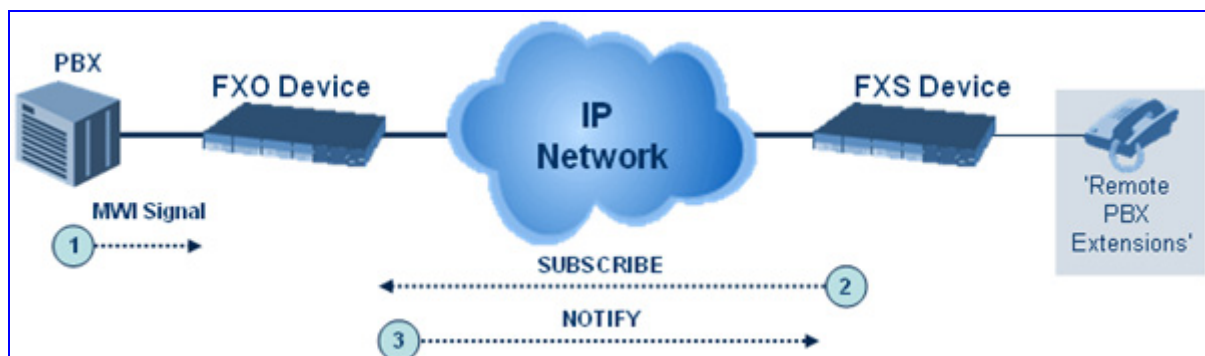
The device supports the relaying of Message Waiting Indications (MWI) for remote extensions (and voice mail applications). Instead of subscribing to an MWI server to receive notifications of pending messages, the FXO device receives subscriptions from the remote FXS device and notifies the appropriate extension when messages (and the number of messages) are pending.

The FXO device detects an MWI message from the Tel (PBX) side using any one of the following methods:

- 100 VDC (sent by the PBX to activate the phone's lamp)
- Stutter dial tone from the PBX
- MWI display signal (according to the parameter CallerIDType)

Upon detection of an MWI message, the FXO device sends a SIP NOTIFY message to the IP side. When receiving this NOTIFY message, the remote FXS device generates an MWI signal toward its Tel side.

Figure 8-24: MWI for Remote Extensions



8.3.5.3.4 Call Waiting for Remote Extensions

When the FXO device detects a Call Waiting indication (FSK data of the Caller Id - CallerIDType2) from the PBX, it sends a proprietary INFO message, which includes the caller identification to the FXS device. Once the FXS device receives this INFO message, it plays a call waiting tone and sends the caller ID to the relevant port for display. The remote extension connected to the FXS device can toggle between calls using the Hook Flash button.

Figure 8-25: Call Waiting for Remote Extensions



8.3.5.3.5 FXS Gateway Configuration

The procedure below describes how to configure the FXS interface (at the 'remote PBX extension').

➤ **To configure the FXS interface:**

1. In the 'Hunt Group Table' page (see , assign the phone numbers 100 to 104 to the device's endpoints.

Figure 8-26: 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 184), enter the phone numbers of the FXO device in the 'Destination Phone Number' fields. When a phone connected to Port #1 off-hooks, the FXS device automatically dials the number '200'.

Figure 8-27: 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 165), enter 20 for the destination phone prefix, and 10.1.10.2 for the IP address of the FXO device.

Figure 8-28: FXS Tel-to-IP Routing Configuration

	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address
1				20	*		10.1.10.2



Note: For the transfer to function in remote PBX extensions, Hold must be disabled at the FXS device (i.e., Enable Hold = 0) and hook-flash must be transferred from the FXS to the FXO (HookFlashOption = 4).

8.3.5.3.6 FXO Gateway Configuration

The procedure below describes how to configure the FXO interface (to which the PBX is directly connected).

➤ **To configure the FXO interface:**

1. In the 'Hunt Group Table' page (see , assign the phone numbers 200 to 204 to the device's FXO endpoints.

Figure 8-29: 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 8-30: 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 8-31: 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 182), set the parameter 'Dialing Mode' to 'Two Stages' (IsTwoStageDial = 1).

8.3.6 Configuring Alternative Routing (Based on Connectivity and QoS)

The Alternative Routing feature enables reliable routing of Tel-to-IP calls when a Proxy isn't used. The device periodically checks the availability of connectivity and suitable Quality of Service (QoS) before routing. If the expected quality cannot be achieved, an alternative IP route for the prefix (phone number) is selected.

The following parameters are used to configure the Alternative Routing mechanism:

- AltRoutingTel2IPEnable
- AltRoutingTel2IPMode
- IPConnQoSMaxAllowedPL
- IPConnQoSMaxAllowedDelay

8.3.6.1 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 165). 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.

8.3.6.2 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:

- **QoS:** The QoS of an IP connection is determined according to RTCP statistics of previous calls. Network delay (in msec) and network packet loss (in percentage) are separately quantified and compared to a certain (configurable) threshold. If the calculated amounts (of delay or packet loss) exceed these thresholds, the IP connection is disallowed.
- **DNS resolution:** When host name is used (instead of IP address) for the destination route, it is resolved to an IP address by a DNS server. Connectivity and QoS are then applied to the resolved IP address.

8.3.6.3 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 Hunt Group using the Routing parameters (see "Configuring iptotelrouteMP500>" on page 172).

8.3.7 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 443)
- Fax and modem transport modes (see "Fax/Modem Transport Modes" on page 443)
- V.34 fax support (see V.34 Fax Support on page 449)
- V.152 support (see "V.152 Support" on page 452)

8.3.7.1 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 452): fax/modem capabilities are negotiated between the device and the remote endpoint at the establishment of the call. During a call, when a fax/modem signal is detected, transition from voice to VBD (or T.38) is automatically performed and no additional SIP signaling is required. If negotiation fails (i.e., no match is achieved for any of the transport capabilities), fallback to existing logic occurs (according to the parameter `IsFaxUsed`).

8.3.7.2 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 444)
- G.711 Transport: switching to G.711 when fax/modem is detected (see "G.711 Fax / Modem Transport Mode" on page 445)
- Fax fallback to G.711 if T.38 is not supported (see "Fax Fallback" on page 445)
- Fax and modem bypass: a proprietary method that uses a high bit rate coder (see "Fax/Modem Bypass Mode" on page 446)
- NSE Cisco's Pass-through bypass mode for fax and modem (see "Fax / Modem NSE Mode" on page 447)
- Transparent with events: passing the fax / modem signal in the current voice coder with adaptations (see "Fax / Modem Transparent with Events Mode" on page 448)
- Transparent: passing the fax / modem signal in the current voice coder (see "Fax / Modem Transparent Mode" on page 448)
- RFC 2833 ANS Report upon Fax/Modem Detection (see "RFC 2833 ANS Report upon Fax/Modem Detection" on page 449)

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

8.3.7.2.1 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 444)
- 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 444)

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

You can change the fax rate declared in the SDP, using the parameter FaxRelayMaxRate (this parameter doesn't affect the actual transmission rate). In addition, you can enable or disable Error Correction Mode (ECM) fax mode using the FaxRelayECMEnable parameter.

When using T.38 mode, you can define a redundancy feature to improve fax transmission over congested IP networks. This feature is activated using the FaxRelayRedundancyDepth and FaxRelayEnhancedRedundancyDepth parameters. Although this is a proprietary redundancy scheme, it should not create problems when working with other T.38 decoders.

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

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

To configure T.38 mode using SIP Re-INVITE messages, set IsFaxUsed to 1. Additional configuration parameters include the following:

- FaxRelayEnhancedRedundancyDepth
- FaxRelayRedundancyDepth
- FaxRelayECMEnable
- FaxRelayMaxRate



Note: The terminating gateway sends T.38 packets immediately after the T.38 capabilities are negotiated in SIP. However, the originating device by default, sends T.38 (assuming the T.38 capabilities are negotiated in SIP) only after it receives T.38 packets from the remote device. This default behavior cannot be used when the originating device is located behind a firewall that blocks incoming T.38 packets on ports that have not yet received T.38 packets from the internal network. To resolve this problem, the device should be configured to send CNG packets in T.38 upon CNG signal detection (CNGDetectorMode = 1).

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

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

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

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

8.3.7.2.2 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.

8.3.7.2.3 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=gpmde:0 vbd=yes;ecan=on
- **For G.711 μ -law:** a=gpmde:8 vbd=yes;ecan=on

In this mode, the parameter FaxTransportMode is ignored and automatically set to 'transparent'.

To configure fax fallback mode, set IsFaxUsed to 3.

8.3.7.2.4 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
 - FaxModemBypassDJBufMinDelay



Note: When the device is configured for modem bypass and T.38 fax, V.21 low-speed modems are not supported and fail as a result.



Tip: When the remote (non-AudioCodes') gateway uses G711 coder for voice and doesn't change the coder payload type for fax or modem transmission, it is recommended to use the Bypass mode with the following configuration:

- EnableFaxModemInbandNetworkDetection = 1
- FaxModemBypassCoderType = same coder used for voice
- FaxModemBypassM = same interval as voice
- ModemBypassPayloadType = 8 if voice coder is A-Law; 0 if voice coder is Mu-Law

8.3.7.2.5 Fax / Modem NSE Mode

In this mode, fax and modem signals are transferred using Cisco-compatible Pass-through bypass mode. Upon detection of fax or modem answering tone signal, the terminating device sends three to six special NSE RTP packets (using NSEpayloadType, usually 100). These packets signal the remote device to switch to G.711 coder (according to the parameter FaxModemBypassCoderType). After a few NSE packets are exchanged between the devices, both devices start using G.711 packets with standard payload type (8 for G.711 A-Law and 0 for G.711 Mu-Law). In this mode, no Re-INVITE messages are sent. The voice channel is optimized for fax/modem transmission (same as for usual bypass mode).

The parameters defining payload type for the proprietary AudioCodes' Bypass mode FaxBypassPayloadType and ModemBypassPayloadType are not used with NSE Bypass.

When configured for NSE mode, the device includes in its SDP the following line:

```
a=rtpmap:100 X-NSE/8000
```

(where 100 is the NSE payload type)

The Cisco gateway must include the following definition: "modem passthrough nse payload-type 100 codec g711alaw".

To configure NSE mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 2
- NSEMode = 1
- NSEPayloadType = 100
- V21ModemTransportType = 2
- V22ModemTransportType = 2
- V23ModemTransportType = 2
- V32ModemTransportType = 2

- V34ModemTransportType = 2
- BellModemTransportType = 2

8.3.7.2.6 Fax / Modem Transparent with Events Mode

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

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

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

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

8.3.7.2.7 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 138) 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 446) or Transparent with Events (see "Fax / Modem Transparent with Events Mode" on page 448) for modem.

8.3.7.2.8 RFC 2833 ANS Report upon Fax/Modem Detection

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

Relevant parameters:

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

8.3.7.3 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 449)
- T38 Version 0 relay mode, i.e., fallback to T.38 (see "Relay Mode for T.30 and V.34 Faxes" on page 450)

Using the *ini* file parameter V34FaxTransportType, you can configure whether to pass V.34 over T38 fax relay, or use Bypass over the High Bit Rate coder (e.g. PCM A-Law).



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

8.3.7.3.1 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)
- V34FaxTransportType = 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)
- V34FaxTransportType = 2 (Bypass)
- V34ModemTransportType = 2 (Modem bypass)
- V32ModemTransportType = 2
- V23ModemTransportType = 2
- V22ModemTransportType = 2

8.3.7.3.2 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)
- V34FaxTransportType = 1 (Relay)
- V34ModemTransportType = 0 (Transparent)
- V32ModemTransportType = 0
- V23ModemTransportType = 0
- V22ModemTransportType = 0

8.3.7.3.3 V.34 Fax Relay for SG3 Fax Machines

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

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

1. Define an IP Profile with the Fax Signaling Method (IsFaxUsed ini file) parameter set to T.38 Relay (1).
2. Select the codec used by the device to G.729 (or any other supported codec). This is done in the Coders Table page (see "Configuring Coders" on page 139).
3. On the Fax/Modem/CID Settings page (see "Configuring Fax/Modem/CID Settings" on page 105), configure the following:
 - Set the T38 Version (SIPT38Version ini file) parameter to T.38 version 3.
 - Set the Fax Relay Max Rate Fax (RelayMaxRate ini file) parameter to 33,600bps (default).

- Set the CNG Detector Mode (CNGDetectorMode ini file) parameter to Disable (default).
- Set the following parameters to Disable:
 - ◆ V.21 Modem Transport Type (V21ModemTransportType ini file)
 - ◆ V.22 Modem Transport Type (V22ModemTransportType ini file)
 - ◆ V.23 Modem Transport Type (V23ModemTransportType ini file)
 - ◆ V.32 Modem Transport Type (V32ModemTransportType ini file)
 - ◆ V.34 Modem Transport Type (V34ModemTransportType ini file)
- 4. Set the V34FaxTransportType ini file parameter to 1 (i.e., Relay).
- 5. Set the T.38 Max Datagram Size (T38MaxDatagramSize ini file) parameter to 560 (default).
- 6. Set the CEDTransferMode parameter to 0 (default).

**Notes:**

- The T.38 negotiation should be completed at call start according to V.152 procedure (as shown in the INVITE example below).
- Currently, T.38 mid call Re-INVITEs are not supported.

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

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

v=0
o=AudiocodesGW 1938931006 1938930708 IN IP4 10.8.6.55
s=Phone-Call
c=IN IP4 10.8.6.55
t=0 0
m=audio 6010 RTP/AVP 18 97
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:97 telephone-event/8000
a=fmtp:97 0-15
a=ptime:20
```



```
a=sendrecv
m=image 6012 udpt1 t38
a=T38FaxVersion:3
a=T38MaxBitRate:33600
a=T38FaxMaxBuffer:1024
a=T38FaxMaxDatagram:122
a=T38FaxRateManagement:transferredTCF
a=T38FaxUdpEC:t38UDPRedundancy
```

8.3.7.4 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 139).

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

Below is an example of media descriptions of an SDP indicating support for V.152.

```
v=0
o=- 0 0 IN IPV4 <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
```

In the example above, V.152 implementation is supported (using the dynamic payload type 96 and G.711 u-law as the VBD codec) as well as the voice codecs G.711 μ -law and G.729.

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

To configure T.38 mode, use the `CodersGroup` parameter.

8.3.8 Working with Supplementary Services

The device supports the following supplementary services:

- Call Hold and Retrieve (see "Call Hold and Retrieve" on page 453)
- BRI suspend-resume (see BRI Suspend and Resume on page 455)
- Consultation (see Consultation Feature on page 455)
- Call Transfer (see "Call Transfer" on page 456)
- Call Forward (see "Call Forward" on page 457)
- Call Waiting (see Call Waiting on page 460)
- Message Waiting Indication (see "Message Waiting Indication" on page 461)
- Caller ID (see Caller ID on page 463)
- Three-way conferencing (see Three-Way Conferencing on page 465)
- Multilevel Precedence and Preemption (see "Multilevel Precedence and Preemption" on page 467)

To activate these supplementary services, enable each service's corresponding parameter using the Web interface or ini file.



Notes:

- All call participants must support the specific supplementary service that is used.
- When working with certain application servers (such as BroadSoft's BroadWorks) in client server mode (the application server controls all supplementary services and keypad features by itself), the device's supplementary services must be disabled.

8.3.8.1 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.

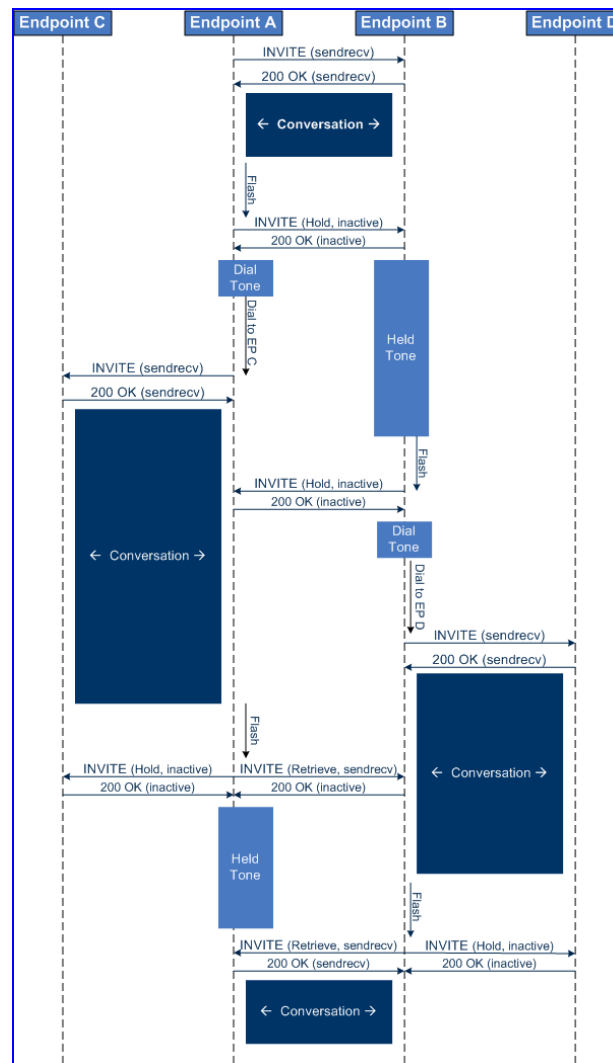
Receiving Hold/Retrieve:

- 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 8-32: Double Hold SIP Call Flow



The flowchart above describes the following "double" call-hold scenario:

1. A calls B and establishes a voice path.
2. A places B on hold; A hears a Dial tone and B hears a Held tone.
3. A calls C and establishes a voice path.
4. B places A on hold; B hears a Dial tone.
5. B calls D and establishes a voice path.
6. A ends call with C; A hears a Held tone.
7. B ends call with D.
8. B retrieves call with A.



Notes:

- If a party that is placed on hold (e.g., B in the above example) is called by another party (e.g., D), then the on-hold party receives a Call Waiting tone instead of the Held tone.
- While in a Double Hold state, placing the phone on-hook disconnects both calls (i.e. call transfer is not performed).

8.3.8.2 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.

8.3.8.3 Consultation Feature

The device's Consultation feature allows you to place one number on hold and consult privately with another party.

- The Consultation feature is relevant only for the holding party.
- After holding a call (by pressing hook-flash), the holding party hears a dial tone and can then initiate a new call, which is called a Consultation call.
- While hearing a dial tone, or when dialing to the new destination (before dialing is

complete), the user can retrieve the held call by pressing hook-flash.

- The held call can't be retrieved while Ringback tone is heard.
- After the Consultation call is connected, the user can toggle between the held and active call by pressing the hook-flash key.



Note: The Consultation feature is applicable only to FXS interfaces.

8.3.8.4 Call Transfer

The device supports the following call transfer types:

- Consultation Transfer (see "Consultation Call Transfer" on page 456)
- Blind Transfer (see "Blind Call Transfer" on page 457)



Notes:

- Call transfer is initiated by sending REFER with REPLACES.
- The device can receive and act upon receiving REFER with or without REPLACES.
- The device can receive and act upon receiving INVITE with REPLACES, in which case the old call is replaced by the new one.
- The INVITE with REPLACES can be used to implement Directed Call Pickup.

8.3.8.4.1 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.

8.3.8.4.2 Blind Call Transfer

Blind call transfer is done (using SIP REFER messages) after a call is established between call parties A and B, and party A decides to immediately transfer the call to C without speaking to C. The result of the transfer is a call between B and C (similar to consultation transfer, but skipping the consultation stage).



Note: Currently, the device does not support blind transfer for BRI interfaces.

8.3.8.5 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 186) or *ini* file to activate one of the call forward modes. These modes are configurable per endpoint.



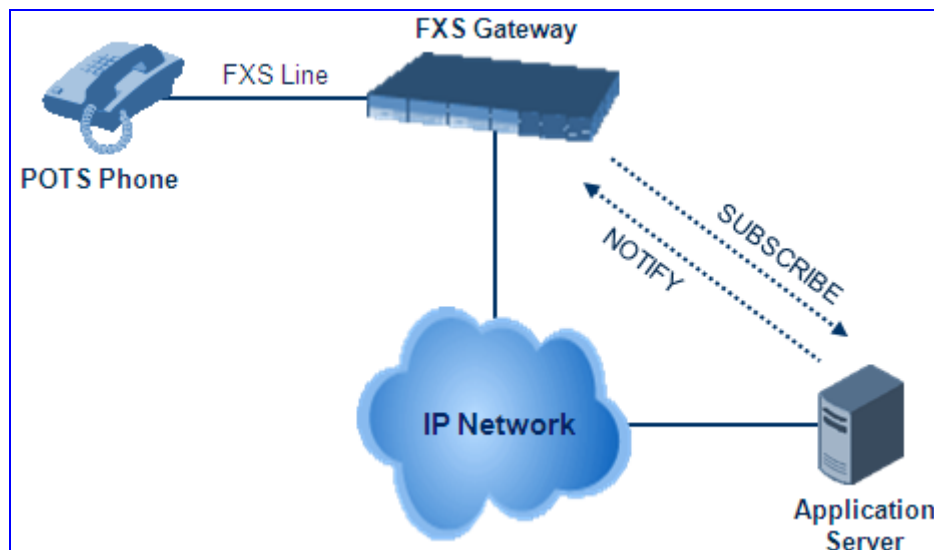
Notes:

- When call forward is initiated, the device sends a SIP 302 response with a contact that contains the phone number from the forward table and its corresponding IP address from the routing table (or when a proxy is used, the proxy's IP address).
- For receiving call forward, the device handles SIP 3xx responses for redirecting calls with a new contact.

8.3.8.5.1 Call Forward Reminder Ring

The device supports the Call Forward Reminder Ring feature for FXS interfaces, whereby the device's FXS endpoint emits a short ring burst (only if in **onhook** state) when a third-party Application Server (e.g., softswitch) forwards an incoming call to another destination. This is important in that it notifies (audibly) the FXS endpoint user that a call forwarding service is currently being performed.

Figure 8-33: Call Forward Reminder with Application Server



The device generates a Call Forward Reminder ring burst to the FXS endpoint each time it receives a SIP NOTIFY message with a "reminder ring" xml body. The NOTIFY request is sent from the Application Server to the device each time the Application Server forwards an incoming call. The service is cancelled when an UNSUBSCRIBE request is sent from the device, or when the Subscription time expires.

The Reminder Ring tone can be defined by using the parameter `CallForwardRingToneID`, which points to a ring tone defined in the Call Progress Tone file.

The following parameters are used to configure this feature:

- EnableNRTSubscription
- ASSubscribeIPGroupID
- NRTRetrySubscriptionTime
- CallForwardRingToneID

8.3.8.5.2 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

8.3.8.5.3 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=z9hG4bKWDSUKUHWFEQSVUUVJGM
From: <sip:400@10.33.2.5;user=phone>;tag=DUOROSXSQYJJLNBFRQTG
To: <sip:*72100@10.33.8.53;user=phone>
Call-ID: GMNOVQRRXUUCYCQSFQHS@10.33.2.5
CSeq: 1 INVITE
Contact: <sip:400@10.33.2.5:5060>
Supported: em,100rel,timer,replaces
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE
User-Agent: Sip Message Generator V1.0.0.5
User-to-User: 31323334;pd=4
Content-Type: application/sdp
Content-Length: 155
```

8.3.8.6 Call Waiting

The Call Waiting feature enables FXS devices to accept an additional (second) call on busy endpoints. If an incoming IP call is designated to a busy port, the called party hears a call waiting tone (several configurable short beeps) and (for Bellcore and ETSI Caller IDs) can view the Caller ID string of the incoming call. The calling party hears a Call Waiting Ringback Tone. The called party can accept the new call using hook-flash, and can toggle between the two calls.

➤ To enable call waiting:

1. Set the parameter EnableCallWaiting to 1.
2. Set the parameter EnableHold to 1.

3. Define the Call Waiting indication and Call Waiting Ringback tones in the Call Progress Tones file. You can define up to four Call Waiting indication tones (refer to the parameter FirstCallWaitingToneID in SIP Configuration Parameters).
4. To configure the Call Waiting indication tone cadence, modify the following parameters: NumberOfWaitingIndications, WaitingBeepDuration and TimeBetweenWaitingIndications.
5. To configure a delay interval before a Call Waiting Indication is played to the currently busy port, use the parameter TimeBeforeWaitingIndication. This enables the caller to hang up before disturbing the called party with Call Waiting Indications. Applicable only to FXS modules.

Both the calling and called sides are supported by FXS interfaces; FXO interfaces support only the calling side.

To indicate Call Waiting, the device sends a 182 Call Queued response. The device identifies Call Waiting when a 182 Call Queued response is received.



Note: The Call Waiting feature is applicable only to FXS/FXO interfaces.

8.3.8.7 Message Waiting Indication

The device supports Message Waiting Indication (MWI) according to IETF Internet-Draft draft-ietf-sipping-mwi-04, including SUBSCRIBE (to MWI server).



Note: For a detailed description on IP voice mail configuration, refer to the *IP Voice Mail CPE Configuration Guide*.

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
- 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. 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.

8.3.8.8 Caller ID

This section discusses the device's Caller ID support.



Note: The Caller ID feature is applicable only to FXS/FXO interfaces.

8.3.8.8.1 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`.

8.3.8.8.2 Debugging a Caller ID Detection on FXO

The procedure below describes debugging caller ID detection in FXO interfaces.

➤ **To debug a Caller ID detection on an FXO interface:**

1. Verify that the parameter EnableCallerID is set to 1.
2. Verify that the caller ID standard (and substandard) of the device matches the standard of the PBX (using the parameters CallerIDType, BellcoreCallerIDTypeOneSubStandard, and ETSICallerIDTypeOneSubStandard).
3. Define the number of rings before the device starts the detection of caller ID (using the parameter RingsBeforeCallerID).
4. Verify that the correct FXO coefficient type is selected (using the parameter CountryCoefficients), as the device is unable to recognize caller ID signals that are distorted.
5. Connect a phone to the analog line of the PBX (instead of to the device's FXO interface) and verify that it displays the caller ID.

If the above does not solve the problem, you need to record the caller ID signal (and send it to AudioCodes), as described below.

➤ **To record the caller ID signal using the debug recording mechanism:**

1. Access the FAE page (by appending "FAE" to the device's IP address in the Web browser's URL, for example, http://10.13.4.13/FAE).
2. Press the **Cmd Shell** link.
3. Enter the following commands:


```
dr
ait <IP address of PC to collect the debug traces sent from
the device>
AddChannelIdTrace ALL-WITH-PCM <port number, which starts from
0>
Start
```
4. Make a call to the FXO.
5. To stop the DR recording, at the CLI prompt, type **STOP**.

8.3.8.8.3 Caller ID on the IP Side

Caller ID is provided by the SIP From header containing the caller's name and "number", for example:

```
From: "David" <SIP:101@10.33.2.2>;tag=35dfsgasd45dg
```

If Caller ID is restricted (received from Tel or configured in the device), the From header is set to:

```
From: "anonymous" <anonymous@anonymous.invalid>; tag=35dfsgasd45dg
```

The P-Asserted (or P-Preferred) headers are used to present the originating party's caller ID even when the caller ID is restricted. These headers are used together with the Privacy header.

- If Caller ID is restricted:
 - The From header is set to "anonymous" <anonymous@anonymous.invalid>
 - The 'Privacy: id' header is included
 - The P-Asserted-Identity (or P-Preferred-Identity) header shows the caller ID
- If Caller ID is allowed:
 - The From header shows the caller ID
 - The 'Privacy: none' header is included
 - The P-Asserted-Identity (or P-Preferred-Identity) header shows the caller ID

In addition, the caller ID (and presentation) can be displayed in the Calling Remote-Party-ID header.

The 'Caller Display Information' table (CallerDisplayInfo) is used for the following:

- **FXS interfaces** - to define the caller ID (per port) that is sent to IP.
- **FXO interfaces** - to define the caller ID (per port) that is sent to IP if caller ID isn't detected on the Tel side, or when EnableCallerID = 0.
- **FXS and FXO interfaces** - to determine the presentation of the caller ID (allowed or restricted).
- **To maintain backward compatibility** - when the strings 'Private' or 'Anonymous' are set in the Caller ID/Name field, the caller ID is restricted and the value in the Presentation field is ignored.

The value of the 'Presentation' field that is defined in the 'Caller Display Information' table can be overridden by configuring the 'Presentation' parameter in the 'Tel to IP Source Number Manipulation' table. Therefore, this table can be used to set the presentation for specific calls according to Source / Destination prefixes.

The caller ID can be restricted/allowed (per port) using keypad features KeyCLIR and KeyCLIRDeact (FXS only).

AssertedIdMode defines the header that is used (in the generated INVITE request) to deliver the caller ID (P-Asserted-Identity or P-preferred-Identity). Use the parameter UseTelURIForAssertedID to determine the format of the URI in these headers (sip: or tel:).

The parameter EnableRPIheader enables Remote-Party-ID (RPI) headers for calling and called numbers for Tel-to-IP calls.

8.3.8.9 Three-Way Conferencing

The device supports three-way conference calls. These conference calls can also occur simultaneously.

The following example demonstrates three-way conferencing. This example assumes that a telephone "A" connected to the device wants to establish a three-way conference call with two remote IP phones "B" and "C":

1. User A has an ongoing call with IP phone B.
2. User A places IP phone B on hold (by pressing the telephone's flash hook button, defined by the parameter HookFlashCode).

3. User A hears a dial tone, and then makes a call to IP phone C.
4. IP phone C answers the call.
5. User A can now establish a three-way conference call (between A, B and C) by pressing the flash-hook button, defined by the parameter ConferenceCode (e.g., regular flash-hook button or "*1").


Notes:

- Instead of using the flash-hook button to establish a three-way conference call, you can dial a user-defined hook-flash code (e.g., "*1"), configured by the HookFlashCode parameter.
- Three-way conferencing is applicable only to FXS interfaces.
- The device supports high definition, three-way conferencing using wideband codecs (e.g., G.722 and AMR-WB). This allows conference participants to experience wideband voice quality. Call conferences can also include narrowband and wideband participants.

The 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. For this mode, the 3WayConferenceMode parameter is set to 2.

To enable three-way conferencing, the following parameters need to be configured:

- Enable3WayConference
- ConferenceCode = '!' (default, which is the hook flash button)
- HookFlashCode
- 3WayConferenceMode (conference mode)
- FlashKeysSequenceStyle = 1 or 2 (makes a three-way call conference using the Flash button + 3)

8.3.8.10 Multilevel Precedence and Preemption

The device's Multilevel Precedence and Preemption (MLPP) service can be enabled using the CallPriorityMode parameter. MLPP is a call priority scheme, which does the following:

- Assigns a precedence level (priority level of call) to specific phone calls or messages.
- Allows higher priority calls (*precedence call*) and messages to preempt lower priority calls and messages (i.e., terminates existing lower priority calls) that are recognized within a user-defined domain (*MLPP domain ID*). The domain specifies the collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber that belongs to a particular domain places a precedence call to another MLPP subscriber that belongs to the same domain, MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher-precedence call. MLPP service availability does not go across different domains

MLPP is typically used in the military where for example, high-ranking personnel can preempt active calls during network stress scenarios, such as a national emergency or degraded network situations.

The Resource Priority value in the Resource-Priority SIP header can be any 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 8-5: MLPP Call Priority Levels (Precedence) and DSCP Configuration Parameters

MLPP Precedence Level	Precedence Level in Resource-Priority SIP Header	DSCP Configuration Parameter
0 (lowest)	routine	MLPPRoutineRTPDSCP
2	priority	MLPPPRIORITYRTPDSCP
4	immediate	MLPPImmediateRTPDSCP
6	flash	MLPPFlashRTPDSCP
8	flash-override	MLPPFlashOverRTPDSCP
9 (highest)	flash-override-override	MLPPFlashOverOverRTPDSCP

- **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

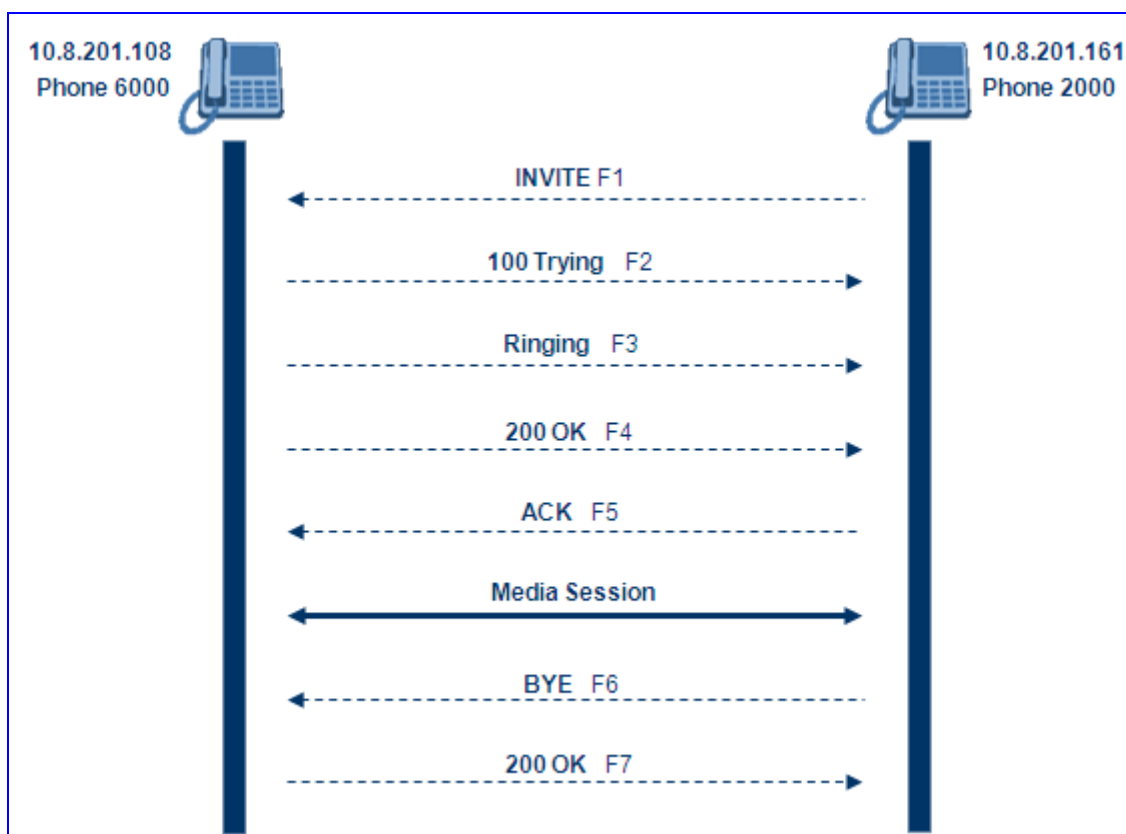
For a complete list of the MLPP parameters, see "MLPP Parameters" on page [777](#).

8.3.9 SIP Call Routing Examples

8.3.9.1 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 8-34: 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 800 MSBG/v.6.00.010.006
Supported: 100rel,em
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,
NOTIFY,PRACK,REFER,INFO
Content-Type: application/sdp
Content-Length: 208

v=0
o=AudiocodesGW 18132 74003 IN IP4 10.8.201.108
s=Phone-Call
c=IN IP4 10.8.201.108
t=0 0
```

```
m=audio 4000 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

■ F2 TRYING (10.8.201.161 >> 10.8.201.108):

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
Server: Audiocodes-Sip-Gateway/Mediant 800 MSBG/v.6.00.010.006
CSeq: 18153 INVITE
Content-Length: 0
```

■ F3 RINGING 180 (10.8.201.161 >> 10.8.201.108):

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
Server: Audiocodes-Sip-Gateway/Mediant 800 MSBG/v.6.00.010.006
CSeq: 18153 INVITE
Supported: 100rel,em
Content-Length: 0
```



Note: Phone '2000' answers the call and then sends a 200 OK message to device 10.8.201.108.

■ F4 200 OK (10.8.201.161 >> 10.8.201.108):

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
CSeq: 18153 INVITE
Contact: <sip:2000@10.8.201.161;user=phone>
Server: Audiocodes-Sip-Gateway/Mediant 800 MSBG/v.6.00.010.006
Supported: 100rel,em
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,
NOTIFY,PRACK,REFER,INFO
Content-Type: application/sdp
Content-Length: 206

v=0
o=AudiocodesGW 30221 87035 IN IP4 10.8.201.161
s=Phone-Call
c=IN IP4 10.8.201.10
t=0 0
m=audio 7210 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=ptime:20
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
```

■ F5 ACK (10.8.201.108 >> 10.8.201.10):

```
ACK sip:2000@10.8.201.161;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacZYpJWxZ
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
User-Agent: Audiocodes-Sip-Gateway/Mediant 800 MSBG/v.6.00.010.006
CSeq: 18153 ACK
Supported: 100rel,em
Content-Length: 0
```



Note: Phone '6000' goes on-hook and device 10.8.201.108 sends a BYE to device 10.8.201.161. A voice path is established.

■ F6 BYE (10.8.201.108 >> 10.8.201.10):

```
BYE sip:2000@10.8.201.161;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacRKCVBud
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
User-Agent: Audiocodes-Sip-Gateway/Mediant 800 MSBG/v.6.00.010.006
CSeq: 18154 BYE
Supported: 100rel,em
Content-Length: 0
```

■ F7 OK 200 (10.8.201.10 >> 10.8.201.108):

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacRKCVBud
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
Server: Audiocodes-Sip-Gateway/Mediant 800 MSBG/v.6.00.010.006
CSeq: 18154 BYE
Supported: 100rel,em
Content-Length: 0
```

8.3.9.2 SIP Authentication Example

The device supports basic and digest (MD5) authentication types, according to SIP RFC 3261 standard. A proxy server might require authentication before forwarding an INVITE message. A Registrar/Proxy server may also require authentication for client registration. A proxy replies to an unauthenticated INVITE with a 407 Proxy Authorization Required response, containing a Proxy-Authenticate header with the form of the challenge. After sending an ACK for the 407, the user agent can then re-send the INVITE with a Proxy-Authorization header containing the credentials.

User agents, Redirect or Registrar servers typically use 401 Unauthorized response to challenge authentication containing a WWW-Authenticate header, and expect the re-INVITE to contain an Authorization header.

The following example describes the Digest Authentication procedure, including computation of user agent credentials:

1. The REGISTER request is sent to a Registrar/Proxy server for registration:

```
REGISTER sip:10.2.2.222 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.200
From: <sip:122@10.1.1.200>;tag=1c17940
To: <sip:122@10.1.1.200>
Call-ID: 634293194@10.1.1.200
User-Agent: Audiocodes-Sip-Gateway/Mediant 800 MSBG/v.6.00.010.006
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
```

2. Upon receipt of this request, the Registrar/Proxy returns a 401 Unauthorized response:

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 10.2.1.200
From: <sip:122@10.2.2.222 >;tag=1c17940
To: <sip:122@10.2.2.222 >
Call-ID: 634293194@10.1.1.200
Cseq: 1 REGISTER
Date: Mon, 30 Jul 2001 15:33:54 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0

WWW-Authenticate: Digest realm="audiocodes.com",
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
stale=FALSE,
algorithm=MD5
```

3. According to the sub-header present in the WWW-Authenticate header, the correct REGISTER request is created.
4. Since the algorithm is MD5:
 - The username is equal to the endpoint phone number 122.
 - The realm return by the proxy is audiocodes.com.
 - The password from the *ini* file is AudioCodes.
 - The equation to be evaluated is (according to RFC this part is called A1) **'122:audiocodes.com:AudioCodes'**.
 - The MD5 algorithm is run on this equation and stored for future usage.
 - The result is 'a8f17d4b41ab8dab6c95d3c14e34a9e1'.
5. Next, the par called A2 needs to be evaluated:
 - The method type is 'REGISTER'.
 - Using SIP protocol 'sip'.
 - Proxy IP from *ini* file is '10.2.2.222'.
 - The equation to be evaluated is **'REGISTER:sip:10.2.2.222'**.
 - The MD5 algorithm is run on this equation and stored for future usage.
 - The result is 'a9a031cfddcb10d91c8e7b4926086f7e'.

6. Final stage:

- The A1 result: The nonce from the proxy response is '11432d6bce58ddf02e3b5e1c77c010d2'.
- The A2 result: The equation to be evaluated is '**A1:11432d6bce58ddf02e3b5e1c77c010d2:A2**'.
- The MD5 algorithm is run on this equation. The outcome of the calculation is the response needed by the device to register with the Proxy.
- The response is 'b9c45d0234a5abf5ddf5c704029b38cf'.

At this time, a new REGISTER request is issued with the following response:

```
REGISTER sip:10.2.2.222 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c23940
To: <sip: 122@10.1.1.200>
Call-ID: 654982194@10.1.1.200
Server: Audiocodes-Sip-Gateway/Mediant 800 MSBG/v.6.00.010.006
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
Authorization: Digest, username: 122,
realm="audiocodes.com",
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
uri="10.2.2.222",
response="b9c45d0234a5abf5ddf5c704029b38cf"
```

7. Upon receiving this request and if accepted by the Proxy, the proxy returns a 200 OK response closing the REGISTER transaction:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c23940
To: <sip: 122@10.1.1.200>
Call-ID: 654982194@10.1.1.200
Cseq: 1 REGISTER
Date: Thu, 26 Jul 2001 09:34:42 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0
Contact: <sip:122@10.1.1.200>; expires="Thu, 26 Jul 2001 10:34:42 GMT"; action=proxy; q=1.00
Contact: <122@10.1.1.200:>; expires="Tue, 19 Jan 2038 03:14:07 GMT"; action=proxy; q=0.00
Expires: Thu, 26 Jul 2001 10:34:42 GMT
```

8.3.9.3 Establishing a Call between Two Devices

This section provides an example on configuring two AudioCodes' devices with FXS interfaces for establishing call communication. After configuration, you can make calls between telephones connected to the same device and between the two devices.

This example assumes the following:

- The IP address of the first device is 10.2.37.10 and its endpoint numbers are 101 to 104.
- The IP address of the second device is 10.2.37.20 and its endpoint numbers are 201 to 204.
- A SIP Proxy is not used. Internal call routing is performed using the device's 'Outbound IP Routing Table'.

➤ To configure the two devices for call communication:

1. For the *first* device (10.2.37.10), in the 'Hunt Group Table' page, assign the phone numbers 101 to 104 to the device's endpoints.

Figure 8-35: Assigning Phone Numbers to Device 10.2.37.10

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 'Hunt Group Table' page, assign the phone numbers 201 to 204 to the device's endpoints.

Figure 8-36: Assigning Phone Numbers to Device 10.2.37.20

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 settings for *both* devices:

In the 'Outbound IP Routing Table' page (see "Configuring Outbound IP Routing Table" on page 165), add the following routing rules:

- a. In the first row, enter 10 for the destination phone prefix and enter 10.2.37.10 for the destination IP address (i.e., IP address of the first device).
- b. In the second row, enter 20 for the destination phone prefix and 10.2.37.20 for the destination IP address (i.e., IP address of the second device).

These settings enable the routing (from both devices) of outgoing Tel-to-IP calls that start with 10 to the first device and calls that start with 20 to the second device.

Figure 8-37: Routing Calls Between Devices

	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	

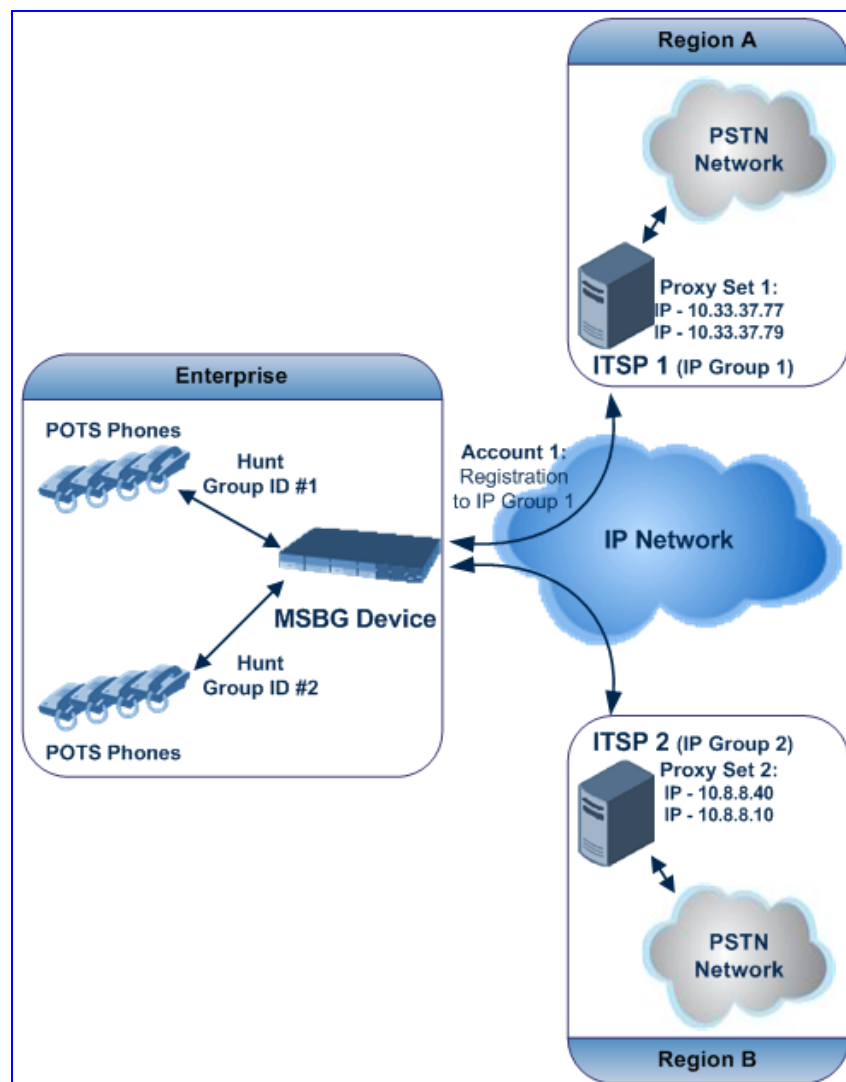
4. Make a call. Pick up the phone connected to port #1 of the first device and dial 102 (to the phone connected to port #2 of the same device). Listen for progress tones at the calling phone and for the ringing tone at the called phone. Answer the called phone, speak into the calling phone, and check 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.

8.3.9.4 SIP Trunking between Enterprise and ITSPs

By implementing the device's enhanced and flexible routing capabilities, you can "design" complex routing schemes. This section provides an example of an elaborate routing scheme for SIP trunking between an Enterprise's PBX and two Internet Telephony Service Providers (ITSP), using the device.

Scenario: In this example, an Enterprise has deployed the device with FXS interfaces. The first four phones operate with ITSP 1 (using UDP), while the next four phones (channels 5-8) operate with ITSP 2 (using TCP). ITSP 1 requires single registration (i.e., one registration for all four phones), while ITSP 2 requires registration per phone. Each ITSP implements two servers for redundancy and load balancing. The figure below illustrates this example setup:

Figure 8-38: Routing between ITSP and Enterprise PBX Example

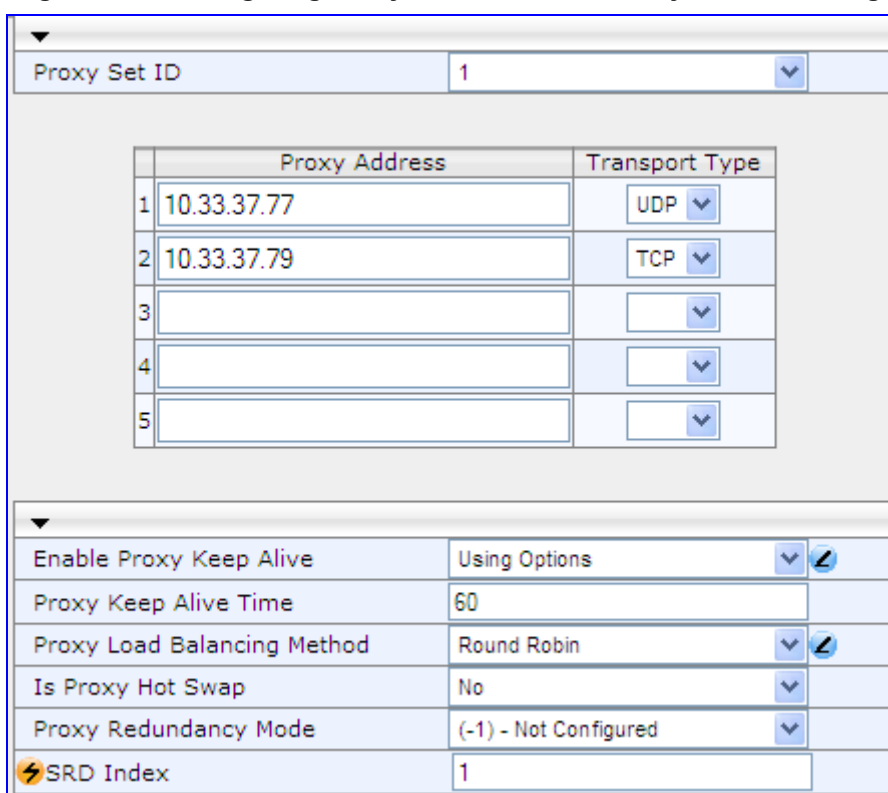


➤ **To configure call routing between an Enterprise and two ITSPs:**

1. Enable the device to register to a Proxy/Registrar server using the parameter IsRegisterNeeded.
2. In the 'Proxy Sets Table' page (see "Configuring Proxy Sets Table" on page 126), configure two Proxy Sets and for each, enable Proxy Keep-Alive (using SIP OPTIONS) and 'round robin' load-balancing method:
 - Proxy Set #1 includes two IP addresses of the first ITSP (**ITSP 1**) - 10.33.37.77 and 10.33.37.79 - and using UDP.
 - Proxy Set #2 includes two IP addresses of the second ITSP (**ITSP 2**) - 10.8.8.40 and 10.8.8.10 - and using TCP.

The figure below displays the configuration of Proxy Set ID #1. Perform similar configuration for Proxy Set ID #2, but using different IP addresses.

Figure 8-39: Configuring Proxy Set ID #1 in the Proxy Sets Table Page



Proxy Set ID: 1

	Proxy Address	Transport Type
1	10.33.37.77	UDP
2	10.33.37.79	TCP
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: 1

3. In the 'IP Group Table' page (see "Configuring IP Groups" on page 119), configure the two IP Groups #1 and #2. Assign Proxy Sets #1 and #2 to IP Groups #1 and #2 respectively.

Figure 8-40: Configuring IP Groups #1 and #2 in the IP Group Table Page

Index	1
Common Parameters	
Type	
Description	ITSP_1
Proxy Set ID	1
SIP Group Name	
Contact User	
Tel Profile ID	0

4. In the 'Hunt Group Table' page, enable the Trunks connected between the Enterprise's PBX and the device (Hunt Group ID #1), and between the local PSTN and the device (Hunt Group ID #2).

Figure 8-41: Assigning Channels to Hunt Groups

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 FXS			1-4	401	1	0
2	Module 2 FXS			5-8	405	2	0

5. In the 'Hunt Group Settings' page, configure 'Per Account' registration for Hunt Group ID #1 (without serving IP Group) and associate it with IP Group #1; Configure 'Per Endpoint' registration for Hunt Group ID #2 and associated it with IP Group #2.

Figure 8-42: Configuring Registration Mode for Hunt Groups and Assigning to IP Group

	Hunt Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	1	Cyclic Ascending	Per Account	1		
2	2	Cyclic Ascending	Per Endpoint	2		

6. In the 'Authentication' page, for channels 5-8 (i.e., Hunt Group ID #2), define for each channel the registration (authentication) user name and password.

Figure 8-43: Configuring Username and Password for Authenticating Channels 5-8

Gateway Port	User Name	Password
Module 1 Port 1 FXS		
Module 1 Port 2 FXS		
Module 1 Port 3 FXS		
Module 1 Port 4 FXS		
Module 3 Port 1 FXS	user1	1111
Module 3 Port 2 FXS	user2	2222
Module 3 Port 3 FXS	user3	3333
Module 3 Port 4 FXS	user4	4444

7. In the 'Account Table' page, configure a single Account for Hunt Group ID #1, including an authentication user name and password, and enable registration for this Account to ITSP 1 (i.e., Serving IP Group is 1).

Figure 8-44: Configuring Account for Registration to ITSP 1

Index	ServedTrunkGroup	ServingIPGroup	Username	Password	HostName	Register
2	1	1	ITSP1user	1234	ITSP1	1

8. In the 'Inbound IP Routing Table' page, configure that INVITEs with "ITSP1" as the hostname in the From URI are routed to Hunt Group #1, and INVITEs with "ITSP2" as the hostname in the From URI are routed to Hunt Group #2. In addition, configure calls received from ITSP1 as associated with IP Group #1.

Figure 8-45: Configuring ITSP-to-Hunt Group Routin

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Hunt Group ID	IP Profile ID	Source IPGroup ID
1		ITSP1	*	*		1		1
2		ITSP2	*	*		2		

9. In the 'Outbound IP Routing Table' page, configure Tel-to-IP routing rules for calls from Hunt Group #1 to IP Group #1, and from Hunt Group #2 to IP Group #2.

Figure 8-46: Configuring Hunt Group to ITSP Routing

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

8.3.10 Mapping PSTN Release Cause to SIP Response

The device's FXO interface interoperates between the SIP network and the PSTN/PBX. This interoperability includes the mapping of PSTN/PBX Call Progress Tones to SIP 4xx or 5xx responses for IP-to-Tel calls. The converse is also true - for Tel-to-IP calls, the SIP 4xx or 5xx responses are mapped to tones played to the PSTN/PBX.

When establishing an IP-to-Tel call, the following rules are applied:

- If the remote party (PSTN/PBX) is busy and the FXO device detects a Busy tone, it sends a SIP 486 Busy response to IP. If it detects a Reorder tone, it sends a SIP 404 Not Found (no route to destination) to IP. In both cases, the call is released. Note that if the parameter DisconnectOnBusyTone is set to 0, the FXO device ignores the detection of Busy/Reorder tones and doesn't release the call.
- For all other FXS/FXO release types (caused when there are no free channels in the specific Hunt Group), or when an appropriate rule for routing the call to a Hunt Group doesn't exist, or if the phone number isn't found), the device sends a SIP response (to IP) according to the parameter DefaultReleaseCause. This parameter defines Q.931 release causes. Its default value is '3', which is mapped to the SIP 404 response. By changing its value to '34', the SIP 503 response is sent. Other causes can be used as well.

8.3.11 Querying Device Channel Resources using SIP OPTIONS

The device reports its maximum and available channel resources in SIP 200 OK responses upon receipt of SIP OPTIONS messages. The device sends this information in the SIP X-Resources header with the following parameters:

- **telchs:** specifies the total telephone channels as well as the number of free (available) telephone channels
- **mediachs:** not applicable

Below is an example of the X-Resources:

```
X-Resources: telchs= 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).

8.4 SBC Application

This section provides a detailed description of the device's SBC application.

This section includes the following subsections:

- Overview of the SBC application (see "Overview" on page [480](#))
- SIP networking definitions (see "SIP Network Definitions" on page [482](#))
- SIP dialog-initiation process (see "SIP Dialog Initiation Process" on page [482](#))
- User registration and the device's database (see "User Registration and Internal Database" on page [490](#))
- Media handling (see "SBC Media Handling" on page [493](#))
- SBC Dialog Admission Control (see "SIP Dialog Admission Control" on page [502](#))
- Handling SIP 3xx Redirect Responses (see "Handling SIP 3xx Redirect Responses" on page [503](#))
- SIP Diversion and History-Info headers interworking (see "Interworking SIP Diversion and History-Info Headers" on page [505](#))
- SBC configuration example (see SBC Configuration Example on page [546](#))

8.4.1 Overview

The SBC application supports up to 150 SBC sessions and provides the following main features:

- NAT traversal (see "NAT Traversal" on page [481](#))
- VoIP firewall and security for signaling and media (see "VoIP Firewall" on page [481](#))
- Topology hiding (see "Topology Hiding" on page [481](#))
- SIP normalization (see "SIP Normalization" on page [482](#))
- Survivability (see "Survivability" on page [482](#))
- Routing (see "SIP Network Definitions" on page [482](#) and "SIP Dialog Initiation Process" on page [482](#)):
 - IP-to-IP routing translations of SIP, UDP, TCP, TLS (when extensive transcoding is not required)
 - Load balancing and redundancy of SIP servers
 - Routing according to Request-URI\Specific IP address\Proxy\FQDN
 - Alternative routing
 - Routing between different Layer-3 networks (e.g., LAN and WAN)
- Load balancing\redundancy of SIP servers
- Internet Telephony Service Providers (ITSP) accounts
- SIP URI user and host name manipulations (see "SIP Dialog Initiation Process" on page [482](#))
- Coder Transcoding (see "SBC Media Handling" on page [493](#))

8.4.1.1 NAT Traversal

The device supports NAT traversal, allowing, for example, communication with ITSPs with globally unique IP addresses, for LAN-to-WAN VoIP signaling (and bearer), using two independent legs. In addition, it also enables communication for "far-end" users located behind a NAT on the WAN. The device supports this by:

- Continually registering far-end users in its dynamic database
- Maintaining remote NAT binding state by frequent registrations, thereby, off-loading far-end registrations from the LAN IP PBX
- Using Symmetric RTP (RFC 4961) to overcome bearer NAT traversal

8.4.1.2 VoIP Firewall

The device provides a firewall for VoIP:

- SIP signaling:
 - Deep and stateful inspection of all SIP signaling packets
 - SIP dialog initiations may be rejected based on values of incoming SIP INVITE message and other Layer-3 characteristics
 - Packets not belonging to an authorized SIP dialog are discarded
- RTP:
 - Opening pinholes (ports) in the device's firewall based on Offer-Answer SDP negotiations
 - Deep packet inspection of all RTP packets
 - Late rouge detection - if a SIP session was gracefully terminated and someone tries to "ride on it" with rouge traffic from the already terminated RTP and SIP context, the VoIP Firewall prevents this from occurring
 - Disconnects call (after user-defined time) if RTP connection is broken
 - Black/White lists for both Layer-3 firewall and SIP classification

8.4.1.3 Topology Hiding

The device supports topology hiding, limiting the amount of topology information displayed to external parties. For example, IP addresses of ITSPs' equipment (e.g. proxies, gateways, and application servers) can be hidden from outside parties.

The device's topology hiding is provided by implementing back-to-back user agent (B2BUA) leg routing:

- Strips all incoming SIP Via header fields and creates a new Via value for the outgoing message
- Each leg has its own Route/Record Route set
- Modifies SIP To, From, and Request-URI host names
- Generates a new SIP Call-ID header value (different between legs)
- Changes the SIP Contact header to the device's own address
- Layer-3 topology hiding by modifying source IP address in the SIP IP header

8.4.1.4 SIP Normalization

The device supports SIP normalization, whereby the SBC application can overcome interoperability problems between SIP user agents. This is achieved by the following:

- Manipulation of SIP URI user and host parts
- Connection to ITSP SIP trunks on behalf of an IP-PBX - the device can register and utilize user and password to authenticate for the IP-PBX

8.4.1.5 Survivability

The device's SBC application provides two survivability features:

- Routing calls to alternative routes such as the PSTN
- Routing calls between user agents in the local network using a dynamic database (built according to registrations of SIP user agents)

For an example of configuring SBC survivability, see "Survivability and Alternative Routing" on page 556.

8.4.2 SIP Network Definitions

The device's SBC application can implement multiple SIP signaling and RTP (media) interfaces. For a detailed description, see "Multiple SIP Signaling/Media Interfaces Environment" on page 405.

8.4.3 SIP Dialog Initiation Process

The device's SIP dialog initiation process concerns all incoming SIP dialog initiation requests. This includes SIP methods such as INVITE, SUBSCRIBE, OPTIONS, REFER, INFO, UNSOLICITED NOTIFY, MESSAGE, and REGISTER.

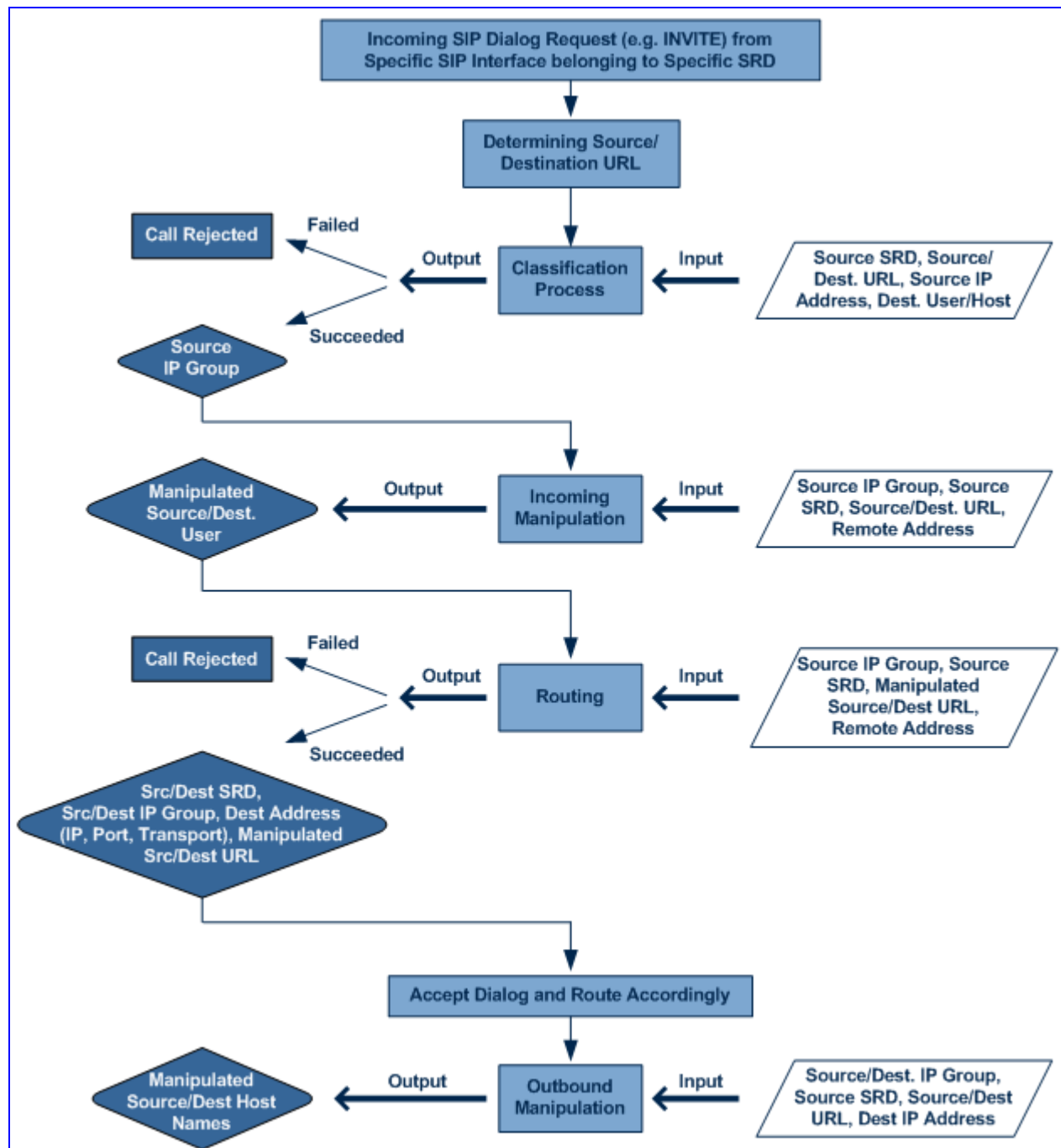
The SIP dialog initiation process consists of the following stages:

- Determining Source and Destination URL (see "Determining Source and Destination URL" on page 483)
- Classifying Source IP Group (see "Source IP Group Classification" on page 484)
- IP-to-IP Routing (see "SBC IP-to-IP Routing" on page 485)
- Manipulating IP-to-IP Inbound and Outbound SIP dialogs (see "IP-to-IP Inbound and Outbound Manipulation" on page 486)

For a description of the Registration process, see "User Registration and Internal Database" on page 490.

The flowchart below illustrates this process:

Figure 8-47: Routing Process



8.4.3.1 Determining Source and Destination URL

The SIP protocol has more than one URL in a dialog establishing request that might represent the source and destination URL. When handling an incoming request, the device determines which SIP headers are used for source and destination URLs. Once these URLs are determined, the input user and host are taken from them.

- **INVITE dialogs:**

- Source URL: if exists, obtained from the P-Asserted\Preferred-Identity header; otherwise, from the From header
- Destination URL: obtained from the Request-URI

■ **REGISTER dialogs:**

- Source URL: obtained from the To header
- Destination URL: obtained from the Request-URI

8.4.3.2 Source IP Group Classification

The device supports the configuration of rules for classifying incoming SIP dialog initiating request. The classification identifies the incoming SIP dialog request as belonging to a specific IP Group (from where the SIP dialog request originated).

Classification begins with the device's Registration database, where it searches for a match by checking if the request arrived from a registered user:

- Compares received Contact to the Contact of the registered user
- Compares P-Asserted/From URL to the registered AOR

If the database search is unsuccessful, the classification process proceeds with locating a Proxy Set (associated with the SIP dialog request's IP address, or IP address, port, and transport type if the ClassificationInput parameter is enabled in the Proxy Set) and then finding a match with a corresponding IP Group in the IP Group table. Each IP Group can be classified according to its Proxy Set (if in the IP Group table the parameter ClassifyByProxySet is enabled). If enabled, the device classifies Requests arriving from the IP Group's Proxy Set as coming from this IP Group. The classification is done according to the Proxy IP list (in case of host names, then according to the dynamically resolved IP address list). Note that this classification is not relevant in cases where multiple IP Groups use the same Proxy Set.

If classification based on Proxy Set is unsuccessful, the device proceeds to the Classification table, which searches for a source IP Group based on the following matching rules: Source IP Address, Source Username Prefix, Source Host Prefix, Destination Username Prefix, Destination Host Prefix, and Source SRD.

If the above classification process fails to determine the source IP Group to which the incoming packet belongs, the call can either be rejected, or allowed and processed (by assigning it to the default IP Group of the default SRD). This last classification is determined by the parameter AllowUnclassifiedCalls.

This IP Group is afterwards used for the following purposes:

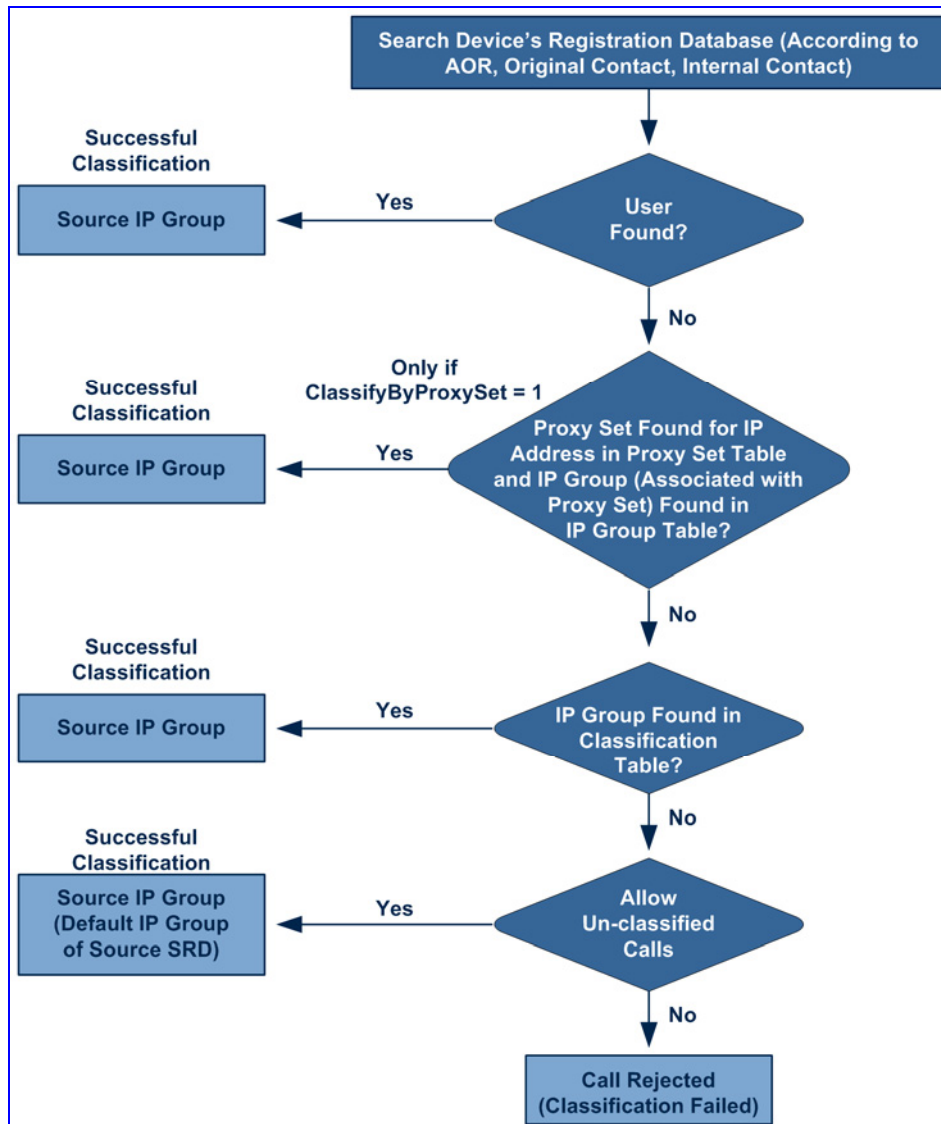
- Input for the manipulation and routing processes
- Defining SIP behavior and IP Profile, Media Realm and matching account



Note: Incoming REGISTER messages are recorded in the device's database and sent to a destination only if they are associated with a source IP Group that is of USER type.

The flowchart below illustrates the classification process:

Figure 8-48: Classification Process (Identifying IP Group or Rejecting Call)



8.4.3.3 SBC IP-to-IP Routing

The device's SBC application employs a comprehensive and flexible routing scheme:

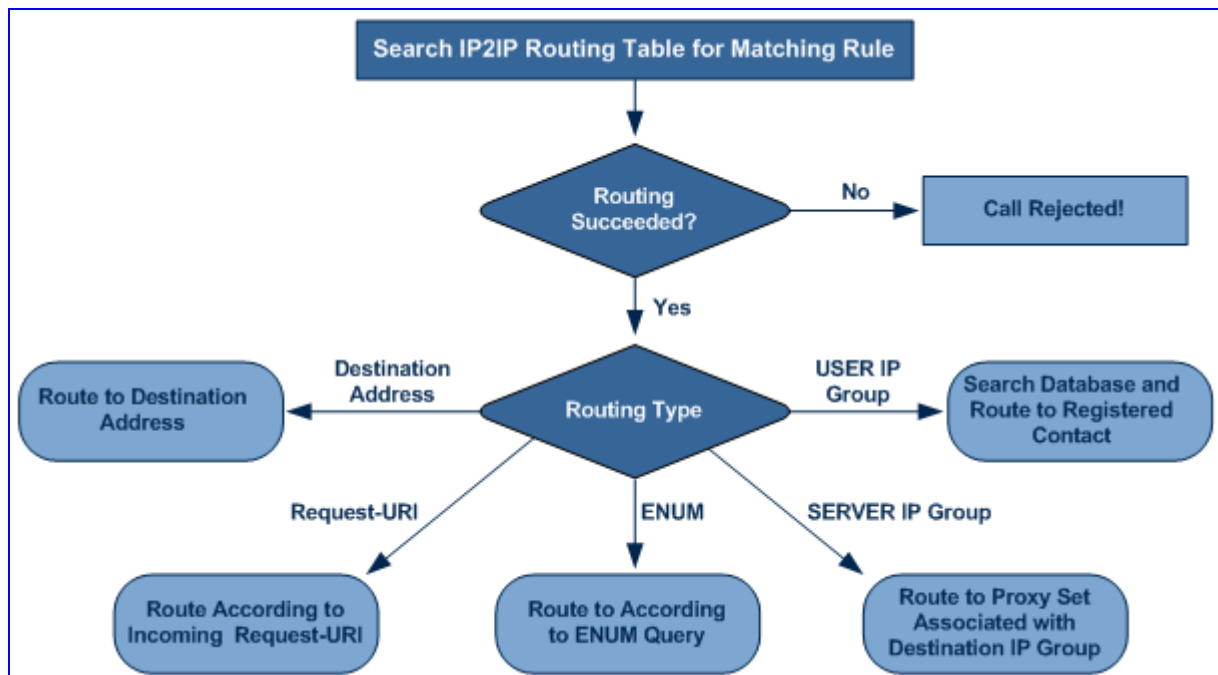
- Routing rules according to Layer-3/4 and SIP characteristics
- Routing to different destination types:
 - Request-URI (of incoming SIP dialog initiating requests)
 - Specific destination IP address (based on IP address, host name, port, transport type, and/or SRD). Routing to a host name can be resolved using NAPTR/SRV/A-Record.
 - Specific FQDN (NAPTR/SRV/A-Record Resolutions)
 - Registered User Contact listed in the device's database (only for USER-type IP Groups)

- Destination IP Group (address defined by Proxy Set associated with the IP Group) with the ability of load balancing and redundancy
- ENUM query
- Alternative Routing
- Routing between two different Layer-3 networks
- Transport protocol translator (UDP to TCP to TLS)
- Source and destination user name manipulation (pre/post routing)

The device's IP-to-IP routing rules are configured in the IP-to-IP Routing table. This table provides enhanced IP-to-IP call routing capabilities for routing received SIP messages such as INVITE messages to a destination IP address. The routing rule must match one of the following input characteristics: Source IP Group, Source Phone Prefix, and/or Source Host Prefix.

For all destination types listed above except destination IP Group, the IP Group can optionally be itself, configured to provide destination SRD and/or IP Profile. If neither destination SRD nor destination IP Group are defined, the destination SRD is the source SRD and the destination IP Group is its default IP Group.

Figure 8-49: IP-to-IP Routing Types

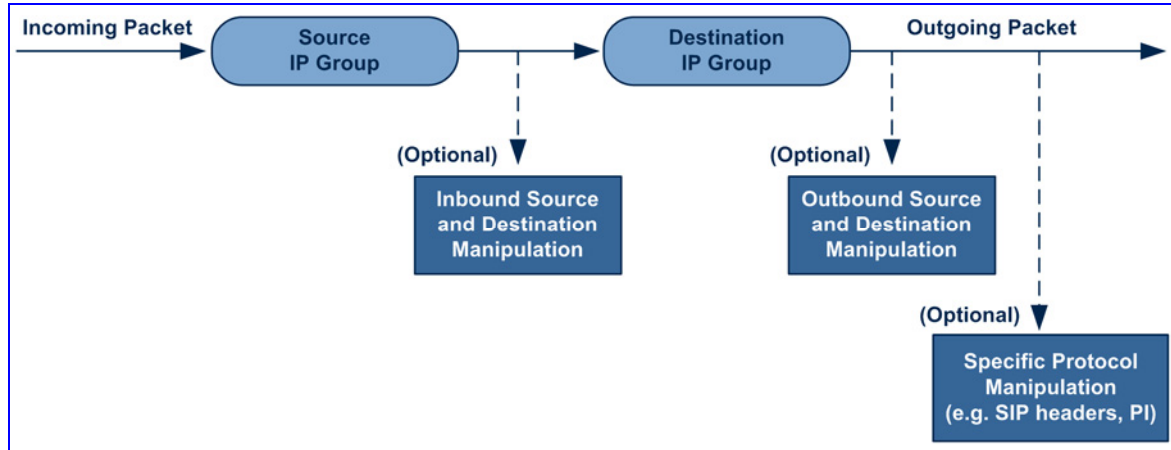


8.4.3.4 IP-to-IP Inbound and Outbound Manipulation

The device supports SIP URI user part (source and destination) manipulations for inbound and outbound routing. These manipulations can be applied to a source IP group, source and destination host and user prefixes, and/or user-defined SIP request (e.g., INVITE, OPTIONS, SUBSCRIBE, and/or REGISTER). Since outbound manipulations are performed after routing, the outbound manipulation rule matching can also be done by destination IP Group.

Manipulated destination user and host are performed on the following SIP headers: Request-URI, To, and Remote-Party-ID (if exists). Manipulated source user and host are performed on the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists).

Figure 8-50: SIP URI Manipulation in IP-to-IP Routing



In addition, you can restrict source user identity in outgoing SIP dialogs in the Outbound Manipulation table (using the column PrivacyRestrictionMode):

- **[0]** Transparent (default): no device intervention in anything SIP data related to privacy
- **[1]** Don't change privacy: the user identity remains the same as in the incoming INVITE. If a restricted number exists, the restricted presentation is normalized as follows:
 - From URL header - anonymous@anonymous.invalid.
 - If a P-Asserted-Identity header exists (either in the incoming INVITE or added by the device), a Privacy header is added with the value "id".
- **[2]** Restrict: the user identity is restricted (the restricted presentation is as mentioned above).
- **[3]** Remove Restriction: the device attempts to reveal the user identity by setting user values to the From header and removing the privacy "id" value if the Privacy header exists.
- If the From header user is anonymous, the value is taken from the P-Preferred-Identity, P-Asserted-Identity, or Remote-Party-ID header (if exists).

The device identifies an incoming user as restricted if one of the following exists:

- From header user is anonymous.
- P-Asserted-Identity and Privacy headers contain the value "id".

All restriction logic is performed after the user number has been manipulated.

The manipulations are configured using the IPOutboundManipulation and IPInboundManipulation parameters.

Host name (source and destination) manipulations are simply host name substitutions with the names defined for the source and destination IP Groups respectively (if any, in the IP Group table).

Below is an example of a call flow and consequent SIP URI manipulations:

Figure 8-51: SIP INVITE (Manipulations) from LAN to WAN

Incoming INVITE (from LAN)	Outgoing INVITE (to WAN)
<pre> INVITE sip:1000@10.2.2.3;user=phone;x=y;z=a SIP/2.0 Via: SIP/2.0/UDP 10.2.2.6;branch=z9hGLLLLan From: <sip:7000@10.2.2.6;user=phone;x=y;z=a>;tag=OILAN;parameter1=arik To: <sip:1000@10.2.2.3;user=phone> Call-ID: USELLLLAN@10.2.2.3 CSeq: 1 INVITE Contact: <sip:7000@10.2.2.3> Supported: em,100rel,timer,replaces Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK User-Agent: Sip Message GeneratorV1.0.0.5 Content-Type: application/sdp Content-Length: 155 v=0 o=SMG 791285 795617 IN IP4 10.2.2.6 s=Phone-Call c=IN IP4 10.2.2.6 t=0 0 m=audio 6000 RTP/AVP 8 a=rtpmap:8 pcma/8000 a=sendrecv a=ptime:20 </pre>	<pre> INVITE sip:9721000@ITSP;user=phone;x=y;z=a SIP/2.0 Via: SIP/2.0/UDP 212.179.1.12;branch=z9hGWwan From: <sip:97000@IP_PBX;user=phone;x=y;z=a>;tag=OWan;parameter1=arik To: <sip:9721000@ITSP;user=phone> Call-ID: USEVWWAN@212.179.1.12 CSeq: 38 INVITE Contact: <sip:7000@212.179.1.12> Supported: em,100rel,timer,replaces Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER User-Agent: Sip Message GeneratorV1.0.0.5 Content-Type: application/sdp Content-Length: 155 v=0 o=SMG 5 9 IN IP4 212.179.1.11 s=Phone-Call c=IN IP4 212.179.1.11 t=0 0 m=audio 8000 RTP/AVP 8 a=rtpmap:8 pcma/8000 a=sendrecv a=ptime:20 </pre>

The SIP message manipulations in the example above (contributing to typical topology hiding) are as follows:

SIP Manipulation	From	To
Inbound Source SIP URI User Name	7000	97000 (blue)
Source IP Group Name (SIP URI Host Name)	10.2.2.6	IP_PBX (blue)
Inbound Destination SIP URI User Name	1000	9721000 (red)
Destination IP Group Name (SIP URI Host Name)	10.2.2.3	ITSP (red)

8.4.3.5 SIP Header Manipulation

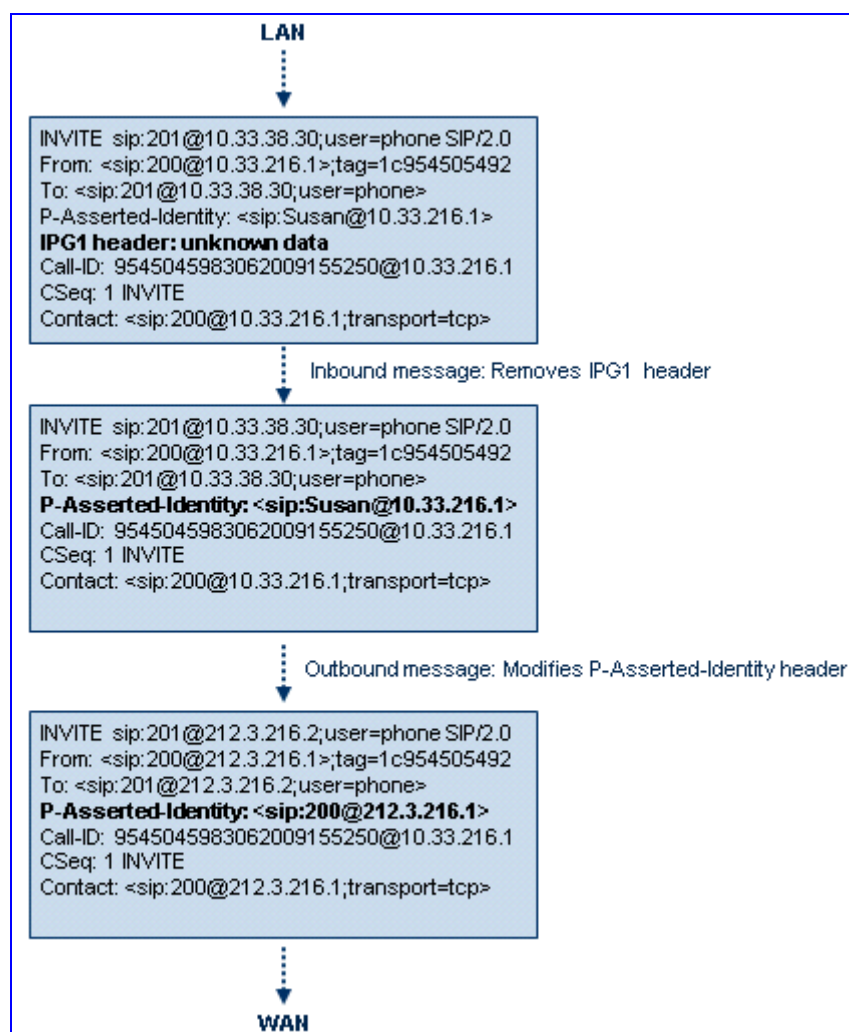
The device provides enhanced SIP header manipulation, including insertion, removal, and/or modification of SIP headers and parameters. This manipulation is configured in the Message Manipulations table (MessageManipulations parameter). This feature enables the normalization of SIP messaging fields between communicating network segments. For example, it allows service providers to design their own policies on the SIP messaging fields that must be present before a SIP call enters their network. Similarly, enterprises and small businesses may have policies for the information that can enter or leave their networks for policy or security reasons from a service provider. The manipulations can also be implemented to resolve incompatibilities between SIP devices inside the enterprise network.

SIP Messaging manipulation supports the following:

- Addition of new headers.
- Removal of headers ("Black list").
- Modification of header components - value, header value (e.g., URI value of the P-Asserted-Identity header can be copied to the From header), call's parameter values.
- Deletion of SIP body (e.g., if a message body isn't supported at the destination network this body is removed).

- Translating one SIP response code to another.
- Topology hiding (generally present in SIP headers such as Via, Record Route, Route and Service-Route).
- Configurable identity hiding (information related to identity of subscribers for example, P-Asserted-Identity, Referred-By, Identity and Identity-Info).
- Apply conditions per rule - the condition can be on parts of the message or call's parameters.
- Multiple manipulation rules on the same SIP message.

Figure 8-52: SIP Header Manipulation Example



The manipulation is performed on SIP messages according to the Classification table (source/destination of username/host prefixes and source IP address). The manipulation can be performed on message type (Method, Request/Response, and Response type). Message manipulations are performed only after the classification, inbound manipulations and routing are successfully performed (i.e., manipulations are performed only in the outgoing leg).

SIP Message manipulation rules can be assigned to an IP Group in the IP Group table (IPGroup parameter) and determined whether they must be performed for inbound or outbound messages.


Notes:

- Unknown SIP parts can only be added or removed.
- SIP manipulations do not allow you to remove or add mandatory SIP headers. Only the modify option is available for mandatory headers and is performed only on requests that initiate new dialogs. Mandatory SIP headers include To, From, Via, CSeq, Call-Id, and Max-Forwards. Mandatory SDP headers include v, o, s, t, c, and m.
- When multiple manipulations rules apply to the same header, the second rule applies to the result string of the first rule.
- Manipulating any value in the message body causes a change to the Content-length header automatically.
- SDP body manipulations are currently not supported.

8.4.4 User Registration and Internal Database

To allow registrations to traverse the SBC, the device must be configured with at least one IP Group of type USER. USER IP Groups represent a group of user agents that share the following characteristics:

- Perform registrations and share the same serving proxy\registrar
- Possess identical SIP and media behavior
- Reside on the same Layer-3 network and are associated with the same SRD

Typically, the device is configured as the user agent's outbound proxy and the device is configured (using the IP2IP Routing table) to route requests received from this IP Group to the serving proxy and vice versa. Survivability can be achieved using the alternative routing feature.

8.4.4.1 Initial Registration Request Processing

Registration requests have different processing policies than other SIP methods:

1. Determining source and destination URL's:
 - The source URL is obtained from the To header
 - The destination URL is obtained from the Request URI
2. Classification: The REGISTER classification process is the same as the general classification process (described in previous sections). The source IP Group must be of type USER. If classification fails or the source IP Group is not of type USER, the registration is rejected.
3. Routing: The REGISTER routing is performed using the IP2IP Routing table:
 - The destination type can be an IP Group, specific IP address, Request-URI, or ENUM query (can also use DNS queries).
 - If the destination IP Group is of type USER, then the registration is not be forwarded. Instead, the device accepts (replies with 200 OK response) or rejects (Reply with 4xx) the request according to the user group policy.

4. Internal registration database: If the source IP Group is of type User and registration succeeds (replied with 200 OK by the IP-PBX), then the device adds a record to its database that identified the specific contact of this specific user (AOR). This record is used later to route requests to this specific user (either in normal or in survivability modes).
5. Alternative Routing: Alternative routing can be configured in the IP2IP Routing table for REGISTER requests.
6. Inbound Manipulation: The SBC record in the device's database includes the Contact header. Every REGISTER request is added to the database before manipulation, allowing correct user identification in the SBC Classification process for the next received request.
7. Session Admission Control: Applies various limitations on incoming and outgoing REGISTER requests. For example, limiting REGISTER requests from a certain IP Group/SRD. Note that this limitation is only for concurrent register dialogs and not concurrent registrations in the internal database.
8. The device can retain the original value of the SIP Expires header received from the user or proxy, in the outgoing REGISTER message. This feature also applies when the device is in "survivability" state (i.e., REGISTER requests cannot be forwarded to the proxy and is terminated by the device). This is configured by the SBCUserRegistrationTime, SBCProxyRegistrationTime, and SBCSurvivabilityRegistrationTime parameters.
9. By default, the Contact of the outgoing REGISTER is populated with a unique Contact generated by the device and associated with this specific registration. Alternatively, the original user can be retained in the Contact and used in the outgoing REGISTER request (using the SBCKeepContactUserinRegister parameter).

8.4.4.2 Internal Database

The device manages a dynamic database that is updated according to registration requests that traverse the SBC. Each database entry represents a binding between an AOR and one or more contact. Database bindings are added upon successful registration responses. For specific registrations, the AOR is obtained from the SIP To header and the contact is taken from the SIP Contact header.

Database bindings are removed in the following cases:

- Successful de-registration responses (REGISTER with Expires header that equals zero)
- Registration failure responses
- Timeout of the Expires header value (in scenarios where the user agent did not send a refresh registration request)

The device's database can include up to 200 registered SBC users.

The database has the following limitations:

- Maximum of five contacts per AOR
- The same contact cannot belong to more than one AOR
- Contacts with identical URIs and different ports and transport types are not supported (same key is created)
- Multiple contacts in a single REGISTER is not supported
- One database is shared between all USER-type IP Groups

8.4.4.3 Routing using Internal Database

Typically, routing using the database is applicable to all method types other than registrations. To route to a registered user (using the internal dynamic database), the following steps must be taken:

1. An IP2IP Routing rule with the desired input parameters (matching characteristics) and the destination type as IP Group (operation rule).
2. The destination IP Group must be of type USER.
3. To find a match for these specific rules, the device attempts to locate a match between the incoming Request-URI and (according to the description order):
 - a. Unique contact - the Contact generated by the SBC and sent in the initial registration request to the serving proxy
 - b. Registered AOR - the AOR of the incoming REGISTER request
 - c. Registered contact - the Contact of the incoming REGISTER request

If registrations are destined to the database (using the above rules), the device does not attempt to find a database match, but instead replies with 200 OK (used for Survivability). Once a match is found, the request is routed either to the contact received in the initial registration or (if the device identifies that the user agent is behind a NAT) to the source IP address of the initial registration.

8.4.4.4 Registration Refreshes

Registration refreshes are incoming REGISTER requests that are associated with a specific registered user. The association is performed by searching the internal registration database. These refreshes are routed to the serving proxy only if the serving proxy Expires time is about to expire; otherwise, the device responds with a 200 OK without routing the REGISTER. Each such refreshes also refresh the internal timer time set on the device for this specific registration.

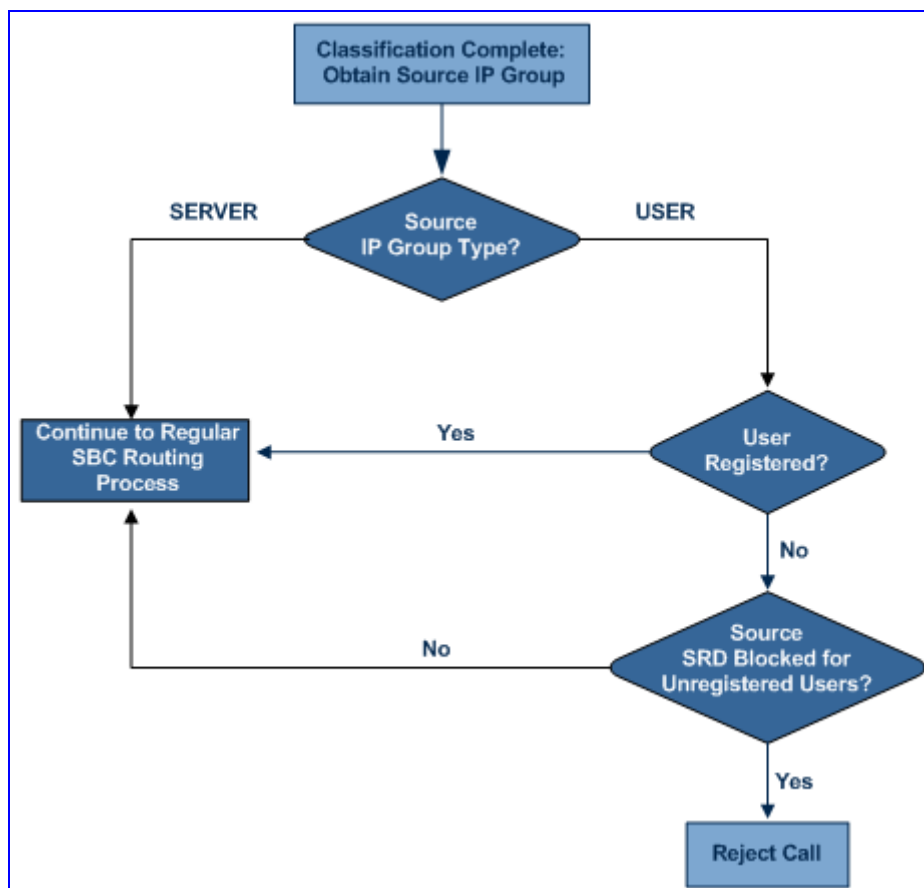
8.4.4.5 Registration Restriction Control

The device provides flexibility in controlling user's registration:

- **Limiting Number of Registrations per Source SRD and/or IP Group:** You can limit the number of users that can register with the device. This limitation can be applied per source IP Group and/or SRD. By default, no limitation exists for registered users. This is configured using the parameters SRD or IPGroup.

- **Blocking Incoming Calls from Unregistered Users:** You can block incoming calls (INVITE requests) from unregistered users (pertaining to USER-type IP Groups). By default, calls from unregistered users are not blocked. This is configured using the parameter SRD. The flowchart below depicts the process for blocking unregistered users. When the call is rejected, the device sends a SIP 500 "Server Internal Error" response to the remote end.

Figure 8-53: Blocking Incoming Calls from Unregistered Users



8.4.5 SBC Media Handling

Media behavior includes anything related to the establishment, management and termination of media sessions within the SIP protocol. Media sessions are created using the SIP "offer"/"answer" mechanism. If successful, the result is a bi-directional media (RTP) flow (e.g. audio, fax, modem, DTMF). Each offer/answer may create more than one media session of different types (e.g. audio and fax). In a SIP dialog, multiple offer/answer transactions may occur, each may change the media sessions characteristics (e.g. IP address, port, coders, media types, and RTP mode). The media capabilities exchanged in an offer/answer transactions include the following:

- Media types (Audio, Secure Audio, Video, Fax, Text...)
- IP addresses and ports of the media flow
- Media flow mode (send receive, receive only, send only, inactive)
- Media coders (coders and their characteristics used in each media flow)
- Other (standard or proprietary) media and session characteristics

Even though the device usually does not change the negotiated media capabilities (mainly performed by the remote user agents), it does examine the media exchange to control negotiated media types (if necessary) and to know how to open the RTP media channels (IP addresses, coder type, payload type etc.).

The device is aware and sometimes active in the offer\answer process due to the following:

- NAT traversal: the device changes the SDP address to be its own address, thereby, resolving NAT problems.
- Firewall and security:
 - RTP pin holes - only RTP packets related to a successful offer\answer negotiation traverse the device: When the device initializes, there are no RTP pin holes opened, this means that each RTP\RTCP packets destined to the device are discarded. Once an offer\answer transaction ends successfully, an RTP pin hole is opened and RTP\RTCP flows between the two remote user agents. Once a pin hole is opened, the payload type and RTP header version is validated for each packet. RTP pin holes close if one of the associated SIP dialogs is closed (may also be due to broken connection).
 - Late rogue detection - once a dialog is disconnected, the related pin holes also disconnect.
 - Deep Packet inspection of the RTP that flows through the opened pin holes.
- Adding of media functionality to SIP user agents:
 - Transcoding (for a description on the transcoding modes, see "Transcoding Modes" on page 499)
 - Broken connection

According to the above functionalities, the call can be configured to operate in one of the following modes:

- **Media Anchoring without Transcoding (Transparent):** RTP traverses the device with minimal RTP packet changes (no DSP resources needed). This is typically used to solve NAT, firewall, and security issues. In this mode, all the "audio" coders in the received offer are included in the SBC outgoing offer. The Coder Table configuration has no effect on the coders in the outgoing offer. For a detailed description, see "Media Anchoring without Transcoding (Transparent)" on page 494.
- **Media Anchoring with Transcoding:** RTP traverses the device and each leg uses a different coder or coder parameters (DSP resources are required). For a detailed description, see "Media Anchoring with Transcoding" on page 495.
- **No Media Anchoring:** The RTP packet flow does not traverse the device. Instead, the two SIP UA's establish a direct RTP/SRTP flow between one another (see "No Media Anchoring" on page 497).

8.4.5.1 Media Anchoring without Transcoding (Transparent)

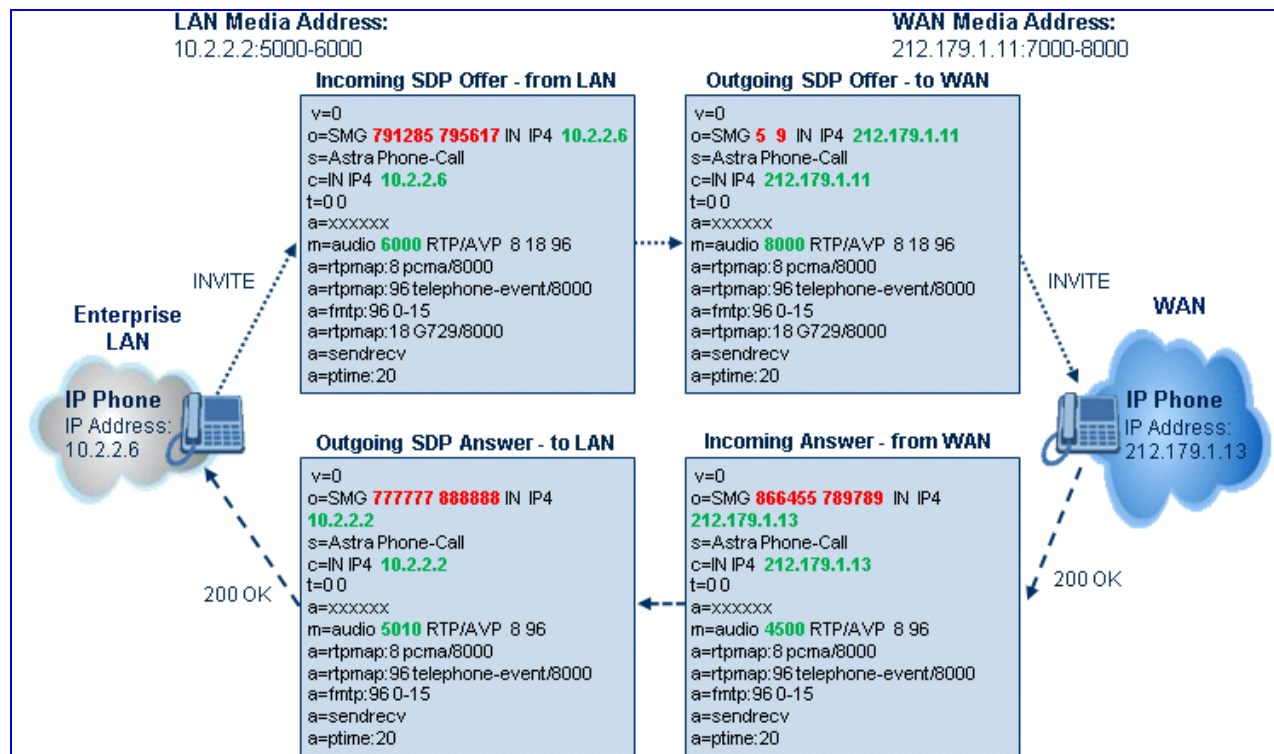
To direct the RTP to flow through the device (for NAT traversal, firewall and security), all IP address fields in the SDP are modified:

- Origin: IP address, session and version id
- Session connection attribute ('c=' field)
- Media connection attribute ('c=' field)

- Media port number
- RTCP media attribute IP address and port (if the parameter EnableRTCPAttribute is set to 1)

Each SBC leg allocates and uses the device's local ports (e.g., for RTP/RTCP/fax). The local ports are allocated from a Media Realm associated with each leg. The legs are associated with a Media Realm as follows: If the leg's IP Group is configured with a Media Realm, then this is the associated Media Realm; otherwise, the leg's SRD Media Realm is the associated one. The figure below illustrates an example of SDP handling for a call between IP Phone 10.2.2.6 (LAN) and a remote IP Phone 212.179.1.13 ().

Figure 8-54: SDP Offer/Answer Example

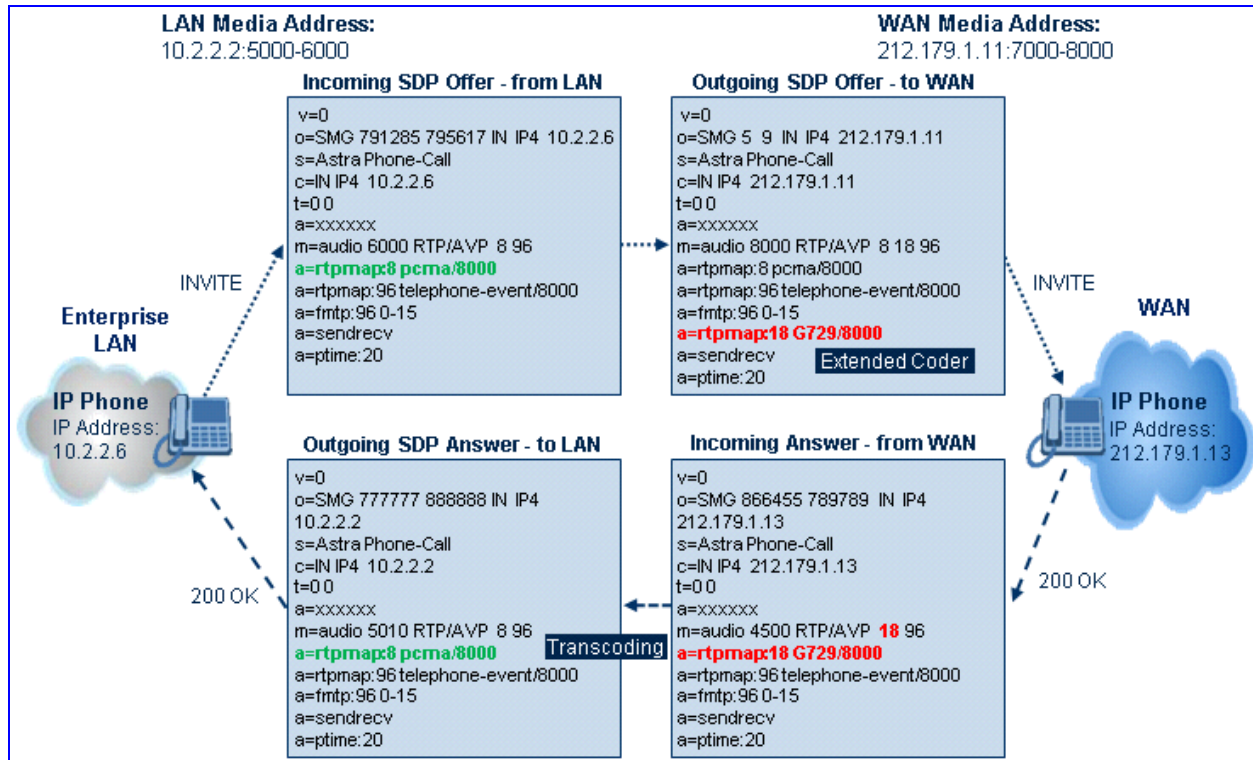


8.4.5.2 Media Anchoring with Transcoding

The device performs transcoding when there are no common coders between the two user agents (i.e., the SDP answer from one user agent doesn't include any coder included in the offer previously sent by the other user agent). For transcoding, the device can be configured to add media capabilities to user agents pertaining to a specific IP Group, and then perform transcoding in cases where the selected coder in the answer SDP is not one that appears in the original offer. The capabilities that can be added are one or more of the device's supported coders and are configured by using the parameter SBCExtensionCodersGroupID (points to a coders list) in the IP Profile table (which is assigned to the IP Group). Therefore, to allow user agents of different IP Groups to communicate with each other (regardless of their capabilities), an extended coders table with at least one coder that is supported by each IP Groups' user agents needs to be assigned to each IP Group. Therefore, each offer destined to specific IP Groups include this coder.

In the scenario depicted in the figure below, the IP phone on the LAN side initiates a call to the IP phone on the WAN. The initial SDP offer (from the LAN leg) includes codec G.711 as its supported codec. Since this is sent to a Destination IP Group that is configured with an extended coder list, on the WAN leg the device adds another supported codec G.729 to the SDP, which is now offered to the WAN IP phone. The WAN IP phone chooses the extended codec (G.729) in its SDP answer to the device's WAN leg. Since this codec was not included in the original incoming offer, the device performs transcoding (between G.729 and G.711) between its two legs, allowing the streaming of media to occur.

Figure 8-55: Transcoding using Extended Coders (Example)



For an SDP offer to provide an extended coder list to a remote user agent, the following prerequisites must be fulfilled:

- An extended coders list has been configured for the user agent's IP Group (i.e., Destination IP Group)
- The incoming offer contains at least one supported coder (otherwise, transcoding can't be performed)
- Both legs have available DSP's
- T.38 doesn't appear in the offer

If the above prerequisites are not met, the SDP offer is sent without the extended coders list. The coders from the extended list are added after the ones from the original offer (decreases transcoding probability). Coders common between the extended coders list and those in the original SDP offer are not added. Transcoding may be performed even in scenarios when the same coder has been chosen - this occurs if the coders use different coder parameters (e.g. rate and packetization time).

The device also supports early media, whereby the first offer/answer transaction is finalized and the media flow starts before the SIP call is connected (before the INVITE 200 OK response). The offer and answer options can be included in the following SIP messages:

- Offer in first INVITE, answer on 180, and no or same answer in the 200 OK
- Offer in first INVITE, answer on 180, and a different answer in the 200 OK (not

standard)

- INVITE without SDP, offer in 180, and answer in PRACK
- PRACK and UPDATE transactions can also be used for initiating subsequent offer\answer transactions before the INVITE 200 OK response.
- In a SIP dialog life time, media characteristics after originally determined by the first offer\answer transaction can be changed by using subsequent offer\answer transactions. These transactions may be carried either in UPDATE or ReINVITE SIP transactions. The media handling is similar to the original offer\answer handling. If the offer is rejected by the remote party, then no media changes occur (e.g. INVITE without SDP, then 200 OK and ACK, offer\answer within an offer\answer, and Hold ReINVITE with IP address of 0.0.0.0 - IP address is unchanged).

8.4.5.3 No Media Anchoring

The No Media Anchoring feature enables the use of SBC signaling capabilities without handling the RTP/SRTP (media) flow between remote SIP user agents (UA). The RTP packet flow does not traverse the device, instead, the two SIP UA's establish a direct RTP/SRTP flow between one another. Signaling continues to traverse the device with minimal intermediation and involvement to enable certain SBC abilities such as routing.

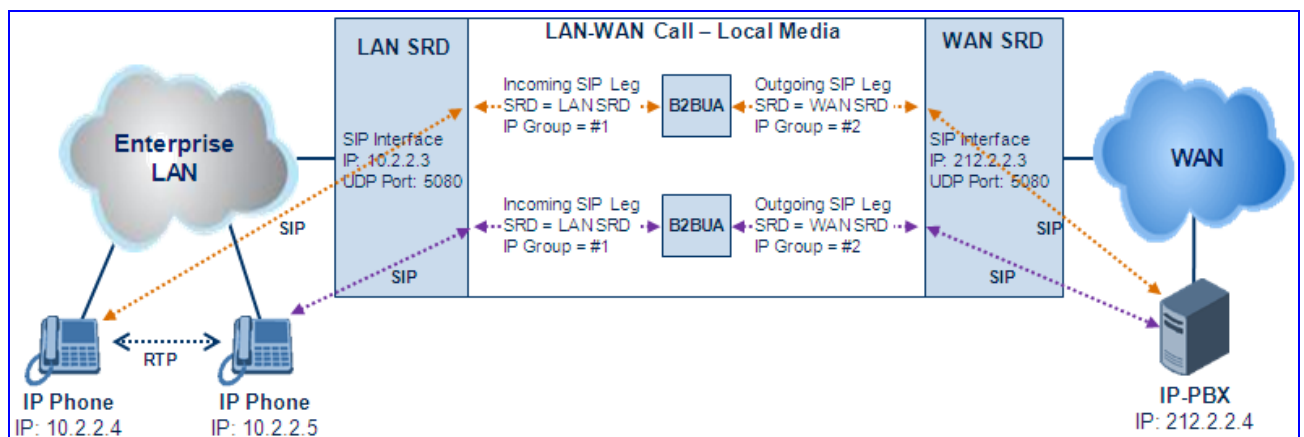
In contrast to the regular SBC implementation, the No Media Anchoring feature:

- Does not perform any manipulation on SDP data (offer/answer transaction) such as ports, IP address, coders.
- Opening voice channels and allocation of IP media ports are not required.

The No Media Anchoring feature is typically implemented in the following scenarios:

- SBC device is located within the LAN.
- Calls between two SIP UA's in the same network (LAN) and signals are sent to a SIP proxy server that is located in the WAN (as illustrated in the figure below).

Figure 8-56: SBC SIP Signaling without RTP Media Flow



The benefits of implementing the No Media Anchoring feature include the following:

- Saves network bandwidth
- Reduces CPU usage (no RTP/SRTP handling)
- Avoids interference in SDP negotiation and header manipulation on RTP/SRTP

The No Media Anchoring process is as follows:

1. Identifying a No Media Anchoring call - according to configuration and the call's properties (such as source, destination, IP Group, and SRD).
2. Handling the identified No Media Anchoring call.

The No Media Anchoring feature is enabled using the parameter `SBCDirectMedia`. You can also enable No Media Anchoring per SRD, where calls between two UA's that pertain to the same SRD (source and destination) are handled as No Media Anchoring (direct media) calls.



Notes:

- No Media Anchoring calls cannot operate simultaneously with the following SBC features:
 - Force transcoding
 - Extension Coders
 - Extension of RFC 2833/Out-of-band DTMF/In-band DTMF
 - Extension of SRTP/RTP
 All restriction features (Allowed Coders, restrict SRTP/SRT, restrict RFC 2833) can operate simultaneously. Once No Media Anchoring is enabled, the features listed above are disabled.
- The Coder Restriction feature operates simultaneously with No Media Anchoring calls. Restricted coders are removed from the SDP offer message.
- When two UA's pertain to the same SRD, the parameter `IntraSRDMediaAnchoring` is set to 1, and one of the UA's is defined as a foreign user (example, "follow me service") located in the WAN, while the other UA is located in the LAN: calls between these two UA's can't be established until `IntraSRDMediaAnchoring` is set to 0, as the device doesn't interfere in the SIP signaling. In other words, parameters such as IP addresses are not manipulated for calls between LAN and WAN (although required).
- When the parameter `SBCDirectMedia` is disabled, No Media Anchoring calls between two UA's belonging to separate SRD's cannot be configured. No Media Anchoring calls between two UA's belonging to the same SRD is configurable only (in this case).

8.4.5.4 Interworking DTMF Methods

The device supports interworking between various DTMF methods such as RFC 2833, In-Band DTMF's, and SIP INFO (Cisco/Nortel/Korea). By default, the device allows the remote user agents to negotiate (in case of RFC 2833) and passes DTMF without intervention. However, if two user agents (UA) support different DTMF methods, the device can interwork these different DTMF methods at each leg.

This DTMF interworking feature is enabled using IP Profiles (*ini* file parameter `IPProfile`):

- `SBCRFC2833Behavior` - affects the RFC 2833 SDP offer\answer negotiation:
 - **[0]** (default): the device does not intervene in the RFC 2833 negotiation.
 - **[1]**: each outgoing offer\answer includes RFC 2833 in the offered SDP (the device adds RFC 2833 only if the incoming offer does not include RFC 2833).
 - **[2]**: the device removes RFC 2833 from the incoming offer.

- **SBCAlternativeDTMFMethod** – the device's first priority for DTMF method at each leg is RFC 2833. Therefore, if a specific leg negotiates RFC 2833 successfully, then the chosen DTMF method for this leg is RFC 2833. For legs where RFC 2833 is not negotiated successfully, the device uses this parameter to determine the DTMF method for the leg.
 - **[0]** (default): the device does not attempt to interwork any special DTMF method
 - **[1]**: In Band
 - **[2]**: INFO, Cisco
 - **[3]**: INFO, Nortel
 - **[4]**: INFO, Korea

The chosen DTMF method determines (for each leg) which DTMF method is used for sending DTMF's. If the device interworks between different DTMF methods and one of the methods is In-band\RFC 2833, detection and generation of DTMF methods requires DSP allocation.

8.4.5.5 Transcoding Modes

The device supports the configuration of the voice transcoding mode (media negotiation) between the two SBC legs. The device can be configured to perform transcoding only when necessary. Typically, the SBC passes RTP packets transparently (RTP-to-RTP) between the two user agents. If the device is configured to always perform transcoding, then transcoding is performed on the outgoing SBC leg and the device's SBC application interworks the media by implementing PSTN transcoding (since both legs have different media capabilities).

In the SBC application, forced transcoding of voice in an SBC session allows the device to receive capabilities that are not negotiated between the SBC legs. For example, if one would like to force Gain Control on the SBC session to use voice transcoding, even though both sides of the session have negotiated without SBC intervention (for example, coder extension).



Note: To implement transcoding, you must configure the number of required DSP channels for transcoding (for example, `MediaChannels = 120`). Each transcoding session uses two DSP resources.

The transcoding mode can be configured using the parameters `TranscodingMode` and `IPProfile`.

8.4.5.6 Coder Restrictions Control

The SBC Allowed Coders (Coders Restriction) feature determines the coders that can be used for a specific SBC leg. This feature provides greater control over bandwidth. This feature enforces the use of specific coders (*allowed coders groups*) while preventing the use of other coders (restricted). The Allowed Coders Groups are configured using the `AllowedCodersGroup` parameter. Coders excluded from the Allowed Coders Group list (restriction list) are removed from the SDP offer and therefore, only coders common between the SDP offered coders and Allowed Coders Group are used. In addition, the device can add coders (referred to as *Extension Coders*) to the SDP offer. This is done by configuring a Coders Group (using the `CodersGroup` parameter), and then selecting this group using the IP Profile's `SBCExtensionCodersGroupID` parameter.

This feature also allows the definition of a coders preference policy for the SDP offered coders. Coders Preference is done on both legs on the original SDP offer (without the extended coders), and the offered side selects its chosen coders from the suggested coders list. Coders listed higher up in the Allowed Coders Group take preference over ones listed lower down in the group.

To configure whether you want to enable only the Allowed Coders list feature, only the Allowed Coders Preference feature, or both, use the IP Profile parameter, SBCAllowedCodersMode.


Notes:

- For a list of supported coders, refer to the *ini* file parameter table CodersGroup.
- If Allowed Coders Groups are configured, unknown coders are blocked by the device.
- Allowed Coders Groups are applicable only to audio media.
- Allowed Coders Groups can be assigned to IP Profiles (using the IPProfile parameter).
- For configuring Allowed Coders Groups (and Extension Coders Groups), use the parameter AllowedCodersGroup.

The Allowed Coders process is as follows:

- a. The device receives an incoming SIP message with SDP (offer) and checks the offered coders.
- b. The source (first) leg may have Allowed Coders (i.e. list of coders that can be used - enforced).
- c. The device checks for common coders between the SDP offered coders and the Allowed Coders Group list.

For example, assume the following:

- The SDP coder offer includes the following coders: G729, G711, and G723.
- The source (first) leg includes the following Allowed Coders: G711 and G729.

The device selects the common coders, i.e., G711 and G729 (with changed preferred coder priority - highest for G711). In other words, it removes the coders that are not in the Allowed Coders list and the order of priority is first according to the Allowed Coders list.

Now assume that the destination (second) leg also includes Allowed Coders and/or extensions. Therefore, the device performs the Allowed Coders procedure (common coders) between the updated coder list and the destination leg's Allowed Coders list (Coders Extension procedure is performed before Allowed Coders). Adding to the example, assume the following:

- For the first leg, the device selects the common coders G711 and G729 (explained in the example above).
- Assume that the second leg includes the Extended coder G726.
- Assume that the second leg includes the following Allowed Coders: G723, G726, and G729.

As a result, the device selects the common coders, i.e., G729 and G726 (coder priority did not change Extended coder order).

If the Allowed Coders policy on SDP returns an empty coders list, the device (source leg) rejects the call (SIP 488 or ACK and BYE). If both Coders Extension and Allowed Coders policies on SDP (in this order) returns an empty coders list, the second leg rejects the call (SIP 488, or ACK and BYE).

Below is an example, assuming that Allowed Coders list (ordered) includes G711A-law (PCMA), G729, and G711U-law (PCMU), and Extended Coder is G729.

1. SDP offer - original offer:

```
m=audio 6050 RTP/AVP 0 8 4 96
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:4 G723/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
a=sendrecv
```

2. SDP offer - after manipulation:

```
m=audio 6010 RTP/AVP 8 0 96 18
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
a=sendrecv
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
```

In the SDP, the "m=audio 6010 RTP/AVP 8 0 96 18" line shows that the coder priority has changed - G711A-law ("8") and then G711U-law ("0") - and that the extended coder G729 ("18") has been added. The G723 coder ("4") in the original offer was removed as it was not defined in the Allowed Coders list (i.e., a restricted coder).

8.4.5.7 SRTP-RTP Transcoding

The device supports transcoding between SRTP and RTP. The device can also enforce SBC legs to use SRTP\RTP, using the IP Profile parameter SBCMediaSecurityBehaviour:

- As is (default): no special handling for RTP\SRTP is done.
- SRTP: SBC legs negotiate only SRTP media lines, and RTP media lines are removed from the incoming SDP offer\answer.
- RTP: SBC legs negotiate only RTP media lines, and SRTP media lines are removed from the incoming offer\answer.
- Both: each offer\answer is extended (if not already) to two media lines - one RTP and the other SRTP.

If two SBC legs (after offer/answer negotiation) use different security types (i.e., one RTP and the other SRTP), then the device performs RTP-SRTP transcoding.

To transcode between RTP and SRTP, the following prerequisites must be met:

- At least one supported SDP "crypto" attribute and parameters
- EnableMediaSecurity must be set to 1

If one of the above transcoding prerequisites is not met:

- Any value other than "As is" is discarded.
- If the incoming offer is SRTP, force transcoding, coder transcoding, and DTMF extensions are not applied.

Transcoding between RTP and SRTP does not require any DSP allocation. SRTP to SRTP does not require DSP allocation.

8.4.5.8 Multiple RTP Media Streams per Call Session

The device's SBC application supports multiple RTP media streams per SBC call session. Up to five different media types can be included in a session:

- Audio (m=audio)
- Video (m=video)
- Text (m=text)
- Fax (m=image)

Therefore, the device can provide transcoding of various attributes in the SDP offer/answer (e.g., codec, port, and packetization time) per media type. If the device is unable to perform transcoding (for example, does not support the codec), it relays the SBC dialog transparently.

8.4.6 SIP Dialog Admission Control

The device allows you to limit the number of concurrent calls (SIP dialogs). These call limits can be applied per SRD and/or IP Group, and per user (identified by its registered contact). This is especially important for MSBG applications where VoIP and Data traffic contend on the WAN throughput, which may be limited by itself. For example, DSL WAN access interface is very limited in the uplink. Therefore, by controlling the number of calls allowed, bandwidth can be reserved for Data applications. In addition, this feature can be useful for implementing Service Level Agreements (SLA) policies.

The SIP dialog limits can be defined per SIP request type and direction (inbound or outbound). These relate to requests that initiate SIP dialogs and not the subsequent requests that can be of different type and direction. The SIP dialog-initiating request types can include SIP INVITEs, REGISTER, and/or SUBSCRIBE, or it can be configured to include all dialogs. Requests that supersede the defined limit are rejected with a SIP 486 "Busy Here" response.

SIP-dialog rate control can also be configured using the "token bucket" mechanism. The token bucket is a control mechanism that dictates the rate of SIP-dialog setups based on the presence of tokens in the bucket – a logical container that holds aggregate SIP dialogs to be accepted or transmitted. Tokens in the bucket are removed ("cached in") for the ability to setup a dialog. Therefore, a flow can set up dialogs up to its peak burst rate if there are adequate tokens in the bucket and if the burst threshold is configured appropriately:

- Every SIP dialog setup request must attempt to take a token from the bucket.

- If there are no tokens, the request is dropped.
- New tokens are added to the bucket at a user-defined rate (token rate).
- If the bucket contains the maximum number of tokens, tokens to be added at that moment are dropped.

A token bucket is configured using the following new parameters:

- Rate = Rate at which tokens are added to the bucket (i.e., token rate). One token is added to the bucket every 1000/Rate milliseconds. The rate of dialog setups per second, or unlimited if set to 0 (default).
- Max Burst = Maximum tokens that can fill the bucket. At any given time, the bucket cannot contain more than this amount of tokens. The maximum burst size for the dialog setup rate, unlimited if set to 0 (default).

Dropped requests are replied with the 486 "Busy Here" SIP response. Dropped requests are not counted in the bucket.

The SIP dialog limits are defined in the Admission Control table (SBCAdmissionControl).

8.4.7 Handling SIP 3xx Redirect Responses

By default, the device's handling of SIP 3xx responses is to send the Contact header unchanged. However, some network setups require that the new INVITE message sent as a result of the 3xx traverse the device. This is enabled by the parameter SBC3xxBehavior.

Reasons for enforcing resultant INVITEs to traverse the SBC may vary:

- The user that receives the 3xx can't route to the 3xx contact (i.e., the user is on the LAN and the new contact is on the WAN). In such a scenario, the device helps the user reach the WAN contact and overcome NAT problems.
- Enforce certain SBC policies (e.g., call admission control, header manipulation, and transcoding) on the resultant INVITE.

The device enforces this by modifying each Contact in the 3xx response as follows:

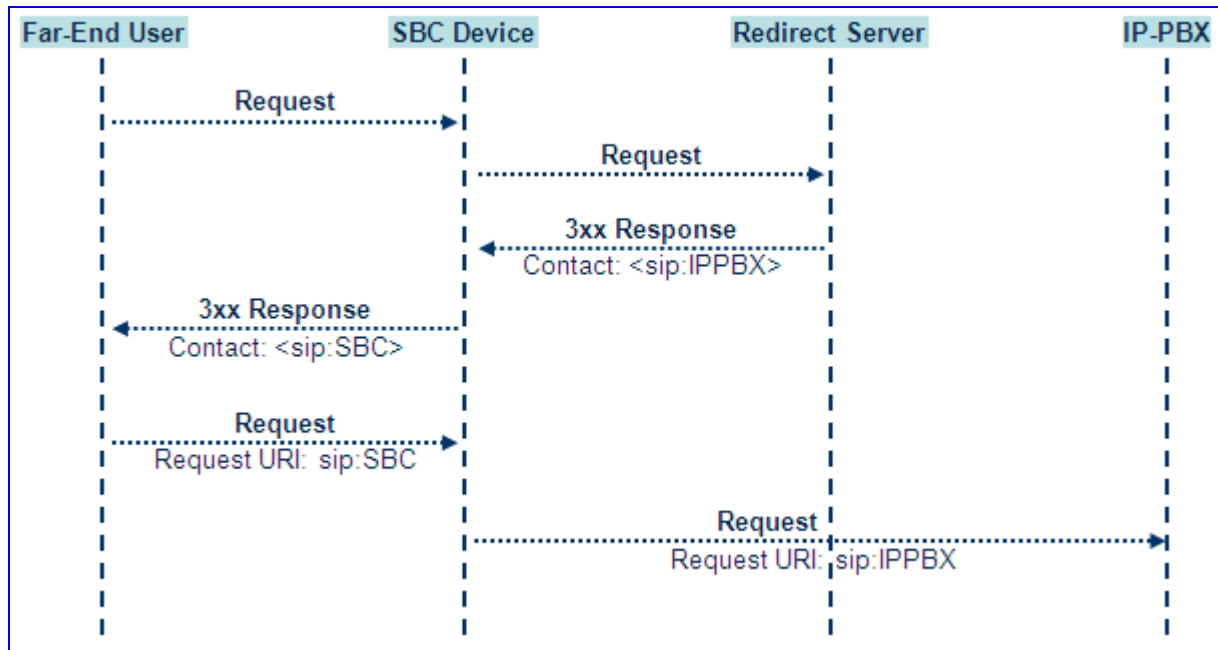
- Changes the host part to the device's IP address – this change causes the remote user agent to send the INVITE to the device.
- Adds a special prefix ("T~&R_") to the Contact user part – to identify the new INVITE as a 3xx resultant INVITE.

The SBC handling for the 3xx resultant INVITE is as follows:

1. The incoming INVITE is identified as a 3xx resultant INVITE according to the special prefix.
2. The device automatically replaces the SBC host part (in the Request-URI) with the host from the 3xx Contact.
3. The prefix ("T~&R_") remains in the user part for the classification, manipulation, and routing mechanisms.
4. The classification, manipulation, and routing processes are done exactly like any other INVITE handling. The special prefix can be used for specific routing rules for 3xx resultant INVITEs.

5. The prefix is removed before the resultant INVITE is sent to the destination.

Figure 8-57: SIP 3xx Response Handling



The process of this feature is described using an example:

1. The device receives the Redirect server's SIP 3xx response (e.g., Contact: <sip:User@IPPBX:5060;transport=tcp;param=a>;q=0.5).
2. The device replaces the Contact header value with the special prefix and database key value as user part, and with the device's URL as host part (e.g., Contact: <sip:Prefix_Key_User@SBC:5070;transport=udp>;q=0.5).
3. The device sends this manipulated SIP 3xx response to the Far-End User (FEU).
4. The FEU sends a new request with the Request-URI set to the value of the received 3xx response's Contact header (e.g., RequestURI: sip:Prefix_Key_User@SBC:5070;transport=udp).
5. Upon receipt of the new request from the FEU, the device replaces the Request-URI with the new destination address (e.g., RequestURI: sip:Prefix_User@IPPBX:5070;transport=tcp;param=a).
6. The device removes the user prefix from the Request-URI, and then sends this Request-URI to the new destination (e.g., RequestURI: sip:User@IPPBX:5070;transport=tcp;param=a).

8.4.8 Interworking SIP Diversion and History-Info Headers

This device can be configured to interwork between the SIP Diversion and History-Info headers. This is important, for example, to networks that support the Diversion header but not the History-Info header, or vice versa. Therefore, mapping between these headers is crucial for preserving the information in the SIP dialog regarding how and why (e.g., call redirection) the call arrived at a certain SIP UA.

This feature is configured in the IP Profile table (IPProfile parameter) using the following new parameters:

- SBCTDiversionMode - defines the device's handling of the Diversion header
- SBCHistoryInfoMode - defines the device's handling of the History-Info header

The handling of the SIP Diversion and History-Info headers is described in the table below:

Table 8-6: Handling of SIP Diversion and History-Info Headers

Parameter Value	SIP Header Present in Received SIP Message		
	Diversion	History-Info	Diversion and History-Info
HistoryInfoMode = Add DiversionMode = Remove	Diversion converted to History-Info. Diversion removed.	Not present	Diversion removed.
HistoryInfoMode = Remove DiversionMode = Add	Not present.	History-Info converted to Diversion. History-Info removed.	History-Info added to Diversion. History-Info removed.
HistoryInfoMode = Disable DiversionMode = Add	Diversion converted to History-Info.	Not present.	Diversion added to History-Info.
HistoryInfoMode = Disable DiversionMode = Add	Not present.	History-Info converted to Diversion.	History-Info added to Diversion.
HistoryInfoMode = Add DiversionMode = Add	Diversion converted to History-Info.	History-Info converted to Diversion.	Headers are synced and sent.
HistoryInfoMode = Remove DiversionMode = Remove	Diversion removed.	History-Info removed.	Both removed.

8.4.9 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 "Configuring Message Manipulations" on page 206.

8.4.9.1 Actions

The table below lists the actions that can be performed on SIP message manipulation in the Message Manipulations table.

Table 8-7: 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.

8.4.9.2 Supported Header Types

8.4.9.2.1 Accept

An example of the header is shown below:

Accept: application/sdp

The header properties as 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:	<p>If the supported header does not contain 'mm,100rel,timer,replaces', then in all INVITE messages add an Accept header:</p> <pre>MessageManipulations 8 = 1, invite, "header.supported != 'mm,100rel,timer,replaces'", header.accept, 0, ' application/x-private ', 0;</pre>
Result:	Accept: application/x-private

8.4.9.2.2 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 as 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: MessageManipulations 0 = 1, invite, , header.accept-language, 0, "en, il, cz, it", 0;
Result:	Accept-Language: en, il, cz, it

8.4.9.2.3 Allow

An example of the header is shown below:

Allow:
REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE

The header properties as 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: MessageManipulations 0 = 1, invite, , header.allow, 0, "'REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, XMESSAGE'", 0;
Result:	Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, XMESSAGE

8.4.9.2.4 Call-Id

An example of the header is shown below:

Call-ID: JN1YXOLCAIWTRHWOINNRR@10.132.10.128

The header properties as 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: MessageManipulations 0 = 1, invite, , header.Xitsp-abc, 0, "header.call-id", 0;
Result:	Xitsp-abc: GIAPOFWRBQKJVAETIODI@10.132.10.128

8.4.9.2.5 Contact

An example of the header is shown below:

Contact: <sip:555@10.132.10.128:5080>

The header properties as 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 530	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: MessageManipulations 0 = 1, Invite, ,header.contact.url.user, 2, "fred", 0;
Result:	Contact: <sip:fred@10.132.10.128:5070>

8.4.9.2.6 Cseq

An example of the header is shown below:

CSeq: 1 INVITE

The header properties as 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. MessageManipulations 0 = 1, Invite, "header.cseq.num=='1'",header.contact.url.user, 2, "'fred'", 0;
Result:	Contact: <sip:fred@10.132.10.128:5070>

8.4.9.2.7 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 as 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 533)	Read/Write
Reason	Enum Reason (see "Reason (Diversion)" on page 533)	Read/Write
Screen	Enum Screen (see "Screen" on page 536)	Read/Write
URL	URL Structure (see "URL" on page 530)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Diversion header to all INVITE messages: <code>MessageManipulations 0 = 1, invite, , header.Diversion, 0, " '<tel:+101>;reason=unknown; counter=1;screen=no; privacy=off'", 0;</code>
	Result:	<code>Diversion: <tel:+101>;reason=user- busy;screen=no;privacy=off;counter=1</code>
Example 2	Rule:	Modify the Reason parameter in the header to 1, see "Reason (Diversion)" on page 533 for possible values: <code>MessageManipulations 1 = 1, invite, , header.Diversion.reason, 2, '1', 0;</code>
	Result:	<code>Diversion: <tel:+101>;reason=user- busy;screen=no;privacy=off;counter=1</code>
Example 3	Rule:	The URL in the Diversion header is modified to that which is contained in the header URL: <code>MessageManipulations 2 = 1, invite, , header.Diversion.URL, 2, "header.from.url", 0;</code>
	Result:	<code>Diversion:<sip:555@IPG2Host;user=phone>;reason=user- busy;screen=no;privacy=off;counter=1</code>

8.4.9.2.8 Event

An example of the header is shown below:

Event: foo; id=1234

The header properties as 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 529)	Read/Write
Param	Param	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add parameter itsp-abc=voip to the Event header: <code>MessageManipulations 0 = 1, invite, , header.event.param.itsp-abc, 0, "'voip'" , 0;</code>
	Result:	<code>Event: foo;id=1234;itsp-abc=voip</code>
Example 2	Rule:	Modify the Event ID string: <code>MessageManipulations 1 = 1, invite, , header.event.EVENTKEY.id, 2, "'5678'", 0;</code>
	Result:	<code>Event: foo;id=5678;</code>
Example 3	Rule:	Modify the Event package enum: <code>MessageManipulations 2 = 1, invite, ,</code>

		<code>header.event.EVENTKEY.EVENTPACKAGE, 2, "'2'", 0;</code>
	Result:	<code>Event: refer;id=5678</code>

8.4.9.2.9 From

An example of the header is shown below:

From: <sip:555@10.132.10.128;user=phone>;tag=YQLQHCAAYBWKKRVIMWEQ

The header properties as 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 530)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Change the user part of the From header if the user is not 654: <code>MessageManipulations 8 = 1, invite, "header.from.url.user != '654'", header.from.url.user, 2, 'fred', 0;</code>
	Result:	<code>From: <sip:fred@IPG2Host;user=phone>;tag=1c20161</code>
Example 2	Rule:	Add a new parameter to the From header called p1 and set its value to myParameter: <code>MessageManipulations 1 = 1, Invite.request, ,header.from.param.p1, 0, "'myParameter'", 0;</code>
	Result:	<code>From: <sip:fred@IPG2Host;user=phone>;p1=myParameter;tag=1c589 1</code>
Example 3	Rule:	Modify the URL in the From header: <code>MessageManipulations 0 = 1, any, , header.from.url, 2, 'sip:3200@110.18.5.41;tusunami=0', 0;</code>
	Result:	<code>From: <sip:3200@110.18.5.41;user=phone;tusunami=0>;tag=1c2375 0</code>

8.4.9.2.10 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 as 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: MessageManipulations 0 = 1, any, , header.History-Info, 0, '<sip:UserA@audc.mydomain.com;index=3>', 0
	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: MessageManipulations 0 = 1, any, , header.History-Info.1, 1, , 0;
	Result:	History-Info: <sip:UserA@ims.example.com;index=1>
Example 3	Rule:	Delete all History-Info from the message: MessageManipulations 0 = 1, any, , header.History-Info, 1, , 0;
	Result:	All history-info headers are removed.

8.4.9.2.11 Min-Se and Min-Expires

An example of the header is shown below:

Min-SE: 3600

Min-Expires: 60

The header properties as 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: <code>MessageManipulations 1 = 1, any, , header.min-se, 0, '50', 0;</code>
	Result:	Min-SE: 50
Example 2	Rule:	Modify a Min-Expires header with the min-expires value and add an additional 0: <code>MessageManipulations 0 = 1, Invite, , header.Min-Expires.param, 2, "header.Min-Expires.time + '0'", 0;</code>
	Result:	Min-Expires: 340;3400
Example 3	Rule:	Modify a Min-Expires header changing the time to 700: <code>MessageManipulations 0 = 1, Invite, , header.Min-Expires.time, 2, "'700'", 0;</code>
	Result:	Min-Expires: 700

8.4.9.2.12P-Asserted-Identity

An example of the header is shown below:

P-Asserted-Identity: Jane Doe <sip:567@itsp.com>

The header properties as 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 530)	Read/Write
Name	String	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a P-Asserted-Id header to all INVITE messages: <code>MessageManipulations 2 = 1, invite, , header.p-asserted-identity, 0, "'<sip:567@itsp.com>'", 0;</code>
	Result:	P-Asserted-Identity: <sip:567@itsp.com>
Example 2	Rule:	Modify the P-Asserted-Identity host name to be the same as the host name in the To header: <code>MessageManipulations 2 = 1, invite, , header.p-asserted-identity.URL.host, 2, header.to.url.host, 0;</code>
	Result:	P-Asserted-Identity: <sip:567@10.132.10.128>

8.4.9.2.13P-Associated-Uri

An example of the header is shown below:

P-Associated-URI: <sip:12345678@itsp.com>

The header properties as 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 530)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a P-Associated-Uri header to all INVITE response messages: MessageManipulations 5 = 1, register.response, ,header.P-Associated-URI, 0, '<sip:admin@10.132.10.108>', 0;
	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': MessageManipulations 5 = 1, register.response, ,header.P-Associated-URI.url.user, 2, 'alice', 0;
	Result:	P-Associated-URI:<sip:alice@10.132.10.108>

8.4.9.2.14P-Called-Party-Id

An example of the header is shown below:

P-Called-Party-ID: <sip:2000@gw.itsp.com>

The header properties as 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 530)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a P-Called-Party-Id header to all messages: MessageManipulations 8 = 1, any, , header.p-called-party-id, 0, 'sip:2000@MSBG.ITSP.COM', 0;
------------------	--------------	---

	Result:	P-Called-Party-ID: <sip:2000@gw.itsp.com>
Example 2	Rule:	Append a parameter (p1) to all P-Called-Party-Id headers: MessageManipulations 9 = 1, invite, , header.p-called-party-id.param.p1, 0, 'red', 0;
	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: MessageManipulations 3 = 1, any, , header.p-called-party-id.name, 2, 'Secretary', 0;
	Result:	P-Called-Party-ID: Secretary <sip:2000@gw.itsp.com>;p1=red

8.4.9.2.15P-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 as 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: MessageManipulations 1 = 1, any, , header.P-Charging-Vector, 0, "'icid-value=1234bc9876e; icid-generated-at=192.0.6.8; orig-ioi=home1.net'", 0;
Result:	P-Charging-Vector: icid-value=1234bc9876e; icid-generated-at=192.0.6.8; orig-ioi=home1.net

8.4.9.2.16P-Preferred-Identity

An example of the header is shown below:

P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@abc.com>

The header properties as 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 530)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a P-Preferred-Identity header to all messages: MessageManipulations 1 = 1, any, , header.P-Preferred-Identity, 0, "'Cullen Jennings <sip:fluffy@abc.com>'", 0;
	Result:	P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@abc.com>
Example 2	Rule:	Modify the display name in the P-Preferred-Identity header: MessageManipulations 2 = 1, any, , header.P-Preferred-Identity.name, 2, "'Alice Biloxi'", 0;
	Result:	P-Preferred-Identity: "Alice Biloxi" <sip:fluffy@abc.com>

8.4.9.2.17 Privacy

An example of the header is shown below:

Privacy: none

The header properties as 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 Privacy header and set it to 'id': MessageManipulations 1 = 1, any, , header.Privacy, 0, "'id'", 0;
	Result:	Privacy: id
Example 2	Rule:	If the Privacy header contains id, then add user to the header: MessageManipulations 3 = 1, any, header.privacy contains 'id', header.privacy, 2, 'user', 0;
	Result:	Privacy: id;user

8.4.9.2.18 Proxy-Require

An example of the header is shown below:

Proxy-Require: sec-agree

The header properties as 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:	Add a Proxy-Require header to the message: <code>MessageManipulations 1 = 1, any, , header.Proxy-Require, 0, "'sec-agree'", 0;</code>
	Result:	Proxy-Require: sec-agree
Example 2	Rule:	Modify the Proxy-Require header to itsip.com: <code>MessageManipulations 2 = 1, any, , header.Proxy-Require, 2, "itsip.com'", 0;</code>
	Result:	Proxy-Require: itsip.com

8.4.9.2.19Reason

An example of the header is shown below:

Reason: SIP ;cause=200 ;text="Call completed elsewhere"

The header properties as 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 529)	Read/Write
Reason	Reason Structure (see "Reason Structure" on page 530)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Reason header: <code>MessageManipulations 0 = 1, any, ,header.reason, 0, "'SIP;cause=200;text='Call completed elsewhere'", 0;</code>
	Result:	Reason: SIP ;cause=200 ;text="Call completed elsewhere"
Example 2	Rule:	Modify the reason cause number: <code>MessageManipulations 0 = 1, any, ,header.reason.reason.cause, 0, '200', 0;</code>
	Result:	Reason: Q.850 ;cause=180 ;text="Call completed elsewhere"
Example 3	Rule:	Modify the cause number: <code>MessageManipulations 0 = 1, any, ,header.reason.reason.reason, 0, '483', 0;</code>
	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.

8.4.9.2.20 Referred-By

An example of the header is shown below:

Referred-By: <sip:referrer@referrer.example>;

The header properties as 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 530)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Referred-By header: MessageManipulations 0 = 1, any, ,header.Referred-By, 0, "'<sip:refer@refer.com>' ", 0;
	Result:	Referred-By: <sip: sip:refer@refer.com>
Example 2	Rule:	Modify the host: MessageManipulations 0 = 1, any, ,header.Referred-By.url.host, 0, "'yahoo.com'", 0;
	Result:	Referred-By: <sip:refer@yahoo.com>
Example 3	Rule:	Add a new parameter to the header: MessageManipulations 0 = 1, any, ,header.Referred-By.param.p1, 0, "'fxs'", 0
	Result:	Referred-By: <sip:referrer@yahoo.com>;p1=fxs

8.4.9.2.21 Refer-To

An example of the header is shown below:

Refer-To: sip:conference1@example.com

Refer-To:

<sips:a8342043f@atlanta.example.com?Replaces=12345601%40atlanta.example.com%3bfrom-tag%3d314159%3bto-tag%3d1234567>

The header properties as 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: MessageManipulations 0 = 1, any, ,header.Refer-to, 0, "'<sip:referto@referto.com>' ", 0;
	Result:	Refer-To: <sip:referto@referto.com>
Example 2	Rule:	Add a Refer-To header with URI headers: 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;
	Result:	Refer-To: <sips:a8342043f@atlanta.example.com?Replaces=12345601%40atlanta.example.com%3bfrom-tag%3d314159%3bto-tag%3d1234567>

8.4.9.2.22 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 as 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 532)	Read/Write
NumberType	Enum Number Type (see "NumberType" on page 532)	Read/Write
Param	Param	Read/Write
Privacy	Enum Privacy (see "Privacy" on page 533)	Read/Write
Reason	Enum Reason (RPI) (see "Reason (Remote-Party-Id)" on page 535)	Read/Write
Screen	Enum Screen (see "Screen" on page 536)	Read/Write
ScreenInd	Enum ScreenInd (see "ScreenInd" on page 536)	Read/Write
URL	URL Structure (see "URL" on page 530)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Remote-Party-Id header to the message: MessageManipulations 0 = 1, invite, ,header.REMOTE-PARTY-ID, 0, "'<sip:999@10.132.10.108>;party=calling'", 0;
	Result:	Remote-Party-ID: <sip:999@10.132.10.108>;party=calling;npi=0;ton=0
Example 2	Rule:	Create a Remote-Party-Id header using the url in the From header using the + operator to concatenate strings: MessageManipulations 0 = 1, Invite, ,header.REMOTE-PARTY-ID, 0, "'<' + header.from.url + '>' + ' ;party=calling'", 0;
	Result:	Remote-Party-ID: <sip:555@10.132.10.128;user=phone>;party=calling;npi=0;ton=0
Example 3	Rule:	Modify the number plan to 1 (ISDN): MessageManipulations 1 = 1, invite, , header.Remote-Party-ID.numberplan, 2, '1', 0;
	Result:	Remote-Party-ID: <sip:555@10.132.10.128;user=phone>;party=calling;npi=1;ton=0
Example 4	Rule:	Modify the Remote-Party-Id header to set the privacy parameter to 1 (Full): MessageManipulations 1 = 1, invite, , header.Remote-Party-ID.privacy, 2, '1', 0;
	Result:	Remote-Party-ID: <sip:555@10.132.10.128;user=phone>;party=calling;privacy=full;npi=0;ton=0

8.4.9.2.23 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 as 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 530)	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

8.4.9.2.24Require

An example of the header is shown below:

Require: 100rel

The header properties as 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 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.

8.4.9.2.25 Resource-Priority

An example of the header is shown below:

Resource-Priority: wps.3

The header properties as 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

8.4.9.2.26 Retry-After

An example of the header is shown below:

Retry-After: 18000

The header properties as 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: MessageManipulations 2 = 1, Invite, ,header.Retry-After, 0, "'3600'", 0;
	Result:	Retry-After: 3600
Example 2	Rule:	Modify the Retry-Time in the header to 1800: MessageManipulations 3 = 1, Invite, ,header.Retry-After.time, 2, "'1800'", 0;
	Result:	Retry-After: 1800

8.4.9.2.27 Server or User-Agent

An example of the header is shown below:

User-Agent: Sip Message Generator V1.0.0.5

The header properties as 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: MessageManipulations 2 = 1, Invite, ,header.user-agent, 1, "", 0;
	Result:	The header is removed.
Example 2	Rule:	Change the user agent name in the header: MessageManipulations 3 = 1, Invite, ,header.user-agent, 2, "itsp analogue gateway", 0;
	Result:	User-Agent: itsp analog gateway

8.4.9.2.28Service-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 as 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: 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;
	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: MessageManipulations 3 = 1, Invite, ,header.service-route.1.serviceroute, 2, "<sip:itsp.com;lr>", 0;
	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>

8.4.9.2.29 Session-Expires

An example of the header is shown below:

Session-Expires: 480

The header properties as 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 536)	Read/Write
Time	Integer	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Session-Expires header: <code>MessageManipulations 0 = 1, any, , header.Session-Expires, 0, "'48' + '0'", 0;</code>
	Result:	Session-Expires: 480
Example 2	Rule:	Modify the Session-Expires header to 300: <code>MessageManipulations 1 = 1, any, , header.Session-Expires.time, 2, "'300'", 0;</code>
	Result:	Session-Expires: 300
Example 3	Rule:	Add a param called longtimer to the header: <code>MessageManipulations 1 = 1, any, , header.Session-Expires.param.longtimer, 0, "'5'", 0;</code>
	Result:	Session-Expires: 480;longtimer=5
Example 4	Rule:	Set the refresher to 1 (UAC): <code>MessageManipulations 3 = 1, any, , header.session-expires.refresher, 2, '1', 0;</code>
	Result:	Session-Expires: 300;refresher=uac;longtimer=5

8.4.9.2.30 Subject

An example of the header is shown below:

Subject: A tornado is heading our way!

The header properties as 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!

8.4.9.2.31 Supported

An example of the header is shown below:

Supported: early-session

The header properties as 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 is a header manipulation example:

Rule:	Add a Supported header: <pre>MessageManipulations 1 = 1, Invite, ,header.supported, 0, "early-session", 0;</pre>
Result:	Supported: early-session

8.4.9.2.32 To

An example of the header is shown below:

To: <sip:101@10.132.10.128;user=phone>

The header properties as 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 530)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Set the user phone Boolean to be false in the To header's URL: <code>MessageManipulations 4 = 1, invite.request, , header.to.url.UserPhone, 2, '0', 0;</code>
	Result:	To: <sip:101@10.132.10.128>
Example 2	Rule:	Change the URL in the To header: <code>MessageManipulations 4 = 1, invite.request, , header.to.url.UserPhone, 2, '0', 0;</code>
	Result:	To: <sip:101@10.20.30.60:65100>
Example 3	Rule:	Set the display name to 'Bob': <code>MessageManipulations 5 = 1, invite.request, , header.to.name, 2, "'Bob'", 0;</code>
	Result:	To: "Bob Dylan" sip:101@10.20.30.60:65100
Example 4	Rule:	Add a proprietary parameter to all To headers: <code>MessageManipulations 6 = 1, invite.request, , header.to.param.artist, 0, "'singer'", 0;</code>
	Result:	To: "Bob Dylan" <sip:101@10.20.30.60:65100>;artist=singer

8.4.9.2.33 Unsupported

An example of the header is shown below:

Unsupported: 100rel

The header properties as 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:	Add an Unsupported header to the message: <code>MessageManipulations 0 = 1, Invite.response, ,header.unsupported, 0, "'early-session, myUnsupportedHeader'", 0;</code>
	Result:	Unsupported: early-session
Example 2	Rule:	Modify the Unsupported header to 'replaces': <code>MessageManipulations 1 = 1, Invite, ,header.unsupported, 2, "'replaces'", 0;</code>
	Result:	Unsupported: replaces

8.4.9.2.34Via

An example of the header is shown below:

Via: SIP/2.0/UDP 10.132.10.128;branch=z9hG4bKUGOKMQPAVFKTAVYDQPTB

The header properties as 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 529)	Read Only
MAddrIp	gnTIPAddress	Read Only
Param	Param	Read/Write
Port	Integer	Read Only
TransportType	Enum TransportType (see "TransportType" on page 537)	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

8.4.9.2.35Warning

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 as 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: <code>MessageManipulations 0 = 1, Invite.response.180, ,header.warning, 0, "'Incompatible 380'", 0;</code>
Result:	Warning: Incompatible 380

8.4.9.2.36 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 as 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: <code>MessageManipulations 0 = 1, , , header.myExp, 0, "'scooby, doo, goo, foo'", 0;</code>
	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: <code>MessageManipulations 0 = 1, any, , header.media, 0, "header.Session-Expires.time + '000' + ';refresher=' + header.Session-Expires.Refresher", 0;</code>
	Result:	MEDIA: 3600000;refresher=1
Example 3	Rule:	Create lists of Unknown headers: <code>MessageManipulations 1 = 1, Invite, , header.myExp.1, 0, "'scooby, doo, goo, foo1'", 0;</code> <code>MessageManipulations 2 = 1, Invite, , header.myExp.2, 0, "'scooby, doo, goo, foo2'", 0;</code>
	Result:	MYEXP: scooby, doo, goo, foo1 MYEXP: scooby, doo, goo, foo2
Example 4	Rule:	Remove the SIP header 'colour' from INVITE messages: <code>MessageManipulations 1 = 1, Invite, , header.colour, 1, "", 0;</code>
	Result:	The colour header is removed.

8.4.9.3 Structure Definitions

8.4.9.3.1 Event Structure

The Event structure is used in the Event header (see "Event" on page 510).

Table 8-8: Event Structure

Keyword	Sub Types	Attributes
EventPackage	Enum Event Package (see "Event Package" on page 531)	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 531).

8.4.9.3.2 Host

The host structure is applicable to the URL structure (see "URL" on page 530) and the Via header (see "Via" on page 527).

Table 8-9: Host Structure

Keyword	Sub Types
Port	Short
Name	String

8.4.9.3.3 MLPP

This structure is applicable to the Reason header (see "Reason" on page 517).

Table 8-10: MLPP Structure

Keyword	Sub Types
Type	Enum MLPP Reason (see "MLPP Reason Type" on page 532)
Cause	Int

8.4.9.3.4 Reason Structure

This structure is applicable to the Reason header (see "Reason" on page 517).

Table 8-11: Reason Structure

Keyword	Sub Types
Reason	Enum Reason (see "Reason (Reason Structure)" on page 533)
Cause	Int
Text	String

8.4.9.3.5 URL

This structure is applicable to the following headers:

- Contact (see Contact)
- Diversion (see Diversion)
- From (see From)
- P-Asserted-Identity (see P-Asserted-Identity)
- P-Associated-Uri (see "P-Associated-Uri" on page 514)
- P-Called-Party-Id (see P-Called-Party-Id)
- P-Preferred-Identity (see P-Preferred-Identity)
- Referred-By (see "Referred-By" on page 518)
- Refer-To (see Refer-To)
- Remote-Party-Id (see Remote-Party-Id)
- Request-Uri (see "Request-Uri" on page 520)
- To (see To)

Table 8-12: URL Structure

Keyword	Sub Types
Type	Enum Type (see "Type" on page 537)
Host	Host Structure (see "Host" on page 529)
MHost	Structure
UserPhone	Boolean
LooseRoute	Boolean
User	String
TransportType	Enum Transport (see "TransportType" on page 537)
Param	Param

8.4.9.4 Enum Definitions

8.4.9.4.1 AgentRole

These ENUMs are applicable to the Server or User-Agent headers (see "Server or User-Agent" on page 522).

Table 8-13: Enum Agent Role

AgentRole	Value
Client	1
Server	2

8.4.9.4.2 Event Package

These ENUMs are applicable to the Server or User-Agent (see "Server or User-Agent" on page 522) and Event (see "Event" on page 510) headers.

Table 8-14: 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

8.4.9.4.3 MLPP Reason Type

These ENUMs are applicable to the MLPP Structure (see "MLPP" on page 529).

Table 8-15: Enum MLPP Reason Type

Type	Value
PreEmption Reason	0
MLPP Reason	1

8.4.9.4.4 Number Plan

These ENUMs are applicable to the Remote-Party-Id header (see Remote-Party-Id).

Table 8-16: Enum Number Plan

Plan	Value
ISDN	1
Data	3
Telex	4
National	8
Private	9
Reserved	15

8.4.9.4.5 NumberType

These ENUMs are applicable to the Remote-Party-Id header (see Remote-Party-Id).

Table 8-17: 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

8.4.9.4.6 Privacy

These ENUMs are applicable to the Remote-Party-Id (see Remote-Party-Id) and Diversion (see Diversion) headers.

Table 8-18: Enum Privacy

Privacy Role	Value
Full	1
Off	2

8.4.9.4.7 Reason (Diversion)

These ENUMs are applicable to the Diversion header (see Diversion).

Table 8-19: Enum Reason

Reason	Value
Busy	1
No Answer	2
Unconditional	3
Deflection	4
Unavailable	5
No Reason	6
Out of service	7

8.4.9.4.8 Reason (Reason Structure)

These ENUMs are used in the Reason Structure (see "Reason Structure" on page 530).

Table 8-20: Enum Reason (Reason Structure)

Reason	Value
INVITE	5
REINVITE	6
BYE	7
OPTIONS	8
ACK	9
CANCEL	10
REGISTER	11
INFO	12
MESSAGE	13

Reason	Value
NOTIFY	14
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

Reason	Value
UNSUPPORTED_URI_SCHEME_416	416
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

8.4.9.4.9 Reason (Remote-Party-Id)

These ENUMs are applicable to the Remote-Party-Id header (see Remote-Party-Id).

Table 8-21: Enum Reason (RPI)

Reason	Value
Busy	1
Immediate	2
No Answer	3

8.4.9.4.10 Refresher

These ENUMs are used in the Session-Expires header (see Session-Expires).

Table 8-22: Enum Refresher

Refresher String	Value
UAC	1
UAS	2

8.4.9.4.11 Screen

These ENUMs are applicable to the Remote-Party-Id (see Remote-Party-Id) and Diversion (see Diversion) headers.

Table 8-23: Enum Screen

Screen	Value
Yes	1
No	2

8.4.9.4.12 ScreenInd

These ENUMs are applicable to the Remote-Party-Id header (see Remote-Party-Id).

Table 8-24: Enum ScreenInd

Screen	Value
User Provided	0
User Passed	1
User Failed	2
Network Provided	3

8.4.9.4.13 TransportType

These ENUMs are applicable to the URL Structure (see "URL" on page 530) and the Via header (see "Via" on page 527).

Table 8-25: Enum TransportType

TransportType	Value
UDP	0
TCP	1
TLS	2
SCTP	3

8.4.9.4.14 Type

These ENUMs are applicable to the URL Structure (see "URL" on page 530).

Table 8-26: Enum Type

Type	Value
SIP	1
Tel	2
Fax	3
SIPS	4

8.4.9.5 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
		">"	Integer	Returns true if value is greater than the value.
		">="	Integer	Returns true if value is greater than or equals to the value.
		"<"	Integer	Returns true if value is less than the value.
		"<="	Integer	Returns true if value is less than or equals to the value.
	Action	Modify	Integer	Sets the integer element to the value. A string value must be a representation of an integer.
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
Attribute		"!="	Boolean	Returns true if the Boolean element not equals to the value. Boolean – can be either "0" or "1".
		"Modify"	Boolean	Sets the Boolean element to the value. Boolean – can be either "0" or "1".
	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.
	Action	"!="	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.
		Modify	Integer *Attribute	Sets the attribute element to the value. An attribute element value must be of the same type of the attribute element.

8.4.9.6 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

Examples:

- header.from.user == 100
- header.contact.header-param.expires > 3600
- header.to.host contains "itsp"
- param.call.dst.user != 100

a. match-type

Description: comparison to be made

Syntax: ("==" / "!=" / ">" / "<" / ">=" / "<=" / "contains" / "exists")

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

3. 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")

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

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

4. 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)

5. 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 + ">"

8.4.10 SBC Configuration Example

This section provides basic SBC configuration examples.



Note: The examples described in this section are for reference only. Modifications to device configuration should be made to suite your networking environment.

8.4.10.1 General SBC Setup

This section provides a basic SBC configuration example scenario.



Notes:

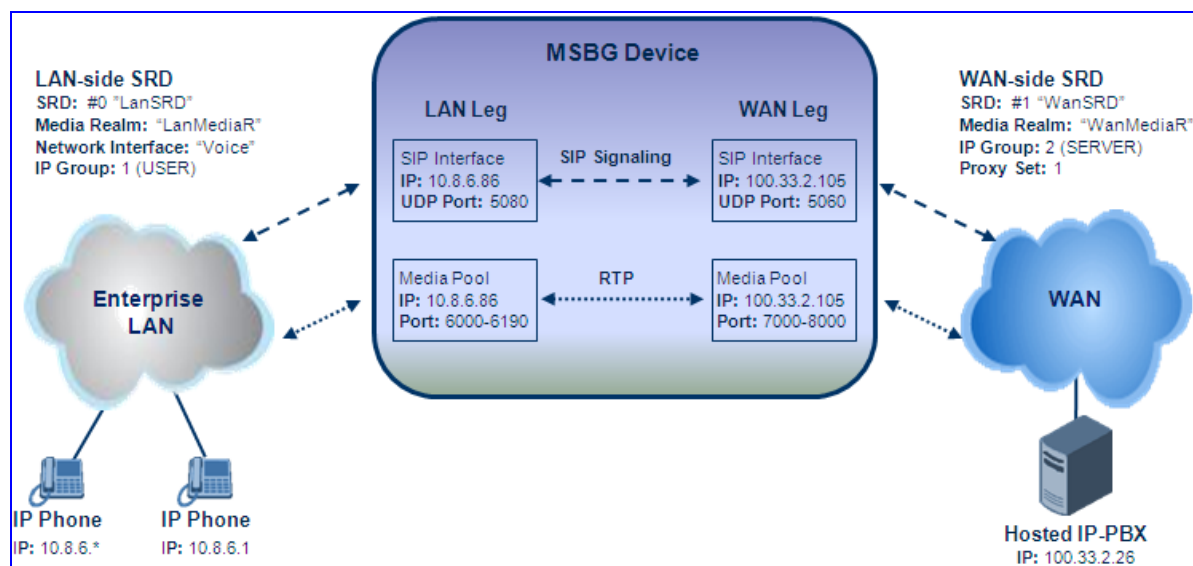
- Ensure that the device's installed Software Upgrade Key includes the "SBC" and "IPMediaChannels" (if transcoding is required) features. For viewing or installing the Software Upgrade Key, see "Loading Software Upgrade Key" on page 339.
- This example assumes that you have already configured the device's data-routing WAN IP address. For detailed information on configuring the WAN IP address, see "Assigning a WAN IP Address" on page 29.

This example assumes the following:

- The device is deployed at the enterprise, interfacing between the enterprise's LAN IP phones and WAN (using a hosted IP-PBX).
- LAN SIP signaling interface leg IP address is 10.8.6.86:5080. SIP phones are connected to this LAN and their registration is done by the device to the hosted IP-PBX (remote proxy).
- WAN SIP signaling leg interface IP address is 100.33.2.105:5060.
- Two IP Groups (i.e., two SIP User Agent entities):
 - IP Group 1 (USER): represents LAN user agents (e.g., IP phones) with IP address 10.8.6.1, 10.8.6.2 (i.e., 10.8.6.*).
 - IP Group 2 (SERVER): represents the WAN IP-PBX defined using a Proxy Set with IP address 100.33.2.26 (pertaining to the WAN SRD).
- Media (RTP) traffic (packets) sent from the LAN leg's UDP port 6000-6190 to the WAN leg's UDP port 7000-8000.
- WAN-LAN port forwarding for SIP and RTP is required for the above.

The figure below illustrates the example scenario setup:

Figure 8-58: SBC Example Scenario



8.4.10.1.1 Step 1: Configure LAN VoIP IP Address

The procedure below describes how to configure the VoIP LAN IP addresses (in our example, 10.8.6.86). This interface is for the OAMP, Media, and Control interface applications and is assigned the name "Voice".

➤ To configure the VoIP LAN IP address

1. Open the 'IP Settings' page, (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**).
2. Select the 'Index' corresponding to Application Type "**OAMP + Media + Control**" (i.e., VoIP and management interface), and then click **Edit**.
3. Configure the new IP address, prefix length, and default gateway so that it corresponds to your network IP scheme (e.g., 10.8.6.86).
4. Click **Apply** and then **Done** to apply and validate settings. If validation fails, the device does not reboot.

Figure 8-59: Multiple Interface Table

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	<input type="radio"/> OAMP + Media + Control	10.8.6.86	16	10.8.0.1	1	Voice

5. Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

8.4.10.1.2 Step 2: Assign VoIP Traffic to WAN Interface

Once you have defined the WAN IP address (see "Assigning a WAN IP Address" on page 29) for the data-routing interface, you then need to associate it with VoIP traffic (i.e., SIP signaling and media / RTP interfaces). The available WAN interfaces depend on the hardware configuration (i.e., Ethernet, T1, or SHDSL) and/or whether VLANs are defined for the WAN interface. If VLANs are defined, then you can select the WAN VLAN on which you want to run the SIP signaling and media interfaces. Once this association is set, VoIP traffic is sent on the WAN and incoming traffic is identified as coming from the WAN. The device also automatically configures the required port forwarding and static NAT rules.

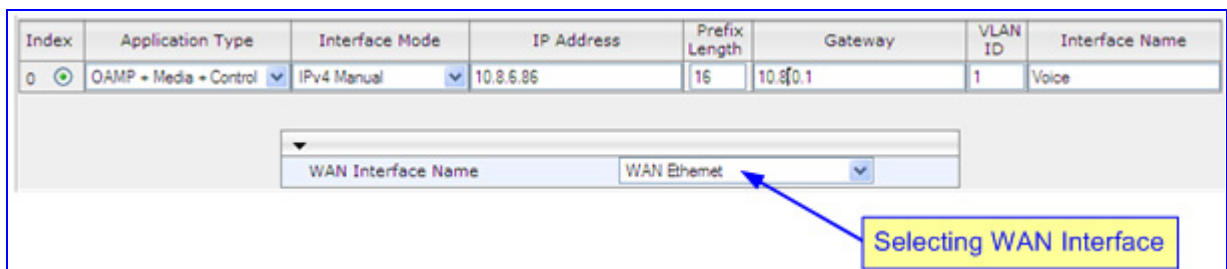


Note: If you do not assign the WAN interface to SIP and media interfaces, then the WAN interface may not be used for VoIP traffic. In such scenarios, the VoIP traffic can be sent and received within the LAN, or sent to the WAN via a third-party LAN router. If a third-party router is used as the interface to the WAN, then you need to define NAT rules (using the NATTranslation parameter) to translate the VoIP LAN IP addresses (defined in the Multiple Interface table and associated with SIP and media interfaces) into global, public IP addresses.

➤ To assign a WAN interface to VoIP traffic:

1. Select the WAN interface:
 - a. Open the 'Multiple Interface Table' page (**Configuration** tab > **VoIP** menu > **Network** submenu > **IP Settings**).

Figure 8-60: Selecting WAN Interface for VoIP Traffic



Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP + Media + Control	IPv4 Manual	10.8.6.86	16	10.8.0.1	1	Voice

WAN Interface Name: WAN Ethernet

Selecting WAN Interface

- b. From the 'WAN Interface Name' drop-down list, select the WAN interface for VoIP traffic.
 - c. Click **Done**, and then reset the device for your setting to take effect.
2. Assign the selected WAN interface to SIP signaling and RTP (media) interfaces. This is done in the SIP Interface and SIP Media Realm tables respectively (whereby the WAN interface is denoted as "WAN"), as described in "Step 4: Configure Multiple SIP and RTP Interfaces" on page 550.

8.4.10.1.3 Step 3: Enable the SBC Application

The procedure below describes how to enable the SBC application. Once enabled, the SBC-specific parameters/pages become available in the Web interface.

➤ **To enable SBC:**

1. Open the 'Applications Enabling' page (**Configuration** tab > **VoIP** menu > **Applications Enabling** submenu > **Applications Enabling**), and then from the 'Enable SBC Application' drop-down list, select 'Enable':

Figure 8-61: Applications Enabling Page

Enable SAS	Disable	▼
Enable SBC Application	Enable	▼
Enable IP2IP Application	Disable	▼

2. Click **Submit**.
3. Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

8.4.10.1.4 Step 4: Define Number of Media Channels

If transcoding is required, the number of DSP channels must be defined, as described in the procedure below. Note that each SBC (B2BUA) session comprises two legs, therefore, if you enter 150, a maximum of 75 calls can occur simultaneously.

➤ **To define the number of media channels for transcoding:**

1. Open the 'IPmedia Parameters' page (**Configuration** tab > **VoIP** menu > **Media** submenu > **IPMedia Settings**), and then in the 'Number of Media Channels' field, enter the number of SBC legs that require transcoding.

Figure 8-62: Defining Number of SBC Sessions

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	0
Answer Machine Detector Sensitivity Resolution	Normal ▼
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	150

Maximum SBC Sessions

2. Click **Submit**.
3. Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

8.4.10.1.5 Step 5: Configure Multiple SIP and RTP Interfaces

The procedure below describes how to configure multiple SIP signaling interfaces and RTP interfaces. The SIP signaling interfaces are defined as *SIP Interfaces*; the RTP interfaces are defined as *Media Realms*. These are associated together under one entity termed *SRD* (Signaling Routing Domain). In the case study, you need to define the following SRD's:

- **LAN SRD:** IP address 10.8.6.86 ("Voice") with SIP signaling interface port 5080 and RTP traffic port range 6000-6190.
- **WAN SRD:** IP address 100.33.2.105 ("WAN") with SIP signaling interface port 5060 and RTP traffic port range 7000-8000.

➤ To configure multiple SIP signaling and RTP interfaces:

1. Configure Media Realms (RTP traffic interfaces) for LAN and WAN legs:
 - a. Open the 'SIP Media Realm Table' page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Realm Configuration**).
 - b. Add a Media Realm for LAN:
 - a. In the 'Media Realm Name' field, enter "LanMediaR".
 - b. In the 'IPv4 Interface Name' field, enter "Voice". **Note:** This string must be identical (and case-sensitive) as that defined in the 'Multiple Interface' table for the 'Interface Name' field (see "Step 1: Configure LAN VoIP IP Address" on page 547).
 - c. In the 'Port Range Start' field, enter "6000".
 - d. In the 'Number of Media Session Legs' field, enter the number of sessions required on LAN (e.g., 20).
 - e. Click **Submit**. Note that the 'Port Range End' field value is automatically calculated (e.g. 6190). For example, the first session uses port 6000, the second session uses port 6010, and so on.
 - c. Add a Media Realm for WAN:
 - a. In the 'Media Realm Name' field, enter "WanMediaR".
 - b. In the 'IPv4 Interface Name' field, enter "WAN". This string is case-sensitive and represents the WAN IP address (interface).
 - c. In the 'Port Range Start' field, enter "7000".
 - d. In the 'Number of Media Session Legs' field, enter the number of sessions required on WAN (e.g., 101).
 - e. Click **Submit**. Note that the 'Port Range End' field value is automatically calculated (e.g. 8000). For example, the first session uses port 7000, the second session uses port 7010, and so on.

Figure 8-63: LAN and WAN Media Realms in SIP Media Realm Table

Index	Media Realm Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End
0	LanMediaR	Voice	6000	20	6190
1	WanMediaR	WAN	7000	101	8000

2. Configure SRD's for LAN and WAN:
 - a. Open the 'SRD Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SRD Table**).
 - b. Add SRD #0 for LAN:
 - a. In the 'Name' field, enter "LanSRD".

- b. In the 'Media Realm' field, enter "LanMediaR". **Note:** This string must be identical (and case-sensitive) as that defined in the 'SIP Media Realm' table (see Step 1.b).
 - c. Click **Apply**.
 - c. Add SRD #1 for WAN:
 - a. In the 'Name' field, enter "WanSRD".
 - b. In the 'Media Realm' field, enter "WanMediaR". **Note:** This string must be identical (and case-sensitive) as that defined in the 'SIP Media Realm' table (see Step 1.c).
 - c. Click **Apply**.

Figure 8-64: SRDs for LAN and WAN in SRD Table

Index	Name	Media Realm	Internal SRD Media Anchoring	Block Unregistered Users	Max Number Of Registered Users	Enable Un-Authenticated Registrations
0	<input type="radio"/> LanSRD	LanMediaR	Anchor Media	NO	-1	YES
1	<input type="radio"/> WanSRD	WanMediaR	Anchor Media	NO	-1	YES

- 3. Configure SIP signaling interfaces for the SBC application for both legs (LAN and WAN):
 - a. Open the 'SIP Interface Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SIP Interface Table**).
 - b. Add a SIP Interface for LAN:
 - a. In the 'Network Interface' field, enter "Voice". **Note:** This string must be identical (and case-sensitive) as that defined in the 'Multiple Interface' table for the 'Interface Name' field (see "Step 1: Configure LAN VoIP IP Address" on page 547).
 - b. From the 'Application Type' drop-down list, select 'SBC'.
 - c. Define the UDP, TCP, and TLS ports as 5080, 5080, and 5081 respectively.
 - d. In the 'SRD' field, enter '0'. This associates the SIP interface with the LAN SRD you defined in Step 2.b.
 - e. Click **Apply**.
 - c. Add a SIP Interface for WAN:
 - a. In the 'Network Interface' field, enter "WAN". **Note:** This string is case-sensitive and represents the WAN IP address.
 - b. From the 'Application Type' drop-down list, select 'SBC'.
 - c. Define the UDP, TCP, and TLS ports as 5060, 5060, and 5061 respectively.
 - d. In the 'SRD' field, enter '1'. This associates this SIP interface with the WAN SRD you defined in Step 2.c.
 - e. Click **Apply**.

Figure 8-65: LAN and WAN SIP Interfaces in the SIP Interface Table

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	<input type="radio"/> Voice	SBC	5080	5080	5081	0
2	<input type="radio"/> WAN	SBC	5060	5060	5061	1

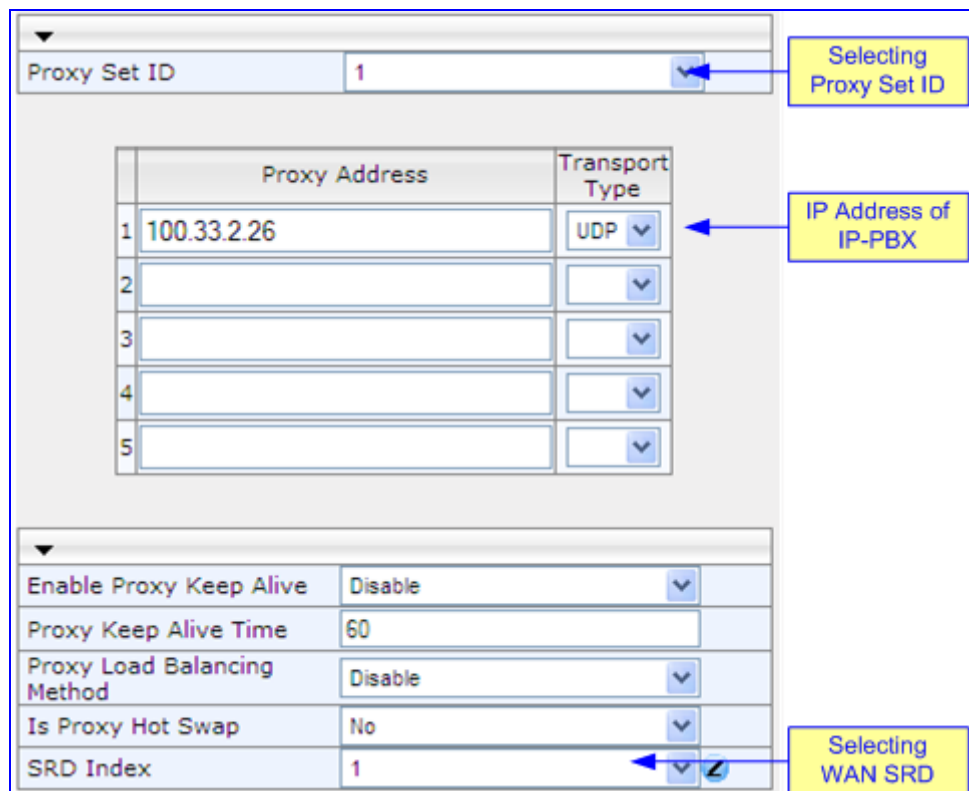
8.4.10.1.6 Step 6: Define Proxy Set for WAN IP-PBX

The procedure below describes how to configure a Proxy Set for the WAN hosted IP-PBX. This represents the IP address of the IP-PBX, which in the case study is 100.33.2.26.

➤ **To configure a Proxy Set for the WAN IP-PBX:**

1. Open the 'Proxy Sets Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).
2. From the 'Proxy Set ID' drop-down list, select '1'.
3. In the 'Proxy Address' field, enter 100.33.2.26, and then from the 'Transport Type' drop-down list, select 'UDP' as the transport type used by the IP-PBX.
4. From the 'SRD Index' drop-down list, select '1'. This associates the Proxy Set with the WAN SRD, configured in "Step 5: Configure Multiple SIP and RTP Interfaces" on page 550. It allows the device to classify calls by Proxy Set for this SRD ID (which is later associated with the IP Group of the WAN IP PBX, configured in "Step 7: Define IP Groups" on page 552).

Figure 8-66: 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: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

SRD Index: 1

5. Click **Submit**.
6. Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

8.4.10.1.7 Step 7: Define IP Groups

An IP Group is a convenient way to represent a SIP User Agent (client or server) entity. An IP Group is defined with a set of characteristics, such as with an SRD and an IP Profile. In our case study, you need to define the following IP Groups:

- Enterprise LAN (users)
- WAN (IP-PBX)

➤ **To configure IP Groups:**

1. Open the 'IP Group Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**).
2. Add IP Group #1 for enterprise LAN (users):
 - a. From the 'Type' drop-down list, select 'USER'.
 - b. In the 'Description' field, enter a brief description of this IP Group (e.g., "LAN users").
 - c. In the 'SRD' field, enter '0' to associate this IP Group with the LAN SRD (defined in "Step 5: Configure Multiple SIP and RTP Interfaces" on page 550).
 - d. Click **Submit**.

Figure 8-67: IP Group 1 (for Enterprise Users) in IP Group Table

Index	
	1

Common Parameters

Type	USER	✎
Description	LAN users	
Proxy Set ID		
SIP Group Name		
Contact User	N/A	
IP Profile ID	0	
SRD	0	
Media Realm		

Gateway Parameters

Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

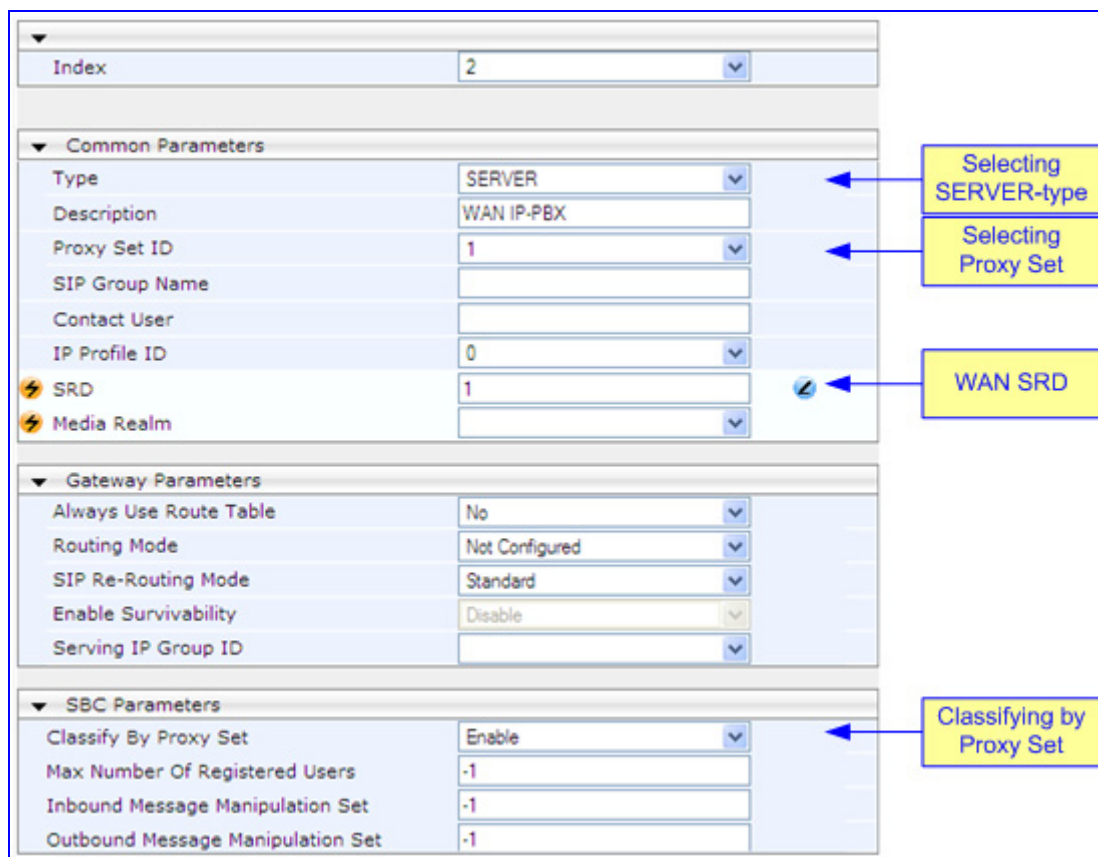
SBC Parameters

Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1

3. Add IP Group #2 for the WAN hosted IP-PBX:
 - a. From the 'Type' drop-down list, select 'SERVER'.
 - b. In the 'Description' field, enter a brief description of this IP Group (e.g., "WAN IP-PBX").
 - c. From the 'Proxy Set ID' drop-down list, select '1' to assign it to the Proxy Set #1 defined in "Step 6: Define Proxy Set for WAN IP-PBX" on page 552. Therefore, this IP Group is defined with IP address 100.33.2.26 and all SIP dialog messages sent to this IP Group are sent to this IP address (i.e., the WAN IP-PBX).

- d. In the 'SRD' field, enter "1" to associate it with the WAN SRD (defined in "Step 5: Configure Multiple SIP and RTP Interfaces" on page 550).
- e. From the 'Classify By Proxy Set' drop-down list, select 'Enable' to allow the device to classify incoming calls as this IP Group based on the Proxy Set.
- f. Click **Submit**.

Figure 8-68: IP Group 2 (for WAN ITSP) in IP Group Table



Index		2
Common Parameters		
Type	SERVER	
Description	WAN IP-PBX	
Proxy Set ID	1	
SIP Group Name		
Contact User		
IP Profile ID	0	
SRD	1	
Media Realm		
Gateway Parameters		
Always Use Route Table	No	
Routing Mode	Not Configured	
SIP Re-Routing Mode	Standard	
Enable Survivability	Disable	
Serving IP Group ID		
SBC Parameters		
Classify By Proxy Set	Enable	
Max Number Of Registered Users	-1	
Inbound Message Manipulation Set	-1	
Outbound Message Manipulation Set	-1	

4. Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

8.4.10.1.8 Step 8: Define Classification Rules for LAN Users

The procedure below describes how to configure Classification rules for classifying LAN users. In our case study, the rule classifies them to the USER-type IP Group #1.

➤ To configure Classification rules for LAN users:

1. Open the 'Classification Table' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Routing SBC** submenu > **Classification Table**).
2. In the 'Source SRD ID' field, enter '0'. This is the LAN SRD configured in "Step 5: Configure Multiple SIP and RTP Interfaces" on page 550.
3. In the 'Source IP Address' field, enter the IP address of the LAN users (IP phones). You can enter the IP address range "10.8.6.*" to represent these IP phones.

4. In the 'Source IP Group' field, enter '1'. This classifies calls from LAN users as belonging to IP Group 1 (defined in "Step 7: Define IP Groups" on page 552).

Figure 8-69: IP Group Classification Rule for LAN Users

Index	Source SRD ID	Source IP Address	Source Username Prefix	Source Host Prefix
1	<input type="text" value="0"/>	<input type="text" value="10.8.6.*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>

Destination Username Prefix	Destination Host Prefix	Source IP Group ID
<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="1"/>

5. Click **Apply**.



Note: There is no need to classify the WAN IP-PBX. This entity's IP Group 2 is configured with Proxy Set #1 and enabled to 'Classify by Proxy'. Therefore, all SIP dialog messages received from the IP address associated with this Proxy Set are automatically classified to belong to IP Group 2.

8.4.10.1.9 Step 9: Define IP-to-IP Routing Rules

The procedure below describes how to configure IP-to-IP routing rules for routing SIP signaling and calls between IP Group 1 (LAN users) and IP Group 2 (WAN IP-PBX).

➤ **To configure IP-to-IP routing rules:**

1. Open the 'IP2IP Routing Table' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Routing SBC** submenu > **IP to IP Routing Table**).
2. Add an IP-to-IP routing rule (Index #1) for routing calls from IP Group 1 to IP Group 2:
 - a. From the 'Source IP Group ID' drop-down list, select '1'. This is the IP Group to which the LAN users belong (as defined in "Step 7: Define IP Groups" on page 552).
 - b. From the 'Destination Type' drop-down list, select 'IP Group'.
 - c. From the 'Destination IP Group ID' drop-down list, select '2'. This routes calls from IP Group 1 to IP Group 2.
 - d. Click **Apply**.
3. Add an IP-to-IP routing rule (Index #1) for routing calls from IP Group 2 to IP Group 1:
 - a. From the 'Source IP Group ID' drop-down list, select '2'. This is the IP Group to which the WAN IP-PBX belongs (as defined in "Step 7: Define IP Groups" on page 552).
 - b. From the 'Destination Type' drop-down list, select 'IP Group'.
 - c. From the 'Destination IP Group ID' drop-down list, select '1'. This routes calls from IP Group 2 to IP Group 1.

- d. Click **Apply**.

Figure 8-70: IP-to-IP Routing Rules

Index	Source IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix
1	<input type="radio"/>	1	*	*
2	<input type="radio"/>	2	*	*

Destination Host	Request Type	Destination Type	Destination IP Group ID
*	All	IP Group	2
*	All	IP Group	1

Destination SRD ID	Destination Address	Destination Port
		0
		0

Destination Transport Type	Alternative Route Options
	Route Row
	Route Row

8.4.10.2 Survivability and Alternative Routing

This section provides an example for configuring SBC Survivability for LAN users. This example is based on the scenario described in "General SBC Setup" on page 546.

In normal operation, the IP-PBX serves the enterprise's IP phones (calls are routed to the IP-PBX). The SBC Survivability feature ensures the continuity (survivability) of calls even if the Proxy server (in our example, the hosted IP-PBX) does not respond or the WAN is unavailable. Therefore, SBC Survivability feature offers an alternative routing mechanism. It does this by utilizing the device's internal registration database to route calls to registered users.

The survivability feature provides the following survivability mechanisms:

- If the IP-PBX does not respond (WAN failure), the SBC application ensures that calls between IP phones within the enterprise's LAN are maintained.
- If there is a WAN failure and the called destination is not a registered user (not registered in the device's database), the calls are routed to the PSTN.

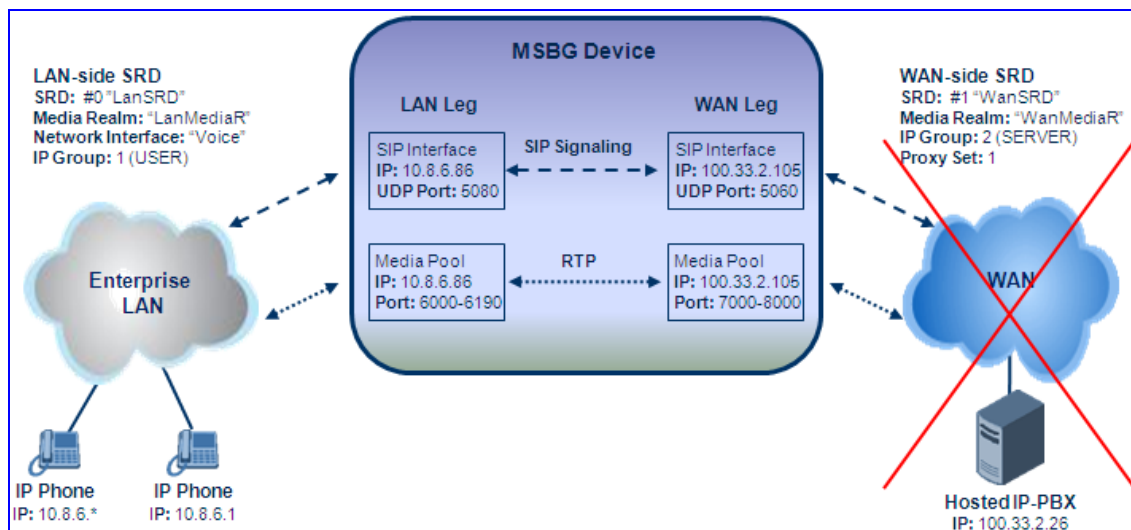
You can view registered users in the device's database by accessing the 'SAS/SBC Registered Users' page (**Status & Diagnostics** tab > **VoIP Status** menu > **SAS/SBC Registered Users**).

In addition to the configuration described in "General SBC Setup" on page 546, this example requires the following additional configurations:

- Enable the Keep-Alive feature for the Proxy Set ID# 1 belonging to the IP-PBX.

- Define an alternative IP-to-IP routing rule for IP Phones IP Group #1 (USER) to IP Phones IP Group #1 (USER). This is the alternative route if the IP-PBX does not respond, whereby the user is searched in the device's users registration database.

Figure 8-71: Survivability Example Setup



8.4.10.2.1 Step 1: Enable Proxy Keep-Alive

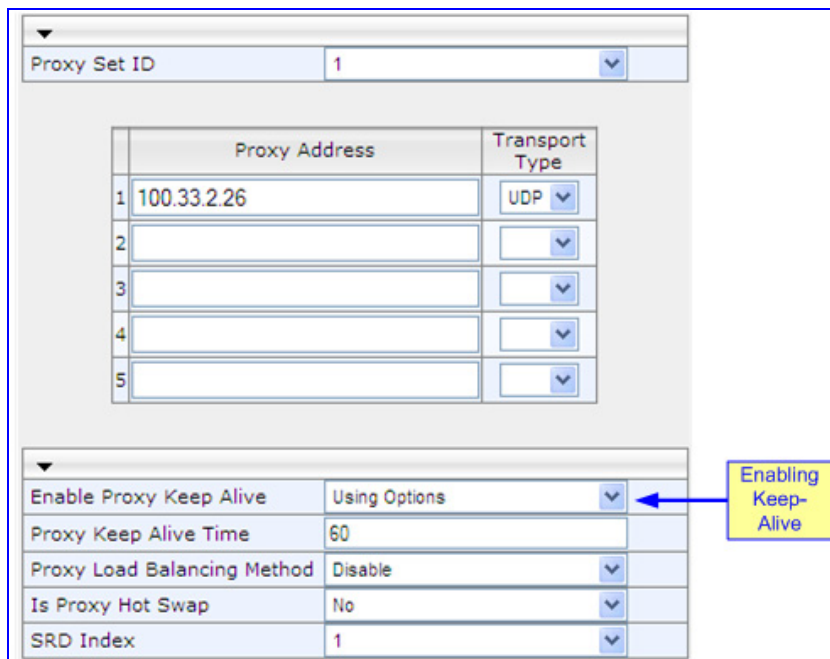
The procedure below describes how to configure the Proxy Keep-Alive mechanism for the hosted IP-PBX. This is done for the Proxy Set that you defined for the IP-PBX (i.e., Proxy Set ID# 1) in "Step 6: Define Proxy Set for WAN IP-PBX" on page 552.

➤ **To enable proxy keep-alive mechanism:**

1. Open the 'Proxy Sets Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).
2. From the 'Proxy Set ID' drop-down list, select '1'. This is the Proxy Set for the IP-PBX.

- From the 'Enable Proxy Keep Alive' drop-down list, select 'Using Options' to enable the Proxy Keep-alive mechanism.

Figure 8-72: Enabling Proxy Keep-Alive



The screenshot shows a configuration window for Proxy Set ID 1. It contains a table for Proxy Address and Transport Type, and a section for Proxy Keep Alive settings. A yellow callout box labeled 'Enabling Keep-Alive' points to the 'Enable Proxy Keep Alive' dropdown menu, which is currently set to 'Using Options'.

	Proxy Address	Transport Type
1	100.33.2.26	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
SRD Index	1

- Click **Submit**.
- Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

8.4.10.2 Step 2: Define Alternative Routing Rules

The procedure below describes how to configure an alternative route for the LAN users if the main route (previously defined in "Step 9: Define IP-to-IP Routing Rules" on page 555) becomes unavailable. Note that the alternative route must be defined in the row located immediately below the main route for IP Group 1 (i.e., LAN users) in the table.

➤ To configure alternative IP-to-IP routing rule:

- Open the 'IP2IP Routing Table' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Routing SBC** submenu > **IP to IP Routing Table**).
- In the 'Add' field, enter '2', and then click **Add**; the new entry is added as Index 2, immediately below the main route for Source IP Group 1. The previous entry Index 2 is now shifted down to Index 3.
- From the 'Source IP Group ID' drop-down list, select '1'. This is the IP Group to which the LAN users belong (as previously defined in "Step 7: Define IP Groups" on page 552).
- From the 'Destination Type' drop-down list, select 'IP Group'.
- From the 'Destination IP Group ID' drop-down list, select '1'. This routes calls between the LAN users (i.e., between IP Group 1 and IP Group 1).

6. From the 'Alternative Route Options' drop-down list, select 'Alt Route Consider Inputs'.

Figure 8-73: Configuring IP-to-IP Routing Rules

Index	Source IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix
1 <input type="radio"/>	1	*	*	*
2 <input type="radio"/>	1	*	*	*
3 <input type="radio"/>	2	*	*	*

Destination Host	Request Type	Destination Type	Destination IP Group ID
*	All	IP Group	2
*	All	IP Group	1
*	All	IP Group	1

Destination SRD ID	Destination Address	Destination Port
		0
0		0
		0

Destination Transport Type	Alternative Route Options
	Route Row
	Alt Route Consider Inputs
	Route Row

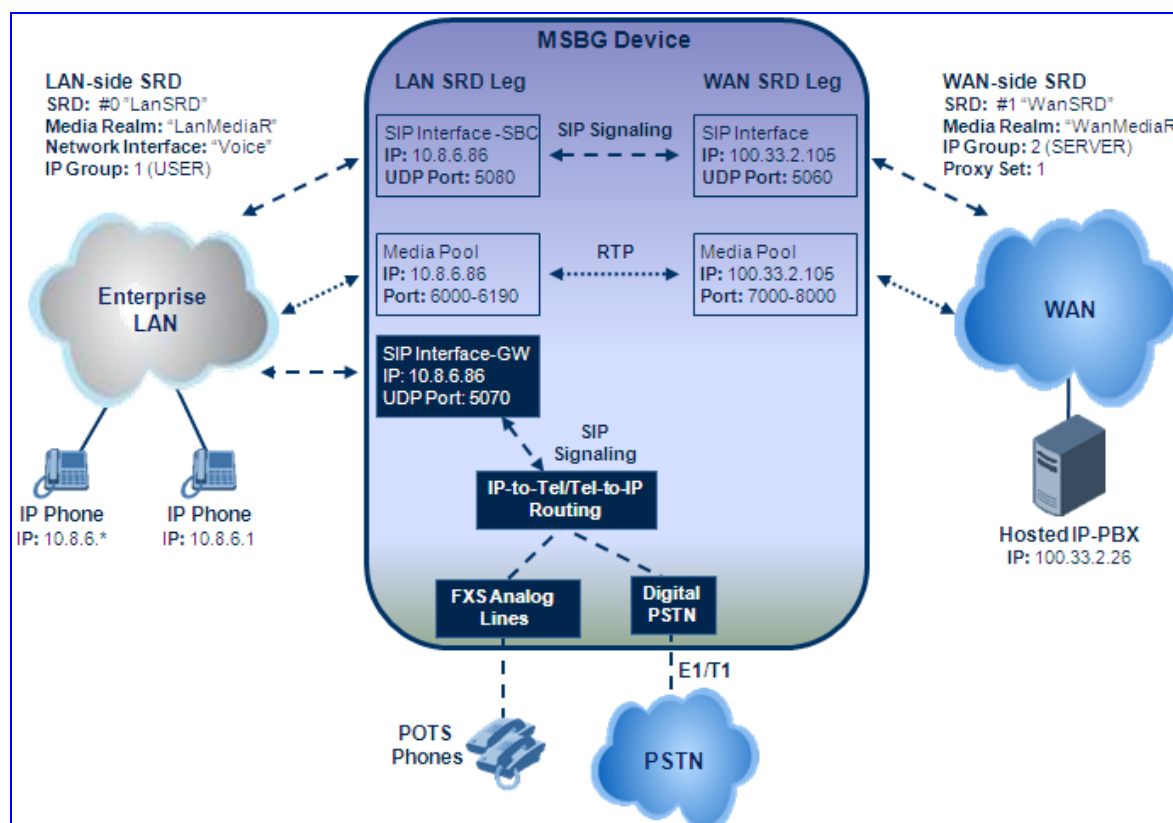
7. Click **Apply**.

8.4.10.3 SBC-to-PSTN Routing

This section describes how to setup the device for SBC-to-PSTN routing. This example is based on the general scenario described in "General SBC Setup" on page 546, but in addition assumes the following:

- The device is connected to the PSTN network by an E1/T1 trunk
- Analog POTS phones are connected directly to the device using the device's FXS module

Figure 8-74: SBC-to-PSTN Routing Example Setup



8.4.10.3.1 Step 1: Add SIP Interface for PSTN

The procedure below describes how to configure a SIP signaling interface for the PSTN. This SIP interface is configured for the "GW/IP2IP" application using port 5070 on the LAN SRD. Note that this SIP interface is in addition to those previously defined in "General SBC Setup" on page 546.

➤ **To configure a SIP interface for the PSTN:**

1. Open the 'SIP Interface Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SIP Interface Table**).
2. In the 'Add' field, enter 3, and then click **Add**.
3. In the 'Network Interface' field, enter "Voice". **Note:** This string must be identical (and case-sensitive) as that defined in the 'Multiple Interface' table for the 'Interface Name' field (see "Step 1: Configure LAN VoIP IP Address" on page 547).
4. From the 'Application Type' drop-down list, select 'GW/IP2IP'.

5. Define the UDP, TCP, and TLS ports as 5070, 5070, and 5071 respectively.
6. In the 'SRD' field, enter '0'. This associates the SIP interface with the LAN SRD you defined "Step 5: Configure Multiple SIP and RTP Interfaces" on page 550.

Figure 8-75: Configuring SIP Interface for PSTN (GW)

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	<input type="radio"/> Voice	SBC	5080	5080	5081	0
2	<input type="radio"/> WAN	SBC	5060	5060	5061	1
3	<input type="radio"/> Voice	GW\IP2IP	5070	5070	5071	0

7. Click **Apply**.

8.4.10.3.2 Step 2: Define Device as a Proxy Set

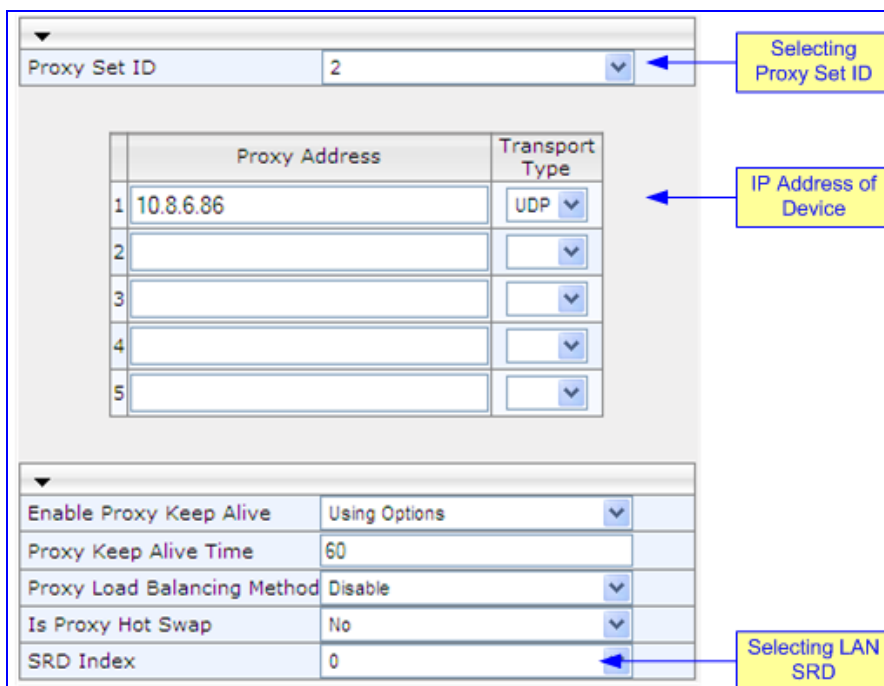
The procedure below describes how to configure the device's LAN SBC interface (i.e., 10.8.6.86) as a Proxy Set. This Proxy Set is later associated with the IP Group #3 for PSTN calls in "Step 3: Define IP Group for PSTN" on page 562.

➤ **To configure the device's LAN SBC as a Proxy Set:**

1. Open the 'Proxy Sets Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).
2. From the 'Proxy Set ID' drop-down list, select '2'.
3. In the 'Proxy Address' field, enter 10.8.6.86, and then from the 'Transport Type' drop-down list, select 'UDP' as the transport type.

4. From the 'SRD Index' drop-down list, select '0'. This associates the Proxy Set with the LAN SRD, configured in "Step 5: Configure Multiple SIP and RTP Interfaces" on page 550. It allows the device to classify calls by Proxy Set for this SRD.

Figure 8-76: Defining Device as Proxy Set



Proxy Set ID: 2

	Proxy Address	Transport Type
1	10.8.6.86	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

SRD Index: 0

5. Click **Submit**.
6. Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

8.4.10.3.3 Step 3: Define IP Group for PSTN

The procedure below describes how to configure an IP Group (#3) for PSTN users. This IP Group represents the device's LAN SRD interface.

➤ **To configure an IP Group for PSTN users:**

1. Open the 'IP Group Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**).
2. From the 'Index' drop-down list, select '3'.
3. From the 'Type' drop-down list, select 'SERVER'.
4. In the 'Description' field, enter a brief description of this IP Group (e.g., "PSTN Users").
5. From the 'Proxy Set ID' drop-down list, select '2' to assign it to Proxy Set #2 defined in "Step 2: Define Device as a Proxy Set" on page 561. Therefore, this IP Group is defined with IP address 10.8.6.86 and all SIP dialog messages sent to this IP Group are sent to this IP address (i.e., the device's LAN interface).
6. In the 'SRD' field, enter "0" to associate it with the LAN SRD (defined in "Step 5: Configure Multiple SIP and RTP Interfaces" on page 550).

7. From the 'Classify By Proxy Set' drop-down list, select 'Disable'. This ensures that the existing Classification rule for 10.8.6.* (defined in "Step 8: Define Classification Rules for LAN Users" on page 554) also applies to PSTN users as belonging to IP Group 1 and FXS users can be registered to the device's database.

Figure 8-77: Defining IP Group for PSTN Users

The screenshot shows a configuration window for defining an IP group. The 'Index' is set to 3. The 'Common Parameters' section includes:

- Type: SERVER (selected)
- Description: PSTN Users
- Proxy Set ID: 2 (selected)
- SIP Group Name: (empty)
- Contact User: (empty)
- IP Profile ID: 0 (selected)
- SRD: 0
- Media Realm: (empty)

The 'Gateway Parameters' section includes:

- Always Use Route Table: No
- Routing Mode: Not Configured
- SIP Re-Routing Mode: Standard
- Enable Survivability: Disable
- Serving IP Group ID: (empty)

The 'SBC Parameters' section includes:

- Classify By Proxy Set: Disable (selected)
- Max Number Of Registered Users: -1
- Inbound Message Manipulation Set: -1
- Outbound Message Manipulation Set: -1

Callouts on the right side of the form indicate the following actions:

- Selecting SERVER-type (points to Type)
- Selecting Proxy Set (points to Proxy Set ID)
- LAN SRD (points to IP Profile ID)
- Disabling Classification by Proxy Set (points to Classify By Proxy Set)

8. Click **Submit**.
9. Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

8.4.10.3.4 Step 4: Define IP-to-IP Routing Rules

The procedure below describes how to configure IP-to-IP routing rules. The following rules need to be included in the configuration:

■ Existing rules:

- Routing from LAN users to IP-PBX (i.e., from IP Group 1 to IP Group 2), as previously defined in "Step 9: Define IP-to-IP Routing Rules" on page 555
- Alternative routing between LAN users in case of WAN or IP-PBX failure, as previously defined in "Survivability and Alternative Routing" on page 556
- Routing from IP-PBX to LAN users (i.e., from IP Group 2 to IP Group 1), as previously defined in "Step 9: Define IP-to-IP Routing Rules" on page 555

■ New rules to add:

- Alternative routing to PSTN for LAN users in case of WAN or IP-PBX failure (this is the secondary alternative route if the user is not registered in the device's user registration database)
- Routing for calls destined to PSTN network

➤ To configure IP-to-IP routing rules:

1. Open the 'IP2IP Routing Table' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Routing SBC** submenu > **IP to IP Routing Table**).
2. Add a secondary alternative IP-to-IP routing rule (Index #3) for routing LAN user calls to PSTN upon WAN/IP-PBX failure:
 - a. In the 'Add' field, enter 3, and then click **Add**; the new entry is added as Index #3 after Index #2. The previous Index #3 is now shifted down to Index #4.
 - b. From the 'Source IP Group ID' drop-down list, select '1'. This is the IP Group to which the LAN users belong.
 - c. From the 'Destination Type' drop-down list, select 'Dest Address' and then in the 'Destination Address' field, enter the IP address 10.8.6.86 (i.e., the IP address of the device's LAN gateway interface).
 - d. In the 'Destination Port' field, enter port number 5070.
 - e. From the 'Alternative Route Options' drop-down list, select 'Alt Route Consider Inputs'.
 - f. Click **Apply**.
3. Add an IP-to-IP routing rule (Index #4) for routing calls destined to the PSTN network:
 - a. From the 'Source IP Group ID' drop-down list, select '2'. This is the IP Group to which the WAN IP-PBX belongs.
 - b. In the 'Destination Username Prefix', enter 01. This represents calls destined for the PSTN. (You can change this according to your PSTN numbering plan.)
 - c. From the 'Destination Type' drop-down list, select 'Dest Address', and then in the 'Destination Address' field, enter the IP address 10.8.6.86 (i.e., the IP address of the device's LAN gateway interface).
 - d. In the 'Destination Port' field, enter port number 5070.

- e. Click **Apply**.

Figure 8-78: Defining IP-to-IP Routing Rules

Index	Source IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix
1 <input type="radio"/>	1	*	*	*
2 <input type="radio"/>	1	*	*	*
3 <input type="radio"/>	1	*	*	*
4 <input type="radio"/>	2	*	*	01
5 <input type="radio"/>	2	*	*	*

Destination Host	Request Type	Destination Type	Destination IP Group ID
*	All	IP Group	2
*	All	IP Group	1
*	All	Dest Address	
*	All	Dest Address	
*	All	IP Group	1

Destination SRD ID	Destination Address	Destination Port
		0
0		0
	10.8.6.86	5070
	10.8.6.86	5070
		0

Destination Transport Type	Alternative Route Options
	Route Row
	Alt Route Consider Inputs
	Alt Route Consider Inputs
	Route Row
	Route Row

The configured rules are summarized below:

- **Index #1:** First choice route for IP Group 1 (i.e., LAN and PSTN users) when calling each other or any user on WAN. The call is sent to IP Group 2 (i.e., WAN IP-PBX) through the device's SBC interface.
- **Index #2:** Alternative route for calls from IP Group 1 (LAN and PSTN users) in case of WAN/IP-PBX failure. This rule uses the device's internal registration database to reach the destination user.
- **Index #3:** Second alternative route for calls from IP Group 1 (LAN and PSTN users) in case of WAN/IP-PBX failure and no user is registered in the database. This rule routes the call to the device's Gateway interface (i.e. 10.8.6.86:5070).
- **Index #4:** For calls coming from IP Group 2 (i.e., WAN IP-PBX) to PSTN users. This rule directs all calls with destination phone number starting with "01" to the device's Gateway interface (i.e. 10.8.6.86:5070).
- **Index #5:** All other calls from IP Group 2 are routed to IP Group 1.

8.4.10.3.5 Step 5: Define Trunk Groups for PSTN Users

The procedure below describes how to configure and enable the PSTN users. This is done by defining Trunk Groups. You need to configure Trunk Groups for the following PSTN interfaces:

- FXS - analog phones connected to the device's FXS module
- E1/T1 trunk - PSTN network connected to the device's PRI TRUNK module

➤ To configure Trunk Groups:

1. Open the 'Trunk Group Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Hunt Group** > **Hunt Group**).
2. Add a Trunk Group for the FXS interfaces:
 - a. From the 'Module' drop-down list, select 'Module 2 FXS'.
 - b. In the 'Channels' field, enter the number of FXS channels. this can be entered as a range (e.g., 1-4 for channels 1 through 4).
 - c. In the 'Phone Number' field, enter the phone numbers of the FXS channels. You need only enter the phone number of the first channel; the next channel is allocated the next consecutive phone number (e.g., if you enter 2200, the next channel is allocated phone number 2201, and so on).
 - d. In the 'Trunk Group ID' field, enter "1" as the Trunk Group ID.
 - e. Click **Submit**.
3. Add a Trunk Group for the E1/T1 interface:
 - a. From the 'Module' drop-down list, select 'Module 1 PRI'.
 - b. In the 'From Trunk' and 'To Trunk' fields, select '1' (i.e., Trunk 1).
 - c. In the 'Channels' field, enter "1-30" for the number of channels.
 - d. In the 'Phone Number' field, enter any phone number for the channels. This is only a logical phone number (i.e., not used).
 - e. In the 'Trunk Group ID' field, enter "2" as the Trunk Group ID.
 - f. Click **Submit**.

Figure 8-79: Defining Trunk Groups

Add Phone Context As Prefix		Disable					
Trunk Group Index		1-10					

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 2 FXS			1-4	2200	1	0
2	Module 1 PRI	1	1	1-30	1100	2	0

4. Define the method for allocating calls to channels of the Trunk Groups:
 - a. Open the 'Trunk Group Settings' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Hunt Group** submenu > **Hunt Group Settings**).
 - b. Define the channel select mode for FXS users (i.e., Trunk Group 1):
 - a. In the 'Trunk Group ID' field, enter '1'.

- b. From the 'Channel Select Mode' drop-down list, select 'By Dest Phone Number'. This setting sends the call to a specific FXS user according to the called (destination) number.
- c. From the 'Registration Mode' drop-down list, select 'Per Endpoint'. This allows the FXS users to register to the device's internal database, using IP Group 3 (defined in "Step 3: Define IP Group for PSTN" on page 562). Since you disabled 'Classify by Proxy' for this IP Group, FXS users are handled as though belonging to IP Group 1 and adhere to the same IP-to-IP routing rules.
- d. From the 'Serving IP Group ID' drop-down list, select '3'.
- e. Click **Submit**.
- c. Define the channel select mode for the PSTN network (i.e., Trunk Group 2):
 - a. In the 'Trunk Group ID' field, enter '2'.
 - b. From the 'Channel Select Mode' drop-down list, select 'Cyclic Ascending'.
 - c. From the 'Registration Mode' drop-down list, select 'Don't Register'.
 - d. From the 'Serving IP Group ID' drop-down list, select '3'.
 - e. Click **Submit**.

Figure 8-80: Defining Channel Select Mode

▼

Index1-12▼

	Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	1	By Dest Phone Number▼	Per Endpoint▼	3▼		
2	2	Cyclic Ascending▼	Don't Register▼	3▼		

Note that both Trunk Groups traverse the device using IP Group 3 (i.e., the device's Gateway interface).

8.4.10.3.6 Step 6: Define IP-to-Tel Routing Rules

The procedure below describes how to configure IP-to-Tel routing rules. These rules route calls to the previously defined Trunk Groups in "Step 5: Define Trunk Groups for PSTN Users" on page 566.

You need to configure the following rules:

- Rule #1: route calls with destination prefix 01 to the E1/T1 trunk/PSTN network (i.e., Trunk Group 2)
- Rule #2: route all other calls to FXS users (i.e., Trunk Group 1)

➤ To configure IP-to-Tel 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**).
2. Add a rule for routing calls with destination prefix 01 to the PSTN:
 - a. In the 'Dest Phone Prefix', enter '01'.
 - b. In the 'Source Phone Prefix' and 'Source IP Address' fields, enter an asterisk symbol (*) to indicate any.

- c. In the 'Trunk Group ID' field, enter '1'.
 - d. Click **Submit**.
3. Add a rule for routing all other calls to FXS users:
 - a. In the 'Dest Phone Prefix', 'Source Phone Prefix' and 'Source IP Address' fields, enter an asterisk symbol (*) to indicate any.
 - b. In the 'Trunk Group ID' field, enter '2'.
 - c. Click **Submit**.

Figure 8-81: Defining IP-to-Tel Routing Rules

Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID
	01	*	*	2
	*	*	*	1

8.4.10.4 Basic Coder Transcoding

This section describes how to configure the SBC coder transcoding feature. This feature enables SIP entities supporting different codecs to communicate with one another by offering additional coders supported by the another.

This example is based on the general scenario described in "General SBC Setup" on page 546, but in addition assumes the following:

- IP Phone #1 (USER1) supports G.711
- IP Phone #2 (USER2) supports G.729

This example configuration allows the two LAN IP Phones (pertaining to IP Group #1) to communicate with one another and requires the following additional configuration:

- Define a Coder Group with coders G.711 and G.729.
- Define an IP Profile with the field 'Extension Coders Group ID' set to the defined Coder Group mentioned above.
- Assign the IP Profile to the LAN users IP Group.

8.4.10.4.1 Step 1: Define a Coder Group

The procedure below describes how to configure a Coder Group, which defines the coders used by the LAN IP Phones.

➤ To configure a Coder Group:

1. Open the 'Coder Group Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **Coders Group Settings**).
2. From the 'Coder Group ID' drop-down list, select '1'.

3. Add an entry for G.711 and another entry for G.729.

Figure 8-82: Configuring the Coder Group

▼				
Coder Group ID				1 ▼
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711A-law ▼	20 ▼	64 ▼	8	Disabled ▼
G.729 ▼	20 ▼	8 ▼	18	Disabled ▼

8.4.10.4.2 Step 2: Define an IP Profile

The procedure below describes how to configure an IP Profile. You need to assign to this IP Profile the Coder Group #1 that you defined in "Step 1: Define a Coder Group" on page 568.

➤ **To configure an IP Profile:**

1. Open the 'IP Profile Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **IP Profile Settings**).
2. From the 'Profile ID' drop-down list, select '1'.
3. Under the **SBC** group, from the 'Extension Coders Group ID' drop-down list, select 'Coders Group 1'.

Figure 8-83: Configuring the IP Profile for Coder Transcoding

▼	
Profile ID	1 ▼
Profile Name	
▼ Common Parameters	
RTT ID DiffServ	4F
▼ SBC	
Transcoding Mode	Only if Required ▼
Extension Coders Group ID	1

Profile ID

Coder Group 1

4. Click **Submit**.
5. Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

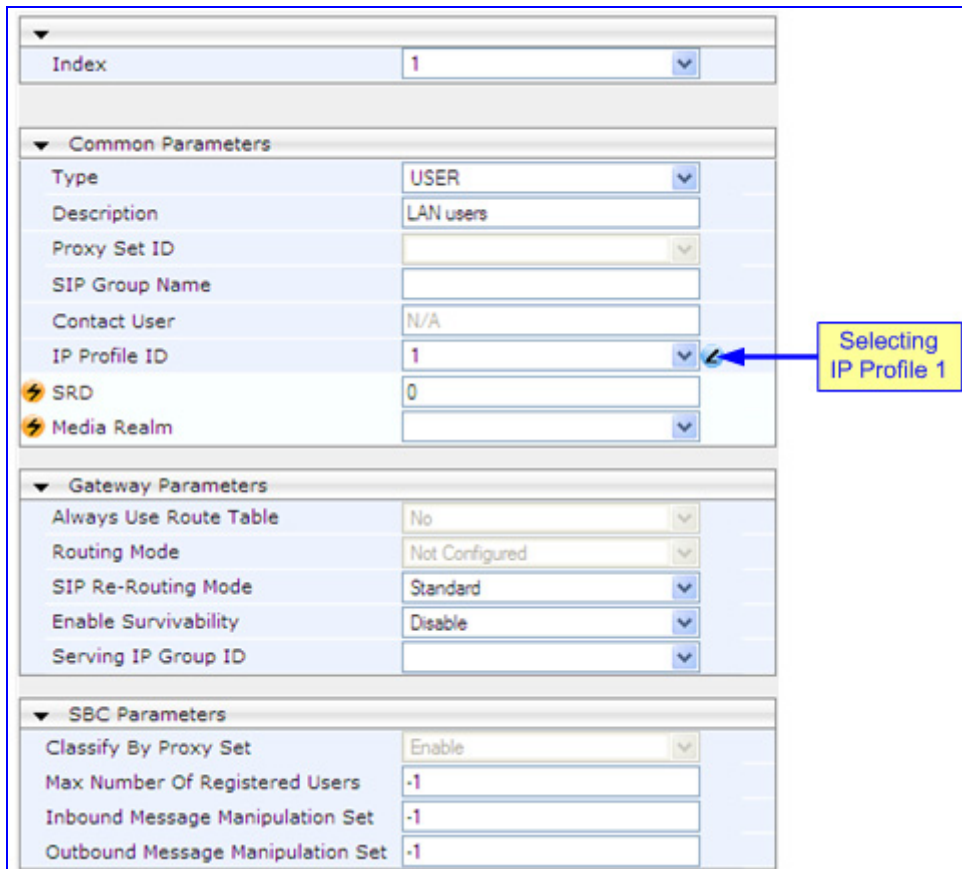
8.4.10.4.3 Step 3: Assign IP Profile to LAN Users IP Group

The procedure below describes how to assign the IP Profile defined in "Step 2: Define an IP Profile" on page 569 to the LAN users IP Group #3. You need to assign to this IP Profile the Coder Group #1 that you defined in "Step 1: Define a Coder Group" on page 568.

➤ **To assign the IP Profile to the LAN users IP Group:**

1. Open the 'IP Group Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**).
2. From the 'Index' drop-down list, select '1' (i.e., the IP Group for the IP Phones).
3. From the 'IP Profile ID' drop-down list, select '1'.

Figure 8-84: Defining IP Profile for USER IP Group



Index		1
Common Parameters		
Type	USER	
Description	LAN users	
Proxy Set ID		
SIP Group Name		
Contact User	N/A	
IP Profile ID	1	
SRD	0	
Media Realm		
Gateway Parameters		
Always Use Route Table	No	
Routing Mode	Not Configured	
SIP Re-Routing Mode	Standard	
Enable Survivability	Disable	
Serving IP Group ID		
SBC Parameters		
Classify By Proxy Set	Enable	
Max Number Of Registered Users	-1	
Inbound Message Manipulation Set	-1	
Outbound Message Manipulation Set	-1	

4. Click **Submit**.
5. Save the settings to flash memory ("burn") and reset the device (see "Saving Configuration" on page 336).

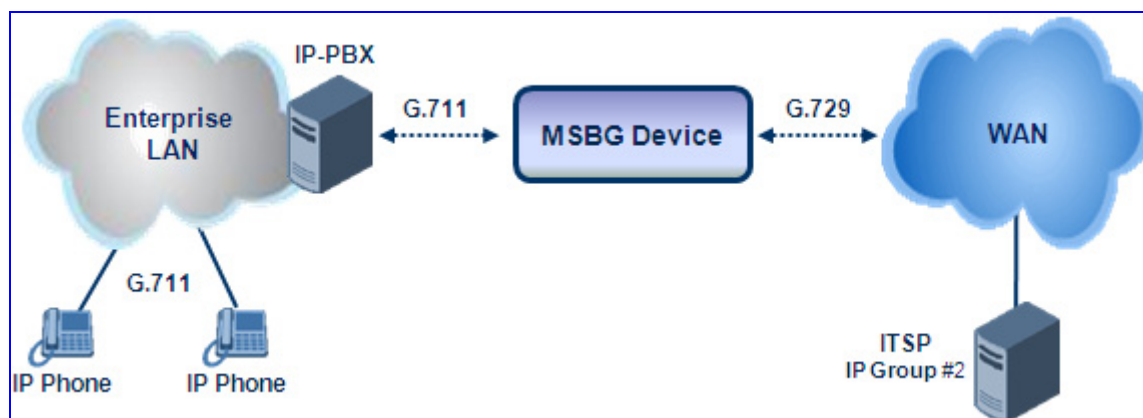
8.4.10.5 Advanced Coder Transcoding

This section describes how to configure an advanced SBC coder transcoding setup. This example is not based on the previous examples and only describes the configuration of the coder transcoding feature itself. It assumes that the other elements such as SRD's and IP Groups have been configured according to your network environment. Advanced transcoding includes the Allowed Coder Groups feature, which allows you to block the use of coders that are not defined in the Allowed Coders Group list.

This example assumes the following:

- Device deployed at an enterprise, interfacing between enterprise's IP-PBX and an Internet Telephony Service Provider (ITSP)
- Enterprise deployed with LAN IP phones for VoIP calls
- LAN IP phones use G.711 coder
- ITSP uses only G.729 coder

Figure 8-85: Advanced Transcoding Example Scenario



8.4.10.5.1 Step 1: Define Coder Groups

The procedure below describes how to configure a Coder Group (with G.711) for the LAN users and a Coder Group (with G.729) for the ITSP. These Coder Groups are later assigned to the IP Profiles of the LAN users and ITSP (in "Step 2: Define an IP Profile" on page 569).

➤ To configure Coder Groups:

1. Open the 'Coder Group Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **Coders Group Settings**).
2. Add a Coder Group for the LAN users:
 - a. From the 'Coder Group ID' drop-down list, select '1'.
 - b. Add an entry for G.711.

Figure 8-86: Defining Coder Group for LAN Users

▼				
Coder Group ID				1 ▼
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711A-law ▼	20 ▼	64 ▼	8	Disabled ▼

- c. Click **Submit**.
3. Add a Coder Group for the ITSP:
 - a. From the 'Coder Group ID' drop-down list, select '2'.

- b. Add an entry for G.729.

Figure 8-87: Defining Coder Group for ITSP

<div> <div>▼</div> <div>Coder Group ID</div> <div>2 ▼</div> </div>				
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.729 ▼	20 ▼	8 ▼	18	Disabled ▼

- c. Click **Submit**.

8.4.10.5.2 Step 2: Define Allowed Coders

The procedure below describes how to configure an Allowed Coders Group for ITSP. This ensures that the device uses only the coder G.729 on its outbound leg to the ITSP. This Allowed Coder Group is later assigned to the IP Profile of the ITSP (in "Step 2: Define an IP Profile" on page 569).

➤ **To configure an Allowed Coder Group:**

1. Open the 'Allowed Coders Group' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Allowed Coders Group**).
2. From the 'Allowed Coders Group ID' drop-down list, select '1'.
3. From the 'Coder Name' drop-down list, select 'G.729'.

Figure 8-88: Defining Allowed Coder Group

<div> <div>▼</div> <div>Allowed Coders Group ID</div> <div>1 ▼</div> </div>	
<div> <div>Coder Name</div> <div>G.729 ▼</div> <div>▼</div> </div>	

4. Click **Submit**.

8.4.10.5.3 Step 3: Define IP Profiles

The procedure below describes how to configure IP Profiles for the LAN users and ITSP. These IP Profiles need to be assigned the following:

- IP Profile for LAN users must be assigned Coder Group #1 (i.e., G.711)
- IP Profile for ITSP must be assigned Coder Group #2 and Allowed Coder Group #1

These IP Profiles are later assigned to the IP Groups for LAN users and ITSP (in "Step 4: Assign IP Profiles to IP Groups" on page 574).

➤ **To configure IP Profiles:**

1. Open the 'IP Profile Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **IP Profile Settings**).
2. Add IP Profile #1 for LAN users:
 - a. From the 'Profile ID' drop-down list, select '1'.
 - b. In the 'Profile Name', enter a brief description (e.g., "LAN Users").
 - c. From the 'Extension Coders Group ID', select '1'. This is the Coders Group that you defined for the LAN users in "Step 1: Define Coders Groups" on page 571.
 - d. Click **Submit**.

Figure 8-89: Defining IP Profile for LAN Users

The screenshot displays the 'IP Profile Settings' form. The top section shows 'Profile ID' set to '1' and 'Profile Name' set to 'LAN Users'. Below this, the 'SBC' section is expanded, showing 'Transcoding Mode' as 'Only if Required', 'Extension Coders Group ID' as 'Coders Group 1', 'Allowed Coders Group ID' as 'None', 'SBC Media Security Behaviour' as 'As Is', and 'Allowed Coders Mode' as 'Restriction'. Two callouts with arrows point to the 'Profile ID' field and the 'Coders Group 1' field in the 'Extension Coders Group ID' dropdown.

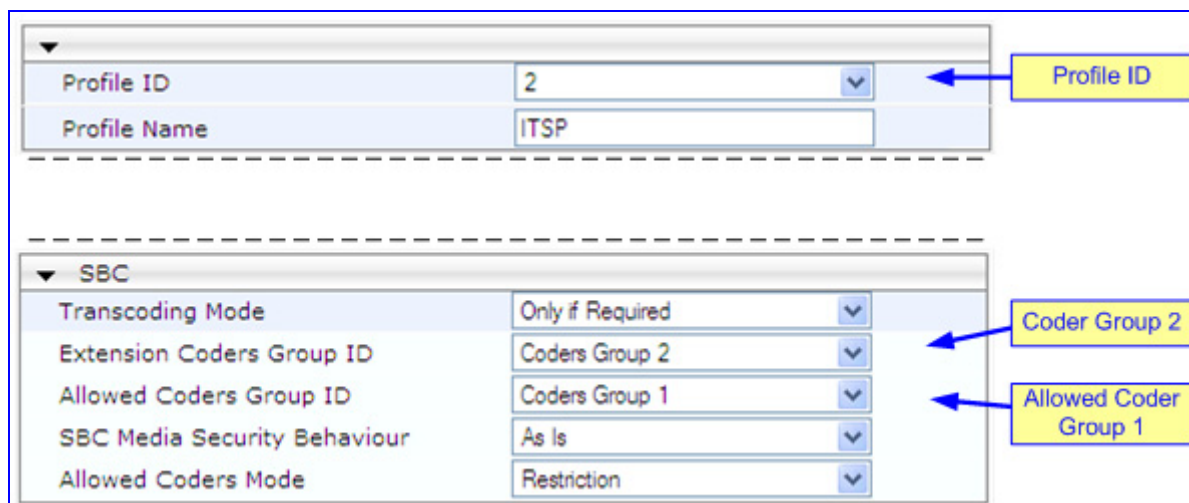
Profile ID	1
Profile Name	LAN Users

SBC	
Transcoding Mode	Only if Required
Extension Coders Group ID	Coders Group 1
Allowed Coders Group ID	None
SBC Media Security Behaviour	As Is
Allowed Coders Mode	Restriction

3. Add IP Profile #2 for the ITSP:
 - a. From the 'Profile ID' drop-down list, select '2'.
 - b. In the 'Profile Name', enter a brief description (e.g., "ITSP").
 - c. From the 'Extension Coders Group ID', select '2'. This is the Coders Group that you defined for the ITSP in "Step 1: Define Coders Groups" on page 571.
 - d. From the 'Allowed Coders Group ID', select '1'. This is the Allowed Coders Group that you defined for the ITSP in "Step 2: Define Allowed Coders" on page 572.

- e. Click **Submit**.

Figure 8-90: Defining IP Profile for ITSP



Profile ID	2	Profile ID
Profile Name	ITSP	

SBC		
Transcoding Mode	Only if Required	
Extension Coders Group ID	Coders Group 2	Coders Group 2
Allowed Coders Group ID	Coders Group 1	Allowed Coders Group 1
SBC Media Security Behaviour	As Is	
Allowed Coders Mode	Restriction	

8.4.10.5.4 Step 4: Assign IP Profiles to IP Groups

The procedure below describes how to assign the IP Profiles defined in "Step 3: Define IP Profiles" on page 572 to the IP Groups for the LAN users and ITSP. This stage assumes that you have defined an IP Group (e.g., #1) for the LAN Users and an IP Group (e.g., #2) for the ITSP.

➤ **To assign IP Profiles to the IP Groups:**

1. Open the 'IP Group Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**).
2. Assign IP Profile #1 to LAN user IP Group #1:
 - a. From the 'Index' drop-down list, select '1'.
 - b. From the 'IP Profile ID' drop-down list, select '1'. This is the IP Profile that you defined for the LAN users.

- c. Click **Submit**.

Figure 8-91: Assigning IP Profile to LAN Users IP Group

The screenshot displays a configuration window for a SIP user group. At the top, the 'Index' dropdown is set to '1', with a yellow callout box labeled 'Selecting Index 1' pointing to it. Below this, the 'Common Parameters' section is expanded, showing fields for 'Type' (USER), 'Description' (LAN users), 'Proxy Set ID' (empty), 'SIP Group Name' (ip-pbx), 'Contact User' (N/A), and 'IP Profile ID' (1). A yellow callout box labeled 'Selecting IP Profile 1' points to the 'IP Profile ID' dropdown. The 'SRD' field is set to 0, and the 'Media Realm' dropdown is empty. Below the common parameters, the 'Gateway Parameters' section is expanded, showing 'Always Use Route Table' (No), 'Routing Mode' (Not Configured), 'SIP Re-Routing Mode' (Standard), 'Enable Survivability' (Disable), and 'Serving IP Group ID' (empty). At the bottom, the 'SBC Parameters' section is expanded, showing 'Classify By Proxy Set' (Enable), 'Max Number Of Registered Users' (-1), 'Inbound Message Manipulation Set' (-1), and 'Outbound Message Manipulation Set' (-1).

Common Parameters	
Type	USER
Description	LAN users
Proxy Set ID	
SIP Group Name	ip-pbx
Contact User	N/A
IP Profile ID	1
SRD	0
Media Realm	

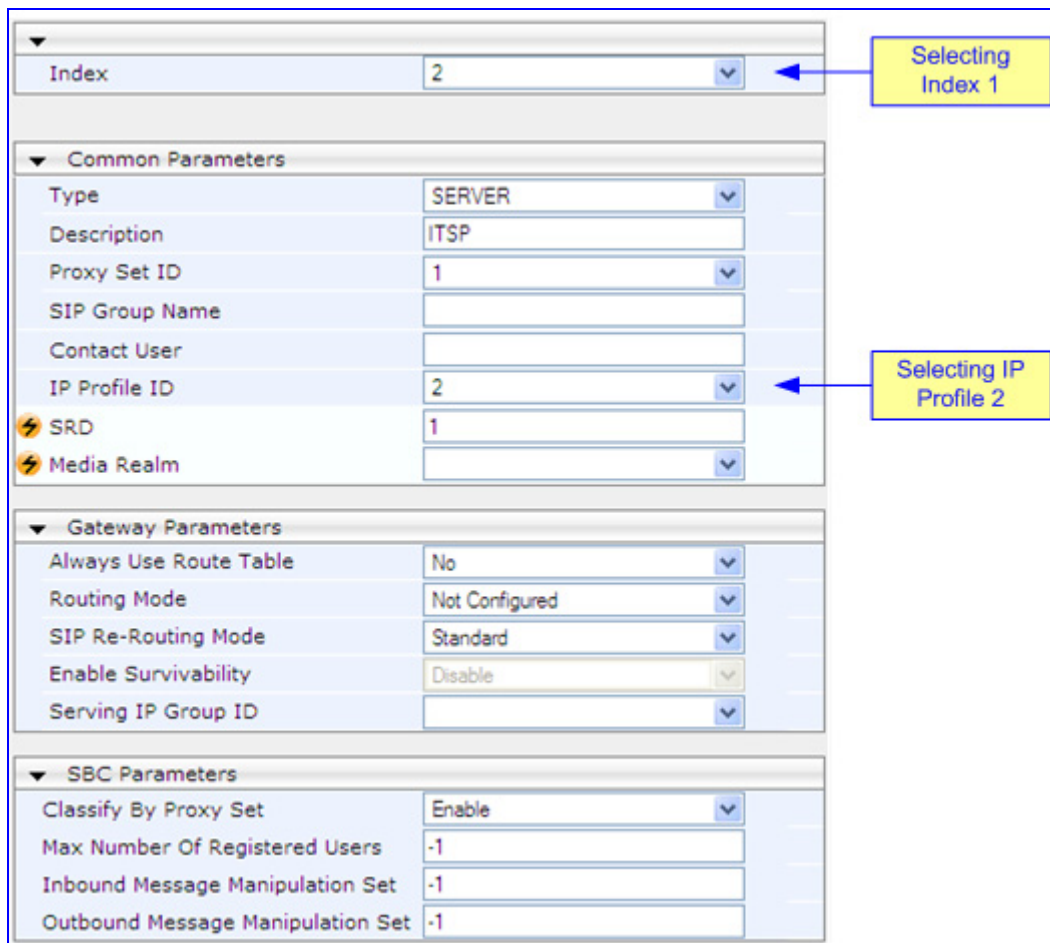
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

SBC Parameters	
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1

3. Assign IP Profile #2 to ITSP IP Group #2:
- From the 'Index' drop-down list, select '2'.
 - From the 'IP Profile ID' drop-down list, select '2'. This is the IP Profile that you defined for the ITSP.

- c. Click **Submit**.

Figure 8-92: Assigning IP Profile to ITSP IP Group



Index	2
-------	---

Common Parameters

Type	SERVER
Description	ITSP
Proxy Set ID	1
SIP Group Name	
Contact User	
IP Profile ID	2
SRD	1
Media Realm	

Gateway Parameters

Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

SBC Parameters

Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
Inbound Message Manipulation Set	-1
Outbound Message Manipulation Set	-1

8.4.10.6 RTP-SRTP Transcoding

This section describes how to configure an RTP-SRTP transcoding scenario. This example is based on the previous examples and only describes the configuration of the transcoding feature itself. It assumes that the other elements such as SRD's and IP Groups have already been configured.

This example assumes the following:

- Device deployed at an enterprise, interfacing between enterprise's LAN IP-PBX and WAN IP-PBX
- LAN IP phones can send and received RTP or SRTP packets
- ITSP can only receive SRTP packets (i.e., RTP packets are dropped)

Therefore, the device must be configured to transcode RTP packets (received from LAN IP phones) to SRTP (for ITSP). This configuration is done by configuring RTP-SRTP transcoding rules for the IP Profiles of LAN users (e.g., IP Profile #1) and ITSP (e.g., IP Profile #2), and then assigning these IP Profiles to the IP Groups of LAN users (e.g., IP Group #1) and ITSP (e.g., IP Group #2).

As the IP Profiles were already assigned to the IP Groups in the previous example, this section only describes the IP Profile configuration.

➤ **To configure RTP-SRTP transcoding:**

1. Open the 'IP Profile Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **IP Profile Settings**).
2. Configure RTP-SRTP transcoding mode for IP Profile #1 (i.e., LAN users):
 - a. From the 'Profile ID' drop-down list, select '1'. This is the IP Profile defined in previous examples for LAN users.
 - b. From the 'SBC Media Security Behaviour', select 'As Is'. This allows the device to simply send the packet as received (RTP or SRTP). In other words, no transcoding is performed for LAN users.
 - c. Click **Submit**.

Figure 8-93: RTP-SRTP Transcoding Mode for LAN Users

The screenshot shows the 'IP Profile Settings' page. The 'Profile ID' is set to '1' and the 'Profile Name' is 'LAN Users'. Under the 'SBC' section, the 'Transcoding Mode' is 'Only if Required', 'Extension Coders Group ID' is 'Coders Group 1', 'Allowed Coders Group ID' is 'None', 'SBC Media Security Behaviour' is 'As Is', and 'Allowed Coders Mode' is 'Restriction'. A yellow callout box labeled 'Selecting Index 1' points to the 'Profile ID' dropdown. Another yellow callout box labeled 'RTP-SRTP Transcoding Mode (None)' points to the 'SBC Media Security Behaviour' dropdown.

3. Configure RTP-to-SRTP transcoding for IP Profile #2 (i.e., ITSP):
 - a. From the 'Profile ID' drop-down list, select '2'.
 - b. From the 'SBC Media Security Behaviour', select 'SRTP'. This ensures that RTP packets received from LAN users are sent to ITSP as SRTP.
 - c. Click **Submit**.

Figure 8-94: RTP-to-SRTP Transcoding for ITSP

The screenshot shows the 'IP Profile Settings' page for Profile ID 2. The 'Profile ID' is set to '2' and the 'Profile Name' is 'ITSP'. Under the 'SBC' section, the 'Transcoding Mode' is 'Only if Required', 'Extension Coders Group ID' is 'Coders Group 2', 'Allowed Coders Group ID' is 'Coders Group 1', 'SBC Media Security Behaviour' is 'SRTP', and 'Allowed Coders Mode' is 'Restriction'. A yellow callout box labeled 'Selecting Index 2' points to the 'Profile ID' dropdown. Another yellow callout box labeled 'Transcoding RTP to SRTP' points to the 'SBC Media Security Behaviour' dropdown.

8.4.10.7 SIP URI Manipulation

This section describes how to configure SBC SIP URI user and host parts manipulation. This example is based on the general scenario described in "General SBC Setup" on page 546.

This example describes how to configure manipulation of the following:

- SIP URI host part: For the SIP INVITE sent from any source destination IP Group (i.e., LAN user IP Group ID #1) to the IP-PBX (i.e., IP Group ID #2), the URI host name is replaced with "ip-pbx" in the outgoing INVITE to the WAN.
- SIP URI user part: For the SIP INVITE containing the destination URI user name prefix "976", sent from the LAN users IP Group #1, the prefix is removed (i.e., "976") in the outgoing INVITE to the WAN.

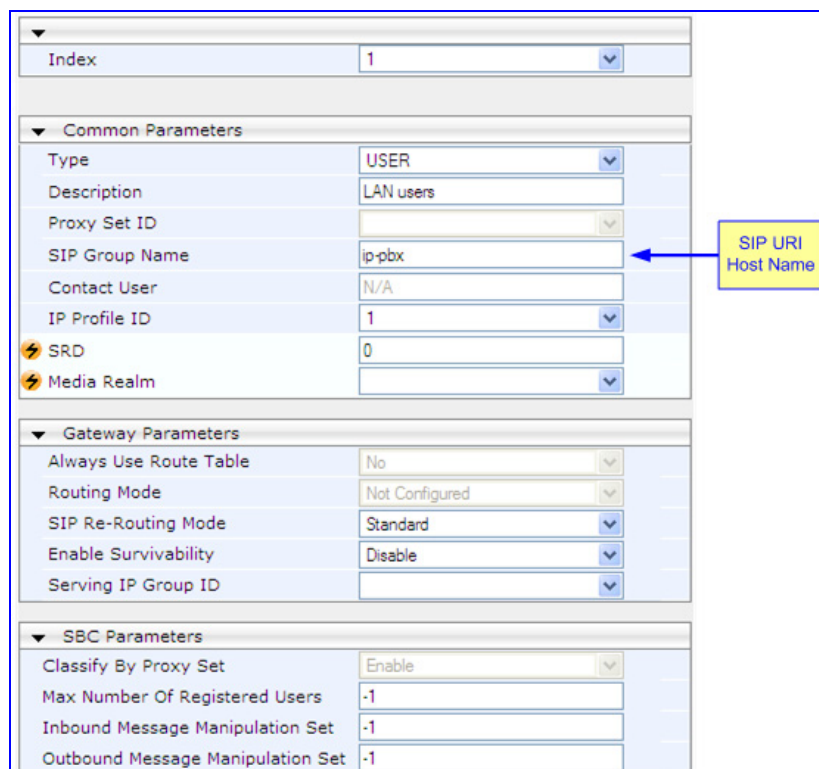
8.4.10.7.1 Step 1: Manipulate SIP URI Host Part

The procedure below describes how to configure a manipulation rule for the SIP URI host part. For this manipulation, the SIP URI host part of SIP messages sent from the LAN IP phones (i.e., IP Group #1), are replaced with the string value "ip-pbx".

➤ To configure manipulation of SIP URI host part:

1. Open the 'IP Group Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**).
2. From the 'Index' drop-down list, select '1'. This is the IP Group representing the LAN IP Phones.
3. In the 'SIP Group Name' field, enter "ip-pbx".

Figure 8-95: Manipulation of SIP URI Host Part



The screenshot shows the 'IP Group Table' configuration page. The 'Index' dropdown is set to '1'. Under the 'Common Parameters' section, the 'SIP Group Name' field is set to 'ip-pbx', which is highlighted by a yellow box and a blue arrow labeled 'SIP URI Host Name'. Other fields include 'Type' (USER), 'Description' (LAN users), 'Contact User' (N/A), 'IP Profile ID' (1), 'SRD' (0), and 'Media Realm'. The 'Gateway Parameters' section includes 'Always Use Route Table' (No), 'Routing Mode' (Not Configured), 'SIP Re-Routing Mode' (Standard), 'Enable Survivability' (Disable), and 'Serving IP Group ID'. The 'SBC Parameters' section includes 'Classify By Proxy Set' (Enable), 'Max Number Of Registered Users' (-1), 'Inbound Message Manipulation Set' (-1), and 'Outbound Message Manipulation Set' (-1).

4. Click **Submit**.

8.4.10.7.2 Step 2: Manipulate SIP URI User Part

The procedure below describes how to configure a manipulation rule for the SIP URI user part. In this manipulation, the destination URI user name prefix "976" in SIP INVITE messages sent from the LAN users IP Group #1 is removed (i.e., "976") in the outgoing INVITE to the WAN IP-PBX.

➤ **To configure manipulation of SIP URI user part:**

1. Open the 'IP2IP Inbound Manipulation' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Manipulations SBC** submenu > **IP to IP Inbound**).
2. From the 'Manipulated URI' drop-down list, select 'Destination'. This indicates that manipulation is done on the destination SIP URI user part.
3. In the 'Source IP Group' field, enter '1'. This is the IP Group of the LAN IP Phones.
4. In the 'Destination Username Prefix' field, enter the destination SIP URI user part prefix that you want manipulated (i.e., "976").
5. From the 'Request Type' drop-down list, select 'INVITE' to apply this rule only to SIP INVITE messages.
6. In the 'Remove From Left' field, enter the number of digits that you want removed from the prefix (i.e., '3', to remove "976").

Figure 8-96: Manipulation of SIP URI User Part

Index	Is Additional Manipulation	Manipulated URI	Manipulation Purpose	Source IP Group	Source Username Prefix
1	<input type="radio"/>	Destination	Normal	1	*

Source Host	Destination Username Prefix	Destination Host	Request Type
*	976	*	INVITE

Remove From Left	Remove From Right	Leave From Right	Prefix to Add	Suffix to Add
3	0	255		

7. Click **Apply**.

8.4.10.8 SIP Header Manipulation

This section provides an example on how to configure a SIP message manipulation rule that adds a P-Asserted-Identity header with the user part from the From header, to all received (inbound) INVITE messages. For example, if the device receives an INVITE from user "1000", it adds a P-Asserted-Identity header to the sent INVITE with the value "1000@msbg.com". Therefore, the caller ID displayed to the remote User Agent is "1000@msbg.com".


```

From: <sip:1000@10.8.5.41>;tag=1c1286571572
To: <sip:FEU8-999-1@WANWAN>
Call-ID: 128652844814102010161846@212.25.26.70
CSeq: 1 INVITE
Contact: <sip:FEU3-998-2@212.25.26.70:5060>
Supported: em,100rel,timer,replaces,path,resource-priority,sdp-anat
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 800/v.6.20A.004
P-Asserted-Identity: <sip:1000@MSBG.com>

```

To configure this SIP message manipulation, you need to do the following:

1. Add a SIP message manipulation rule in the Message Manipulation page (see "Step 1: Add SIP Message Manipulation Rule" on page 580).
2. Assign the SIP message manipulation rule index to the IP Group from where the INVITE is received (see "Step 2: Assign Message Manipulation Rule to IP Group" on page 581).

8.4.10.8.1 Step 1: Add SIP Message Manipulation Rule

The procedure below describes how to add the SIP message manipulation rule required in the example.

➤ To add a SIP message manipulation rule:

1. Open the 'Message Manipulations' page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Manipulations SBC** submenu > **Message**).
2. In the Add field, enter any index number for the manipulation rule, and then click **Add**; an empty index row is added to the table, ready to be configured.
3. Configure the rule as follows:
 - **Message Type:** enter the value, invite
 - **Action Subject:** enter the value, header.p-asserted-identity
 - **Action Type:** select 'Add'
 - **Action Value:** enter the value, '<sip:' + header.from.url.user + '@msbg.com>', where:
 - ♦ header.from.url.user = adds the From header's user part to that of the P-Asserted-Identity header
 - ♦ @msbg.com = adds msbg.com to the host part of the P-Asserted-Identity header
 - **Row Rule:** leave as default ('Use Current Condition')

The manipulation rule is shown in the figure below:

Figure 8-97: SIP Header Manipulation Example

Index	Manipulation Set ID	Message Type	Condition	Action Subject
1	0	invite		header.P-Asserted-Identity

Action Type	Action Value	Row Role
Add	'< sip:' + header.from.uri.user +'	Use Current Condition

4. Click **Apply**.

8.4.10.8.2 Step 2: Assign Message Manipulation Rule to IP Group

The procedure below describes how to assign the configured SIP message manipulation rule (rule #1) to the IP Group belonging to the LAN users.

➤ **To add the SIP message manipulation rule to the IP Group:**

1. Open the 'IP Group Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**).
2. In the 'Inbound Message Manipulation Set' field, enter "1" to assign the Message Manipulation Rule #1 that you configured in "Step 1: Add SIP Message Manipulation Rule" on page 580.

Figure 8-98: Assigning Manipulation Rule to IP Group

The screenshot shows the 'IP Group Table' configuration page. The 'Index' is set to 1. Under 'Common Parameters', 'Type' is 'USER', 'Description' is 'LAN_users', 'Proxy Set ID' is empty, 'SIP Group Name' is empty, 'Contact User' is 'N/A', 'SRD' is 0, 'Media Realm' is empty, and 'IP Profile ID' is 0. Under 'Gateway Parameters', 'Always Use Route Table' is 'No', 'Routing Mode' is 'Not Configured', 'SIP Re-Routing Mode' is 'Standard', 'Enable Survivability' is 'Disable', and 'Serving IP Group ID' is empty. Under 'SBC Parameters', 'Classify By Proxy Set' is 'Enable', 'Max Number Of Registered Users' is -1, 'Inbound Message Manipulation Set' is 1, and 'Outbound Message Manipulation Set' is -1. A yellow callout box labeled 'Manipulation Rule Index' points to the 'Inbound Message Manipulation Set' field.

3. Click **Submit**.

8.5 Stand-Alone Survivability (SAS) Application

The device's Stand-Alone Survivability (SAS) feature ensures telephony communication continuity (survivability) for enterprises using hosted IP services (such as IP Centrex) or IP-PBX in cases of failure of these entities. In case of failure of the IP Centrex, IP-PBX servers (or even WAN connection and access Internet modem), the enterprise typically loses its internal telephony service at any branch, between its offices, and with the external environment. In addition, typically these failures lead to the inability to make emergency calls (e.g., 911 in North America). Despite these possible points of failure, the device's SAS feature ensures that the enterprise's telephony services (e.g., SIP IP phones or soft phones) are maintained, by routing calls to the PSTN (i.e., providing PSTN fallback).



Notes:

- The SAS application is available only if the device is installed with the SAS Software Upgrade Key.
- 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.

8.5.1 SAS Operating Modes

The device's SAS application can be implemented in one of the following main modes:

- **Outbound Proxy:** In this mode, SAS receives SIP REGISTER requests from the enterprise's UAs and forwards these requests to the external proxy (i.e., outbound proxy). When a connection with the external proxy fails, SAS enters SAS emergency state and serves as a proxy, by handling internal call routing for the enterprise's UAs - routing calls between UAs and if setup, routing calls between UAs and the PSTN. For a detailed description, see "SAS Outbound Mode" on page 583.
- **Redundant Proxy:** In this mode, the enterprise's UAs register with the external proxy and establish calls directly through the external proxy, without traversing SAS (or the device per se'). Only when connection with the proxy fails, do the UAs register with SAS, serving now as the UAs redundant proxy. SAS then handles the calls between UAs, and between the UAs and the PSTN (if setup). This mode is operational only during SAS in emergency state. This mode can be implemented, for example, for proxies that accept only SIP messages that are sent directly from the UAs. For a detailed description, see "SAS Redundant Mode" on page 584.



Note: It is recommended to implement the SAS outbound mode.

8.5.1.1 SAS Outbound Mode

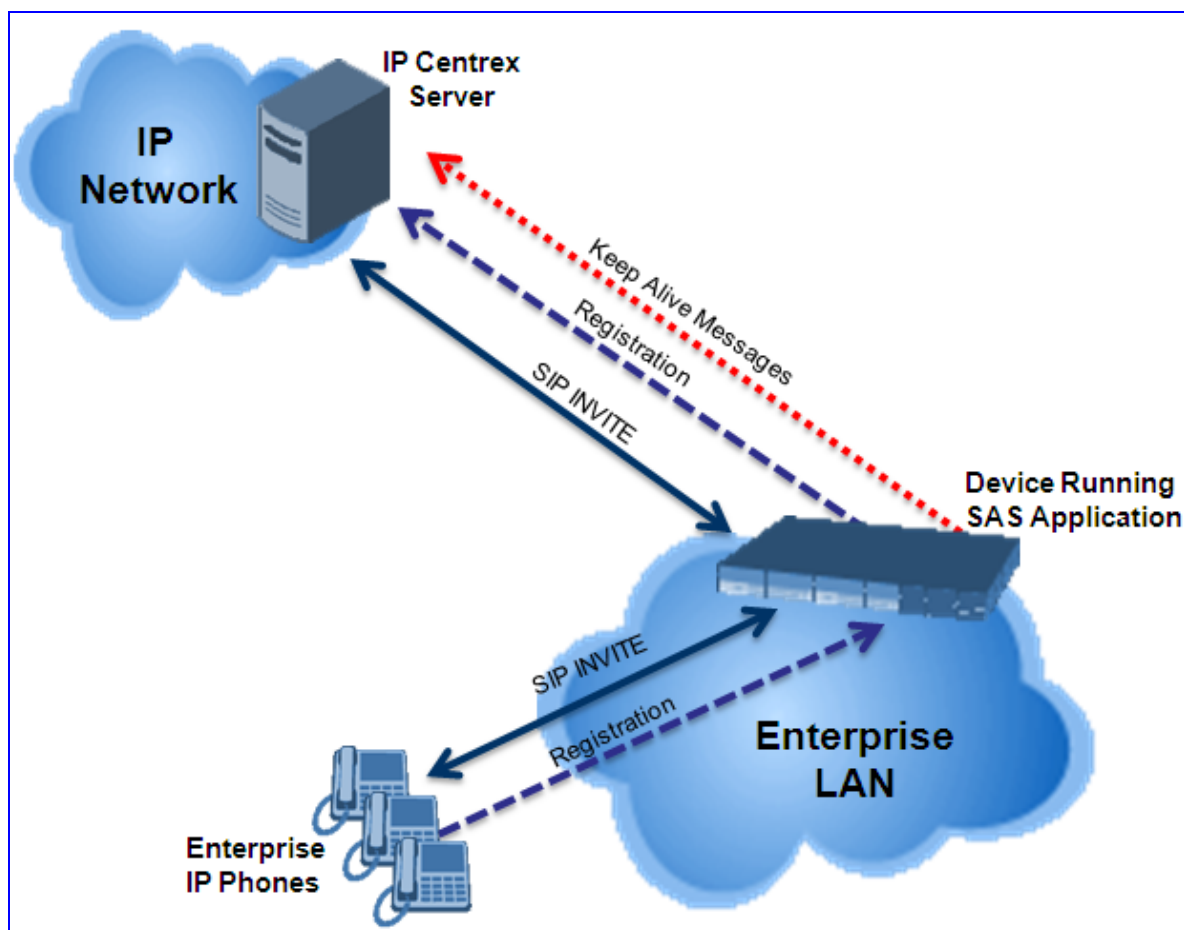
This section describes the SAS outbound mode, which includes the following states:

- Normal state (see "Normal State" on page 583)
- Emergency state (see "Emergency State" on page 584)

8.5.1.1.1 Normal State

In normal state, SAS receives REGISTER requests from the enterprise's UAs and forwards them to the external proxy (i.e., outbound proxy). Once the proxy replies with a SIP 200 OK, the device records the Contact and address of record (AOR) of the UAs in its internal SAS registration database. Therefore, in this mode, SAS maintains a database of all the registered UAs in the network. In addition, SAS continuously maintains a keep-alive mechanism toward the external proxy, using SIP OPTIONS messages. The figure below illustrates the operation of SAS outbound mode in normal state:

Figure 8-99: SAS Outbound Mode in Normal State (Example)



8.5.1.1.2 Emergency State

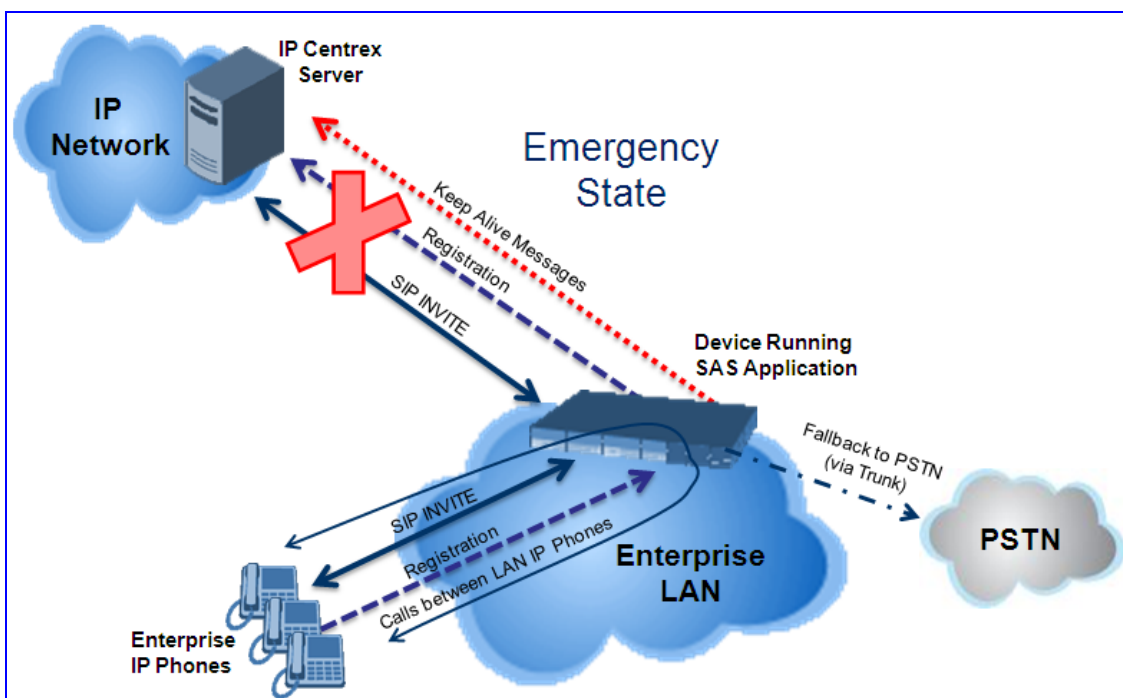
When a connection with the external proxy fails (detected by the device's keep-alive messages), the device enters SAS emergency state. The device serves as a proxy for the UAs, by handling internal call routing of the UAs (within the LAN enterprise).

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 589.

The figure below illustrates the operation of SAS outbound mode in emergency state:

Figure 8-100: 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 586.

8.5.1.2 SAS Redundant Mode

In SAS redundant mode, the enterprise's UAs register with the external proxy and establish calls directly through it, without traversing SAS (or the device per se'). Only when connection with the proxy fails, do the UAs register with SAS, serving now as the UAs redundant proxy. SAS then handles the calls between UAs, and between the UAs and the PSTN (if setup).

This mode is operational only during SAS in emergency state.

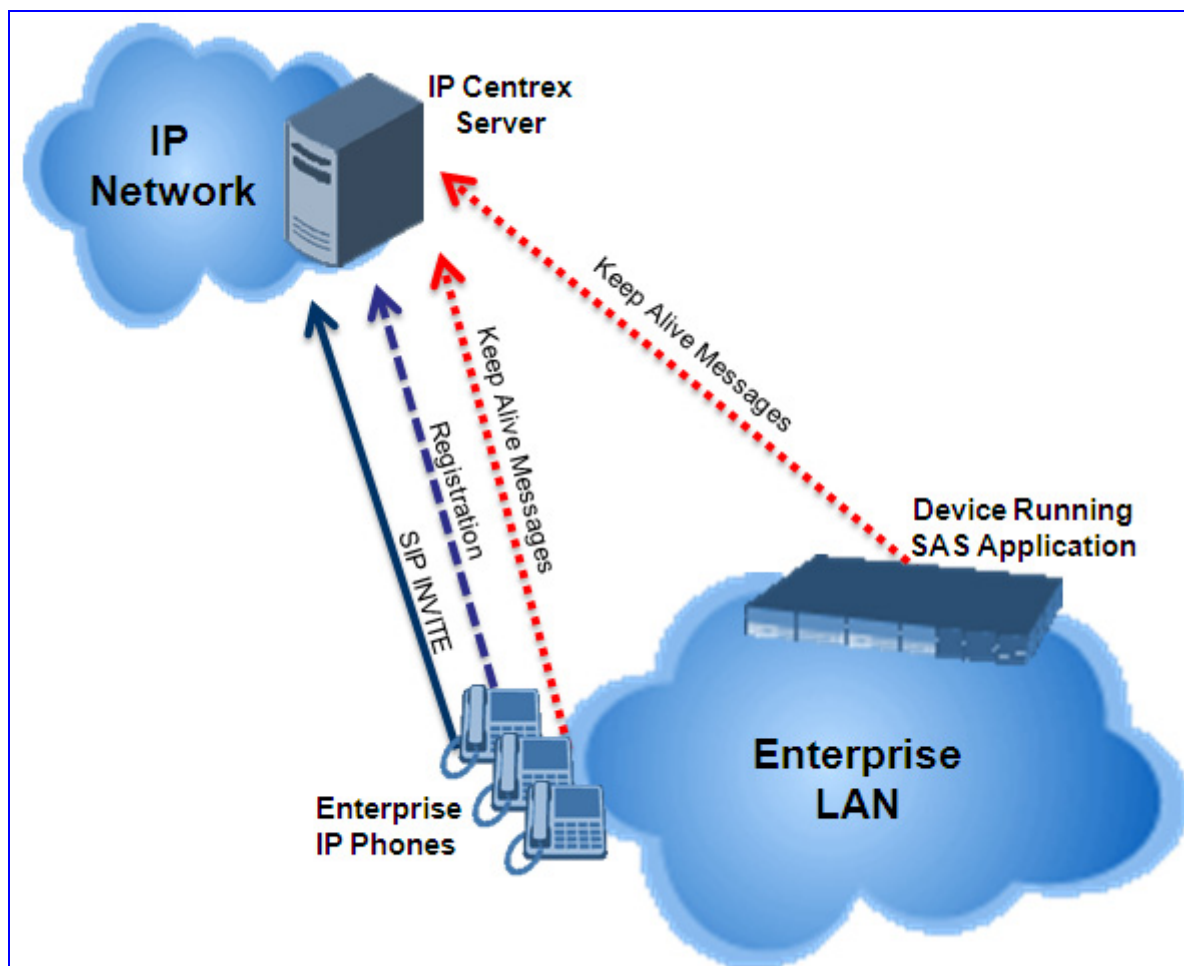


Note: In this SAS deployment, the UAs (e.g., IP phones) must support configuration for primary and secondary proxy servers (i.e., proxy redundancy), as well as homing. Homing allows the UAs to switch back to the primary server from the secondary proxy once the connection to the primary server returns (UAs check this using keep-alive messages to the primary server). If homing is not supported by the UAs, you can configure SAS to ignore messages received from UAs in normal state (the 'SAS Survivability Mode' parameter must be set to 'Always Emergency' / 2) and thereby, “force” the UAs to switch back to their primary proxy.

8.5.1.2.1 Normal State

In normal state, the UAs register and operate directly with the external proxy.

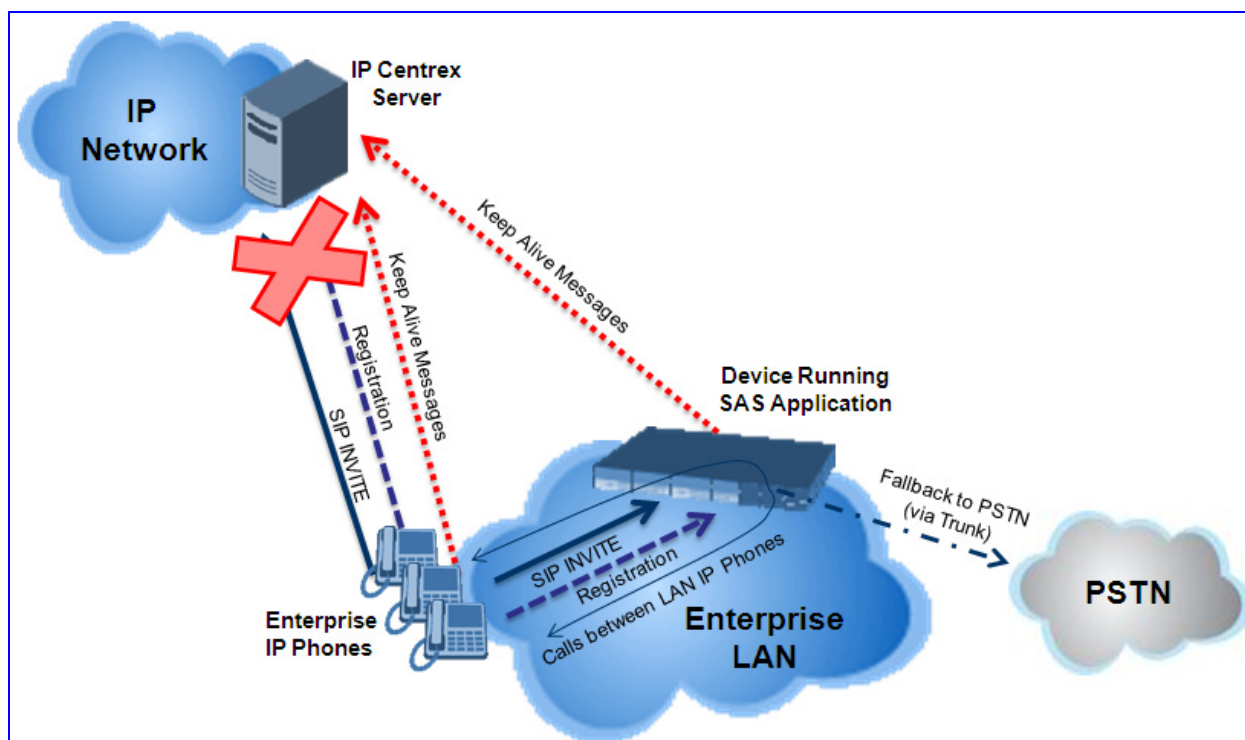
Figure 8-101: SAS Redundant Mode in Normal State (Example)



8.5.1.2.2 Emergency State

If the UAs detect that their primary (external) proxy does not respond, they immediately register to SAS and start routing calls to it.

Figure 8-102: SAS Redundant Mode in Emergency State (Example)



8.5.1.2.3 Exiting Emergency and Returning to Normal State

Once the connection with the primary proxy is re-established, the following occurs:

- **UAs:** switch back to operate with the primary proxy.
- **SAS:** ignores REGISTER requests from the UAs, forcing the UAs to switch back to the primary proxy.

Note: This is applicable only if the 'SAS Survivability Mode' parameter is set to 'Always Emergency' (2).

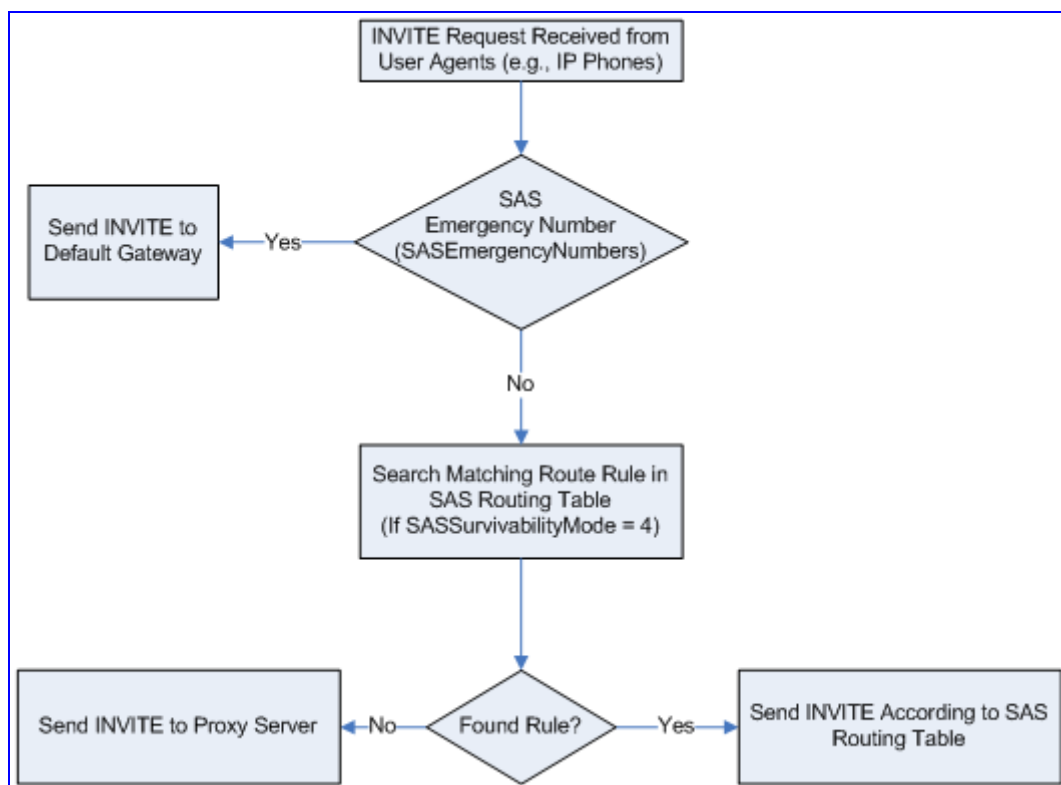
8.5.2 SAS Routing

This section provides flowcharts describing the routing logic for SAS in normal and emergency states.

8.5.2.1 SAS Routing in Normal State

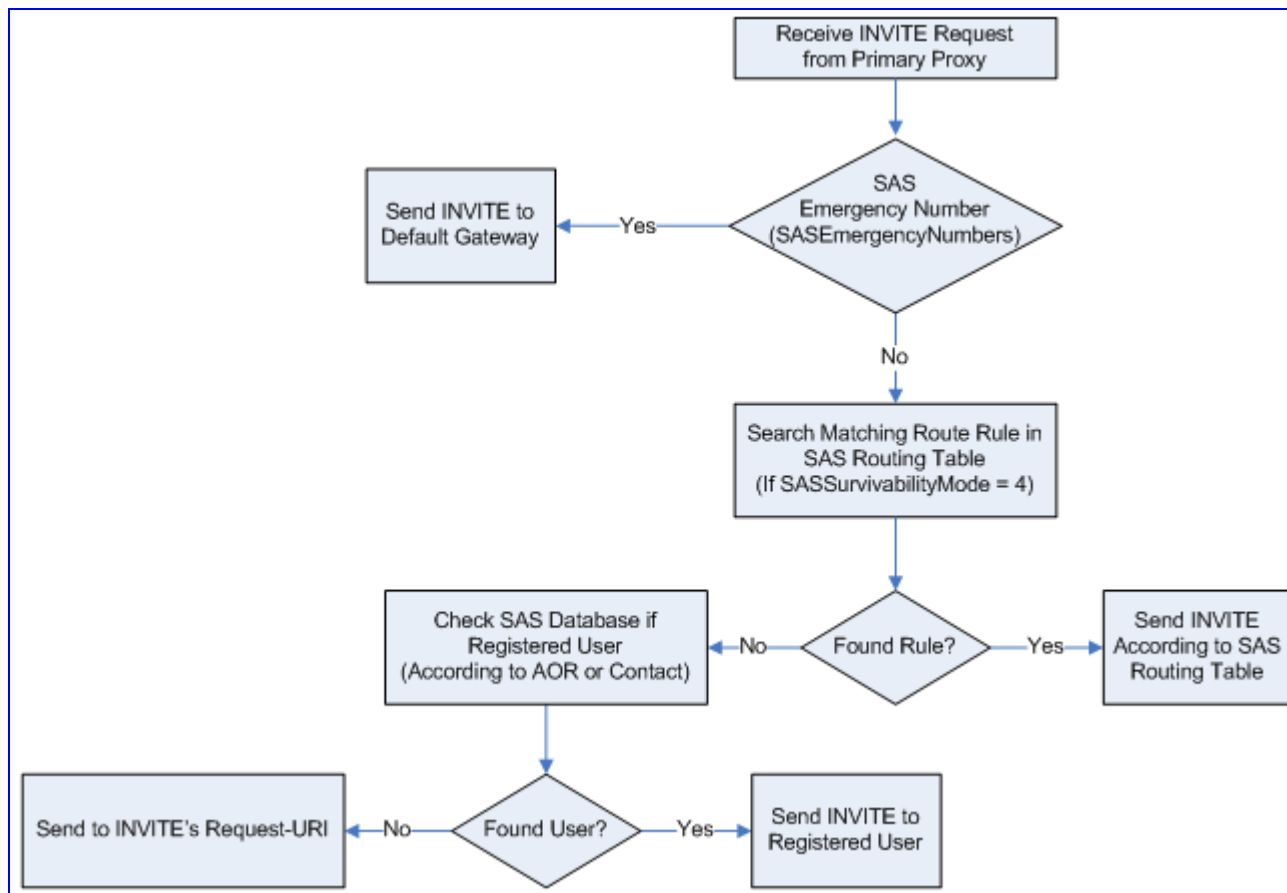
The flowchart below displays the routing logic for SAS in normal state for INVITE messages received from the UAs:

Figure 8-103: Flowchart of INVITE from UA's in SAS Normal State



The flowchart below displays the routing logic for SAS in normal state for INVITE messages received from the external proxy:

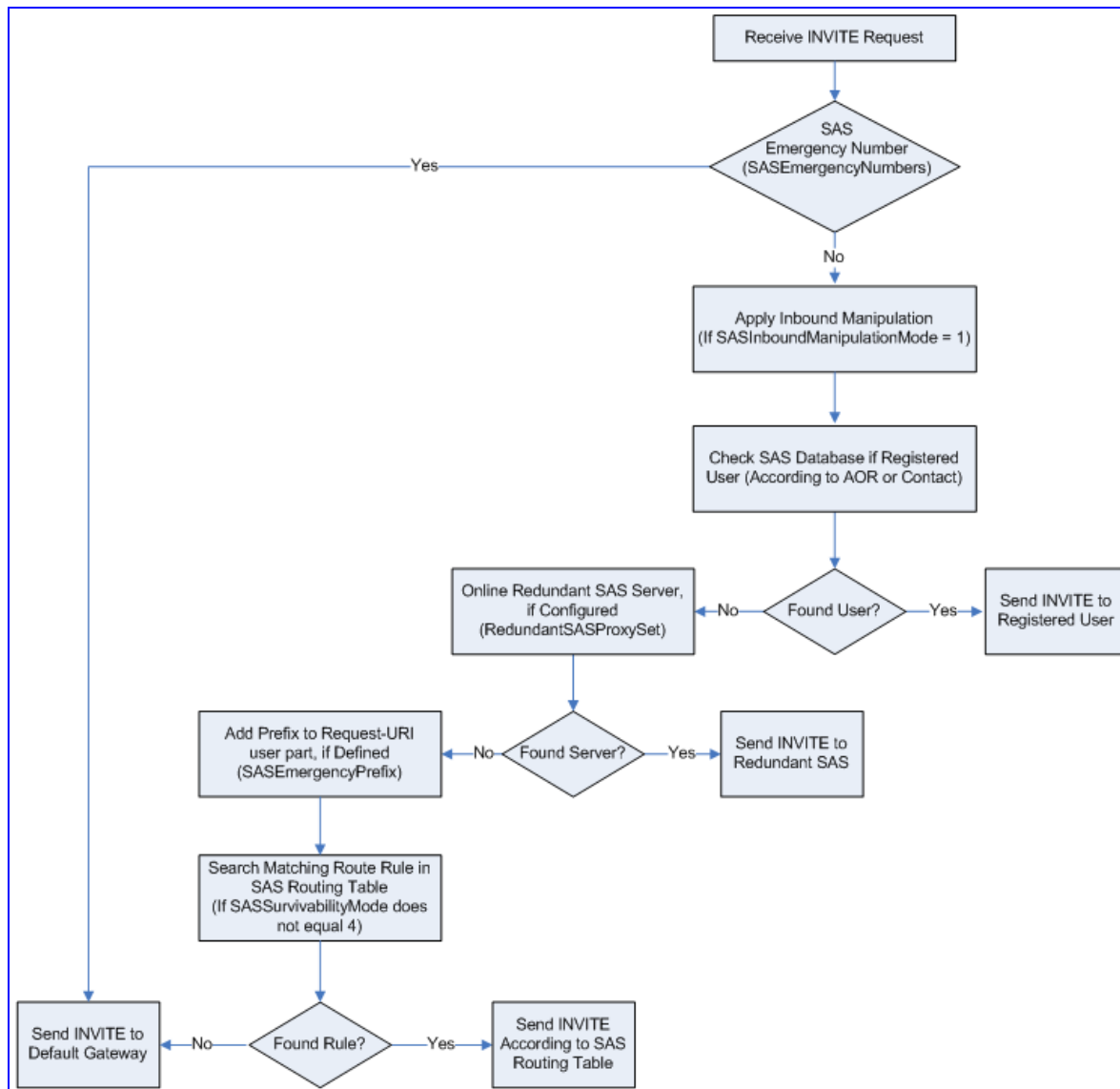
Figure 8-104: Flowchart of INVITE from Primary Proxy in SAS Normal State



8.5.2.2 SAS Routing in Emergency State

The flowchart below shows the routing logic for SAS in emergency state:

Figure 8-105: Flowchart for SAS Emergency State



8.5.3 SAS Configuration

SAS supports various configuration possibilities, depending on how the device is deployed in the network and the network architecture requirements. This section provides step-by-step procedures on configuring the SAS application, using the device's Web interface.

The SAS configuration includes the following:

- General SAS configuration that is common to all SAS deployment types (see "General SAS Configuration" on page 590)
- SAS outbound mode (see "Configuring SAS Outbound Mode" on page 593)
- SAS redundant mode (see "Configuring SAS Redundant Mode" on page 594)
- Gateway and SAS applications deployed together (see "Configuring Gateway Application with SAS" on page 594)
- Optional, advanced SAS features (see "Advanced SAS Configuration" on page 598)

8.5.3.1 General SAS Configuration

This section describes the general configuration required for the SAS application. This configuration is applicable to all SAS modes.

8.5.3.1.1 Enabling the SAS Application

Before you can configure SAS, you need to enable the SAS application on the device. Once enabled, the device's Web interface provides the SAS pages for configuring SAS.

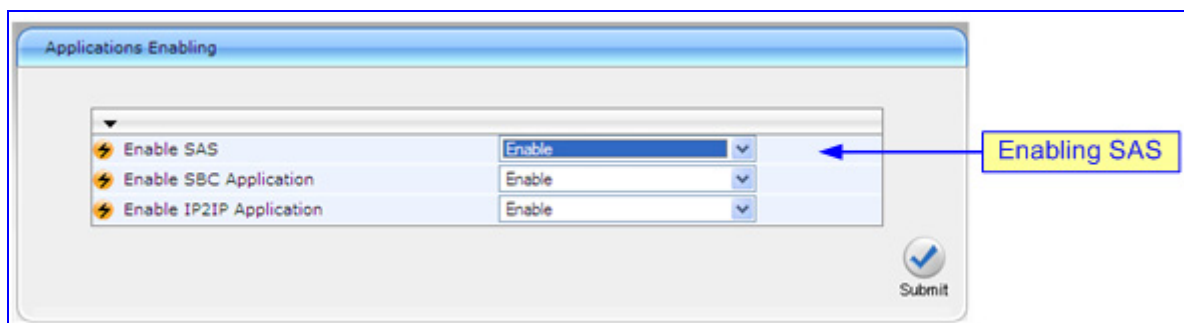


Note: The SAS application is available only if the device is installed with the SAS Software Upgrade Key. If your device is not installed with the SAS feature, contact your AudioCodes representative.

➤ **To enable the SAS application:**

1. Open the 'Applications Enabling' page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).
2. From the 'Enable SAS' drop-down list, select 'Enable'.

Figure 8-106: Enabling the SAS Application



3. Click **Submit**.
4. Save the changes to the flash memory with a device reset; after the device resets, the SAS menu appears and you can now begin configuring the SAS application.

8.5.3.1.2 Configuring Common SAS Parameters

The procedure below describes how to configure SAS settings that are common to all SAS modes. This includes various SAS parameters as well as configuring the Proxy Set for the SAS proxy (if required). The SAS Proxy Set ID defines the address of the UAs' external proxy.

➤ **To configure common SAS settings:**

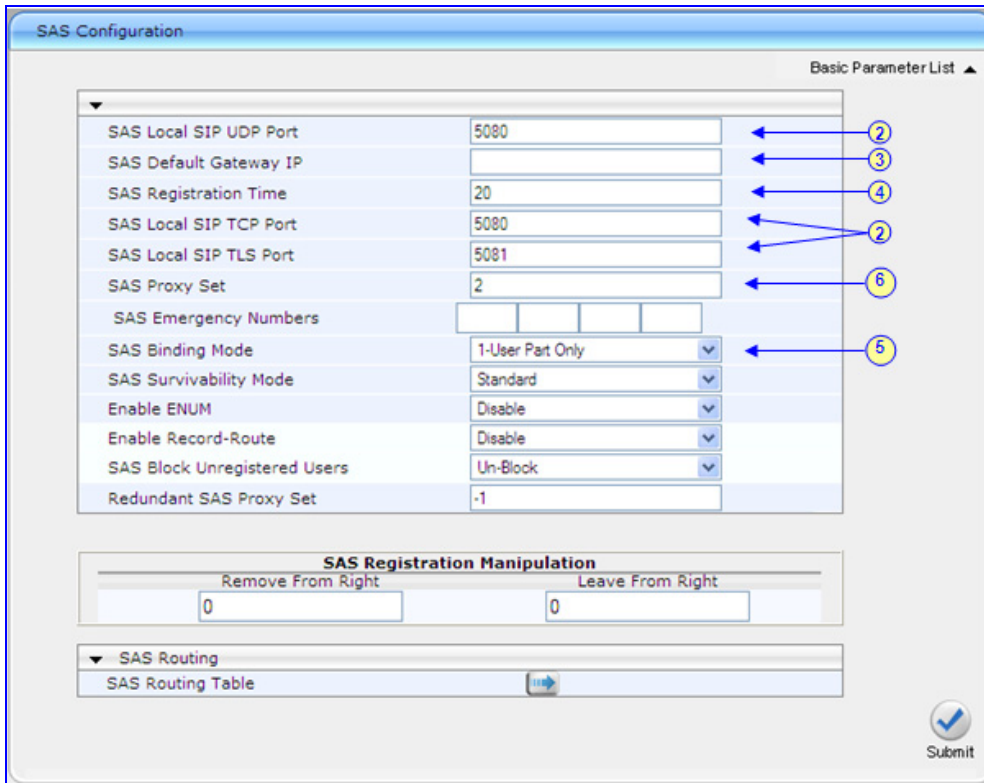
1. Open the 'SAS Configuration' page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. Define the port used for sending and receiving SAS messages. This can be any of the following port types:
 - UDP port - defined in the 'SAS Local SIP UDP Port' field
 - TCP port - defined in the 'SAS Local SIP TCP Port' field
 - TLS port - defined in the 'SAS Local SIP TLS Port' field



Note: This SAS port must be different than the device's local gateway port (i.e., that defined for the 'SIP UDP/TCP/TLS Local Port' parameter in the 'SIP General Parameters' page - **Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

3. In the 'SAS Default Gateway IP' field, define the IP address and port (in the format *x.x.x.x:port*) of the device (i.e., Gateway application). Note that the port of the device is defined by the parameter 'SIP UDP Local Port' (refer to the note in Step 2 above).
4. In the 'SAS Registration Time' field, define the value for the SIP Expires header, which is sent in the 200 OK response to an incoming REGISTER message when SAS is in emergency state.
5. From the 'SAS Binding Mode' drop-down list, select the database binding mode:
 - **0-URI:** If the incoming AOR in the REGISTER request uses a 'tel:' URI or 'user=phone', the binding is done according to the Request-URI user part only. Otherwise, the binding is done according to the entire Request-URI (i.e., user and host parts - user@host).
 - **1-User Part Only:** Binding is done according to the user part only.

You must select '1-User Part Only' in cases where the UA sends REGISTER messages as SIP URI, but the INVITE messages sent to this UA include a Tel URI. For example, when the AOR of an incoming REGISTER is sip:3200@domain.com, SAS adds the entire SIP URI (e.g., sip:3200@domain.com) to its database (when the parameter is set to '0-URI'). However, if a subsequent Request-URI of an INVITE message for this UA arrives with sip:3200@10.1.2.3 user=phone, SAS searches its database for "3200", which it does not find. Alternatively, when this parameter is set to '1-User Part Only', then upon receiving a REGISTER message with sip:3200@domain.com, SAS adds only the user part (i.e., "3200") to its database. Therefore, if a Request-URI of an INVITE message for this UA arrives with sip:3200@10.1.2.3 user=phone, SAS can successfully locate the UA in its database.

Figure 8-107: Configuring Common Settings


The screenshot shows the 'SAS Configuration' window with a 'Basic Parameter List' tab. The settings are as follows:

Parameter	Value
SAS Local SIP UDP Port	5080
SAS Default Gateway IP	
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	2
SAS Emergency Numbers	
SAS Binding Mode	1-User Part Only
SAS Survivability Mode	Standard
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Un-Block
Redundant SAS Proxy Set	-1

Below the main list is the 'SAS Registration Manipulation' section with 'Remove From Right' and 'Leave From Right' fields, both set to 0. At the bottom is the 'SAS Routing' section with a 'SAS Routing Table' field. A 'Submit' button is located at the bottom right.

6. In the 'SAS Proxy Set' field, enter the Proxy Set used for SAS. The SAS Proxy Set must be defined only for the following SAS modes:

- **Outbound mode:** In SAS normal state, SAS forwards REGISTER and INVITE messages received from the UAs to the proxy servers defined in this Proxy Set.
- **Redundant mode and only if UAs don't support homing:** SAS sends keep-alive messages to this proxy and if it detects that the proxy connection has resumed, it ignores the REGISTER messages received from the UAs, forcing them to send their messages directly to the proxy.

If you define a SAS Proxy Set ID, you must configure the Proxy Set as described in Step 8 below.

7. Click **Submit** to apply your settings.
8. If you defined a SAS Proxy Set ID in Step 6 above, then you must configure the SAS Proxy Set ID:
 - a. Open the 'Proxy Sets Table' page (**Configuration** tab > **VoIP** menu > **Control Networks** > **Proxy Set Table**).
 - b. From the 'Proxy Set ID' drop-down list, select the required Proxy Set ID.


Notes:

- The selected Proxy Set ID number must be the same as that specified in the 'SAS Proxy Set' field in the 'SAS Configuration' page (see Step 6).
- Do not use Proxy Set ID 0.

- a. 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 8-108: Defining UAs' Proxy Server

Proxy Sets Table

Proxy Set ID: 2

	Proxy Address	Transport Type
1	10.15.4.52	TLS
2		
3		
4		
5		

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

Proxy Load Balancing: Round Robin

- c. Click **Submit** to apply your settings.

8.5.3.2 Configuring SAS Outbound Mode

This section describes how to configure the SAS outbound mode. These settings are in addition to the ones described in "Configuring Common SAS Parameters" on page 591.



Note: The VoIP CPEs (such as IP phones or residential gateways) need to be defined so that their proxy and registrar destination addresses and ports are the same as that configured for the device's SAS IP address and SAS local SIP port. In some cases, on the UAs, it is also required to define SAS as their outbound proxy, meaning that messages sent by the UAs include the host part of the external proxy, but are sent (on Layer 3/4) to the IP address / UDP port of SAS.

➤ **To configure SAS outbound mode:**

1. Open the 'SAS Configuration' page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the 'SAS Survivability Mode' drop-down list, select 'Standard'.
3. Click **Submit**.

8.5.3.3 Configuring SAS Redundant Mode

This section describes how to configure the SAS redundant mode. These settings are in addition to the ones described in "Configuring Common SAS Parameters" on page 591.



Note: The VoIP CPEs (such as IP phones or residential gateways) need to be defined so that their primary proxy is the external proxy, and their redundant proxy destination addresses and port is the same as that configured for the device's SAS IP address and SAS SIP port.

➤ **To configure SAS redundant mode:**

1. Open the 'SAS Configuration' page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the 'SAS Survivability Mode' drop-down list, select one of the following, depending on whether the UAs support homing (i.e., they always attempt to operate with the primary proxy, and if using the redundant proxy, they switch back to the primary proxy whenever it's available):
 - **UAs support homing:** Select 'Always Emergency'. This is because SAS does not need to communicate with the primary proxy of the UAs; SAS serves only as the redundant proxy of the UAs. When the UAs detect that their primary proxy is available, they automatically resume communication with it instead of with SAS.
 - **UAs do not support homing:** Select 'Ignore REGISTER'. SAS uses the keep-alive mechanism to detect availability of the primary proxy (defined by the SAS Proxy Set). If the connection with the primary proxy resumes, SAS ignores the messages received from the UAs, forcing them to send their messages directly to the primary proxy.
3. Click **Submit**.

8.5.3.4 Configuring Gateway Application with SAS

If you want to run both the Gateway and SAS applications on the device, the configuration described in this section is required. The configuration steps depend on whether the Gateway application is operating with SAS in outbound mode or SAS in redundant mode.



Note: The Gateway application must use the same SAS operation mode as the SIP UAs. For example, if the UAs use the SAS application as a redundant proxy (i.e., SAS redundancy mode), then the Gateway application must do the same.

8.5.3.4.1 Gateway with SAS Outbound Mode

The procedure below describes how to configure the Gateway application with SAS outbound mode.

➤ **To configure Gateway application with SAS outbound mode:**

1. Define the proxy server address for the Gateway application:
 - a. Open the 'Proxy & Registration' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).
 - b. From the 'Use Default Proxy' drop-down list, select 'Yes'.

Figure 8-109: 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 591).

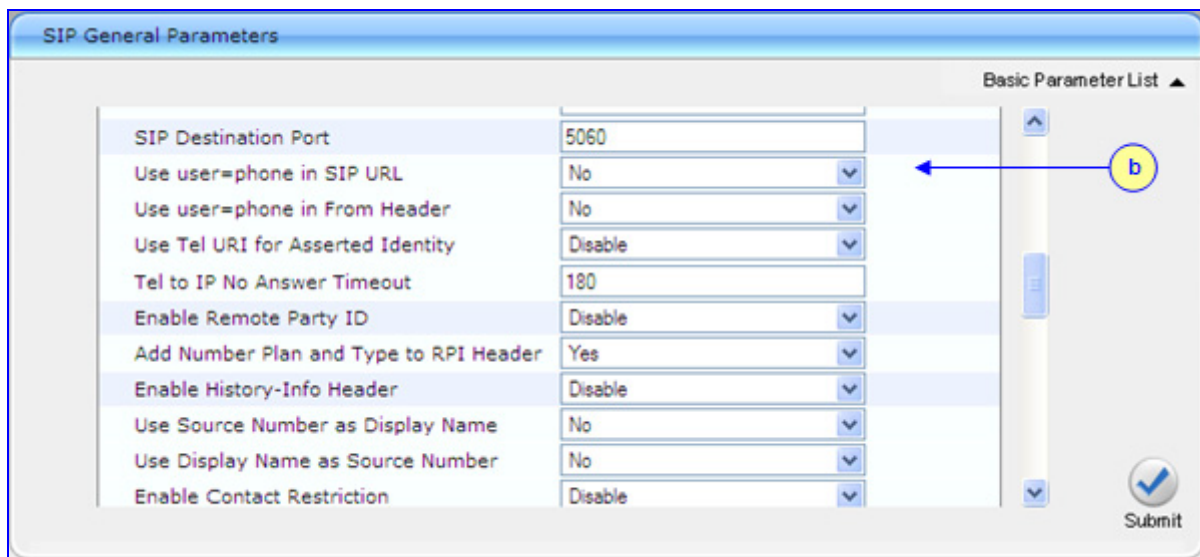
Figure 8-110: Defining Proxy Server for Gateway Application

	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 to not use *user=phone* in the SIP URL and therefore, REGISTER and INVITE messages use SIP URI. (By default, REGISTER messages are sent with *sip uri* and INVITE messages with *tel uri*.)

Figure 8-111: Disabling user=phone in SIP URL



The screenshot shows the 'SIP General Parameters' configuration window. It contains a list of parameters with their current values and dropdown menus. The parameter 'Use user=phone in SIP URL' is highlighted, and a blue arrow labeled 'b' points to its dropdown menu, which is currently set to 'No'. Other parameters include 'SIP Destination Port' (5060), '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), and 'Enable Contact Restriction' (Disable). A 'Submit' button is at the bottom right.

- c. Click **Submit**.

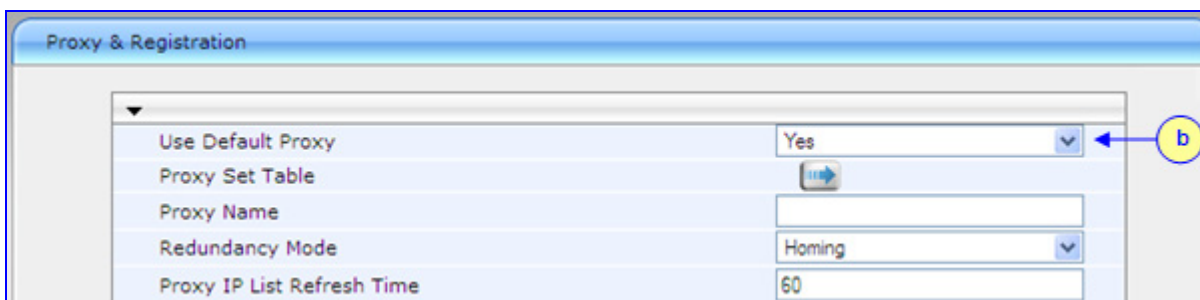
8.5.3.4.2 Gateway with SAS Redundant Mode

The procedure below describes how to configure the Gateway application with SAS redundant mode.

- **To configure Gateway application with SAS redundant mode:**

1. Define the proxy servers for the Gateway application:
 - a. Open the 'Proxy & Registration' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).
 - b. From the 'Use Default Proxy' drop-down list, select 'Yes'.

Figure 8-112: Enabling Proxy Server for Gateway Application



The screenshot shows the 'Proxy & Registration' configuration window. It contains a list of parameters with their current values and dropdown menus. The parameter 'Use Default Proxy' is highlighted, and a blue arrow labeled 'b' points to its dropdown menu, which is currently set to 'Yes'. Other parameters include 'Proxy Set Table' (with a button), 'Proxy Name' (text field), 'Redundancy Mode' (Homing), and 'Proxy IP List Refresh Time' (60).

- 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 591).
- h. From the 'Proxy Redundancy Mode' drop-down list, select 'Homing'.

Figure 8-113: Defining Proxy Servers for Gateway Application

- i. Click **Submit**.
2. Disable the use of *user=phone* in the SIP URL:
 - a. Open the 'SIP General Parameters' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).
 - b. From the 'Use *user=phone* in SIP URL' drop-down list, select 'No'. This instructs the Gateway application to not use *user=phone* in SIP URL and therefore, REGISTER and INVITE messages use SIP URI. (By default, REGISTER messages are sent with *sip uri* and INVITE messages with *tel uri*.)

Figure 8-114: Disabling *user=phone* in SIP URL

- c. Click **Submit**.

8.5.3.5 Advanced SAS Configuration

This section describes the configuration of advanced SAS features that can be optionally implemented in your SAS deployment:

- Manipulating incoming SAS Request-URI user part of REGISTER message (see "Manipulating URI user part of Incoming REGISTER" on page 598)
- Manipulating destination number of incoming SAS INVITE messages (see "Manipulating Destination Number of Incoming INVITE" on page 600)
- Defining SAS routing rules based on the SAS Routing table (see "SAS Routing Based on SAS Routing Table" on page 601)
- Blocking unregistered SAS UA's (see "Blocking Calls from Unregistered SAS Users" on page 602)
- Defining SAS emergency calls (see "Configuring SAS Emergency Calls" on page 602)
- Adding SIP Record-Route header to INVITE messages (see "Adding SIP Record-Route Header to SIP INVITE" on page 603)
- Replacing SIP Contact header (see "Replacing Contact Header for SIP Messages" on page 604)

8.5.3.5.1 Manipulating URI user part of Incoming REGISTER

There are scenarios in which the UAs register to the proxy server with their full phone number (for example, "976653434"), but can receive two types of INVITE messages (calls):

- INVITES whose destination is the UAs' full number (when the call arrives from outside the enterprise)
- INVITES whose destination is the last four digits of the UAs' phone number ("3434" in our example) when it is an internal call within the enterprise

Therefore, it is important that the device registers the UAs in the SAS registered database with their extension numbers (for example, "3434") in addition to their full numbers. To do this, you can define a manipulation rule to manipulate the SIP Request-URI user part of the AOR (in the To header) in incoming REGISTER requests. Once manipulated, it is saved in this manipulated format in the SAS registered users database in addition to the original (un-manipulated) AOR.

For example: Assume the following incoming REGISTER message is received and that you want to register in the SAS database the UA's full number as well as the last four digits from the right of the SIP URI user part:

```
REGISTER sip:10.33.38.2 SIP/2.0
Via: SIP/2.0/UDP 10.33.4.226:5050;branch=z9hG4bKac10827
Max-Forwards: 70
From: <sip: 976653434@10.33.4.226>;tag=1c30219
To: <sip: 976653434@10.33.4.226>
Call-ID: 16844@10.33.4.226
CSeq: 1 REGISTER
Contact: <sip: 976653434@10.10.10.10:5050>;expires=180
Allow:
REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE,
UPDATE
Expires: 180
User-Agent: Audiocodes-Sip-Gateway-/v.
Content-Length: 0
```

After manipulation, SAS registers the user in its database as follows:

- **AOR:** 976653434@10.33.4.226
- **Associated AOR:** 3434@10.33.4.226 (after manipulation, in which only the four digits from the right of the URI user part are retained)
- **Contact:** 976653434@10.10.10.10

The procedure below describes how to configure the manipulation example scenario above (relevant *ini* parameter is SASRegistrationManipulation):

➤ **To manipulate incoming Request-URI user part of REGISTER message:**

1. Open the 'SAS Configuration' page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. In the SAS Registration Manipulation table, in the 'Leave From Right' field, enter the number of digits (e.g., 4) to leave from the right side of the user part. (The 'Leave From Right' field defines the number of digits to retain from the right side of the user part; all other digits in the user part are removed.)

Figure 8-115: Manipulating User Part in Incoming REGISTER

The screenshot shows the 'SAS Configuration' web interface. The 'Basic Parameter List' is expanded, showing various configuration fields. The 'SAS Registration Manipulation' section is highlighted, showing two input fields: 'Remove From Right' (set to 0) and 'Leave From Right' (set to 4). A blue arrow points to the 'Leave From Right' field, which is also marked with a circled '2'. Below this section is the 'SAS Routing' section, which includes a 'SAS Routing Table' button. A 'Submit' button is located at the bottom right of the interface.

SAS Registration Manipulation	
Remove From Right	Leave From Right
0	4

3. Click **Submit**.

8.5.3.5.2 Manipulating Destination Number of Incoming INVITE

You can define a manipulation rule to manipulate the destination number in the Request-URI of incoming INVITE messages when SAS is in emergency state. This is required, for example, if the call is destined to a registered user but the destination number in the received INVITE is not the number assigned to the registered user in the SAS registration database. To overcome this and successfully route the call, you can define manipulation rules to change the INVITE's destination number so that it matches that of the registered user in the database. This is done using the IP to IP Inbound Manipulation table.


For example, in SAS emergency state, assume an incoming INVITE has a destination number "7001234" which is destined to a user whose registered in the SAS database as "55215551234". In this scenario, the received destination number needs to be manipulated to the number "55215551234". 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 55215551234 in its database and if found, it sends the INVITE containing this number to the UA.

➤ To manipulate destination number in SAS emergency state:

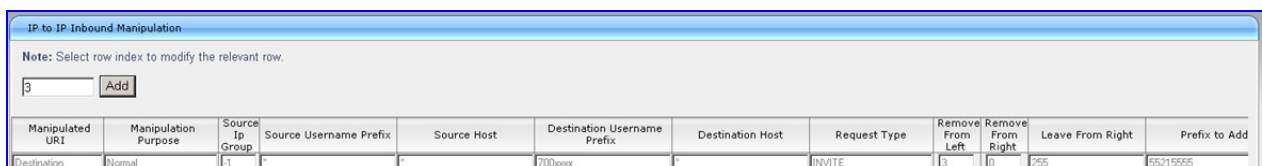
1. Load an *ini* file to the device with the following setting to enable inbound manipulation:

```
SASInboundManipulationMode = 1
```

2. Open the 'SAS Configuration' page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
3. Click the **IP to IP Inbound Manipulation Table**  button to open the 'IP to IP Inbound Manipulation' page.
4. Enter a table index number, and then click **Add**.
5. Define the rules as required, and then click **Apply**.

The figure below displays a manipulation rule for the example scenario described above whereby the destination number "7001234" is changed to "55215551234":

Figure 8-116: 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

In the figure above, the following configuration is done:

- **Manipulated URI field:** 'Destination'
- **Destination Username Prefix field:** '700xxxx'
- **Request Type field:** 'INVITE'
- **Remove From Left field:** '3'
- **Prefix to Add field:** '55215555'

**Notes:**

- The 'Source IP Group' field must not be configured; leave it at '-1'.
- The 'Is Additional Manipulation' field must be set to '0'.
- The 'Manipulation Purpose' field must be set to 'Normal'.
- For a detailed description of the fields in the 'IP to IP Inbound Manipulation' table, see "Configuring IP-to-IP Inbound Manipulations" on page [210](#). This table is currently located under the **SBC** menu.

8.5.3.5.3 SAS Routing Based on SAS Routing Table

SAS routing based on rules configured in the SAS Routing table is applicable for SAS in the following states:

- SAS in normal state, if the SASSurvivabilityMode parameter is set to 4
- SAS in emergency state, if the SASSurvivabilityMode parameter is not set to 4

The SAS routing rule destination can be an IP Group, IP address, Request-URI, or ENUM query.

For a detailed description of the SAS Routing table, see "Configuring IP2IP Routing Table (SAS)" on page [218](#).

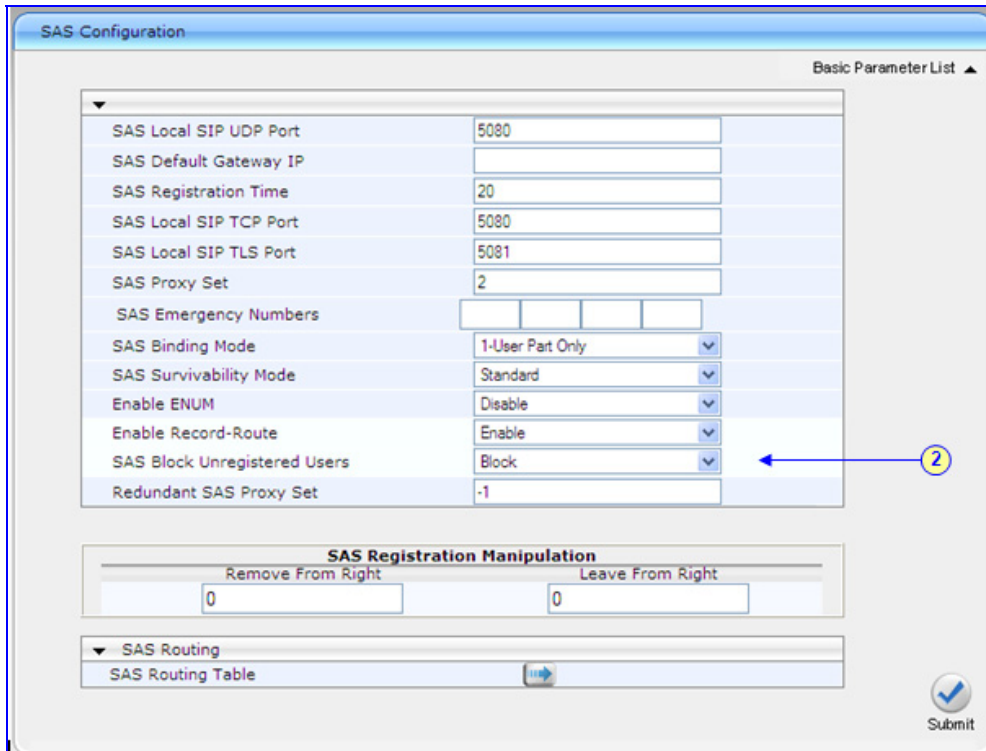
8.5.3.5.4 Blocking Calls from Unregistered SAS Users

To prevent malicious calls (for example, Service Theft), it is recommended to configure the feature for blocking SIP INVITE messages received from SAS users that are not registered in the SAS database. This applies to SAS in normal and emergency states.

➤ To block calls from unregistered SAS users:

1. Open the 'SAS Configuration' page (**Configuration** tab > **VoIP** menu > **SAS Stand Alone Survivability**).
2. From the 'SAS Block Unregistered Users' drop-down list, select 'Block'.

Figure 8-117: Blocking Unregistered SAS Users



The screenshot shows the 'SAS Configuration' web interface. The 'Basic Parameter List' is expanded, showing various configuration fields. The 'SAS Block Unregistered Users' dropdown menu is set to 'Block', which is highlighted by a blue arrow and a yellow circle with the number '2'. Other fields include 'SAS Local SIP UDP Port' (5080), 'SAS Default Gateway IP' (empty), 'SAS Registration Time' (20), 'SAS Local SIP TCP Port' (5080), 'SAS Local SIP TLS Port' (5081), 'SAS Proxy Set' (2), 'SAS Emergency Numbers' (empty), 'SAS Binding Mode' (1-User Part Only), 'SAS Survivability Mode' (Standard), 'Enable ENUM' (Disable), 'Enable Record-Route' (Enable), and 'Redundant SAS Proxy Set' (-1). Below the main list is the 'SAS Registration Manipulation' section with 'Remove From Right' and 'Leave From Right' fields, both set to 0. At the bottom is the 'SAS Routing' section with a 'SAS Routing Table' field and a 'Submit' button.

8.5.3.5.5 Configuring SAS Emergency Calls

You can configure SAS to route emergency calls (such as 911 in North America) directly to the PSTN (through its FXO interface 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 589). The default gateway is defined in the 'SAS Default Gateway IP' field, and this is the device itself. The device then sends the call directly to the PSTN.

This feature is applicable to SAS in normal and emergency states.

➤ **To configure SAS emergency numbers:**

1. Open the 'SAS Configuration' page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. In the 'SAS Default Gateway IP' field, define the IP address and port (in the format x.x.x.x:port) of the device (Gateway application).



Note: The port of the device is defined in the 'SIP UDP/TCP/TLS Local Port' field in the 'SIP General Parameters' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

3. In the 'SAS Emergency Numbers' field, enter an emergency number in each field box.

Figure 8-118: Configuring SAS Emergency Numbers

4. Click **Submit**.

8.5.3.5.6 Adding SIP Record-Route Header to SIP INVITE

You can configure SAS to add the SIP Record-Route header to SIP requests (e.g. INVITE) received from the enterprise UAs. SAS then sends the request with this header to the proxy. The Record-Route header includes the IP address of the SAS application. This ensures that future requests in the SIP dialog session from the proxy to the UAs are routed through the SAS application. If not configured, future request within the dialog from the proxy are sent directly to the UAs (and do not traverse SAS).

This feature can only be configured using the `SASEnableRecordRoute` *ini* file parameter.



Note: This feature is applicable only to SAS outbound mode.

When this feature is enabled, the SIP Record-Route header includes the URI "lr" parameter. The presence of this parameter indicates loose routing; the lack of it indicates strict routing. For example:

■ **Loose routing:**

```
Record-Route: <sip:server10.biloxi.com;lr>
```

■ **Strict routing:**

```
Record-Route: <sip:server10.biloxi.com>
```

8.5.3.5.7 Replacing Contact Header for SIP Messages

You can configure SAS to change the SIP Contact header so that it points to the SAS host. Therefore, this ensures that in the message, the top-most SIP Via header and the Contact header point to the same host.



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.

8.5.4 Viewing Registered SAS Users

You can view all the users that are registered in the SAS registration database. This is displayed in the 'SAS/SBC Registered Users' page, as described in "Viewing SAS/SBC Registered Users" on page 353. The maximum number of users that can be registered in the database is 200.

8.6 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).

8.6.1 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`.

8.6.2 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 605), 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 165):

Figure 8-119: 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.

8.7 General

8.7.1 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 608)



Note: Transcoding can also be implemented using the IP-to-IP (IP2IP) application and SBC application.

8.7.1.1 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
```

8.7.2 Supported RADIUS Attributes

The following table provides explanations on the RADIUS attributes included in the communication packets transmitted between the device and a RADIUS Server.

Table 8-27: Supported RADIUS Attributes

Attribute Number	Attribute Name	VSA No.	Purpose	Value Format	Example	AAA ¹
Request Attributes						
1	User-Name		Account number or calling party number or blank	String up to 15 digits long	5421385747	Start Acc Stop Acc
4	NAS-IP-Address		IP address of the requesting device	Numeric	192.168.14.43	Start Acc Stop Acc
6	Service-Type		Type of service requested	Numeric	1: login	Start Acc Stop Acc
26	H323-Incoming-Conf-Id	1	SIP call identifier	Up to 32 octets		Start Acc Stop Acc
26	H323-Remote-Address	23	IP address of the remote gateway	Numeric		Stop Acc
26	H323-Conf-ID	24	H.323/SIP call identifier	Up to 32 octets		Start Acc Stop Acc
26	H323-Setup-Time	25	Setup time in NTP format 1	String		Start Acc Stop Acc
26	H323-Call-Origin	26	The call's originator: Answering (IP) or Originator (PSTN)	String	Answer, Originate etc	Start Acc Stop Acc
26	H323-Call-Type	27	Protocol type or family used on this leg of the call	String	VoIP	Start Acc Stop Acc
26	H323-Connect-Time	28	Connect time in NTP format	String		Stop Acc
26	H323-Disconnect-Time	29	Disconnect time in NTP format	String		Stop Acc
26	H323-Disconnect-Cause	30	Q.931 disconnect cause code	Numeric		Stop Acc
26	H323-Gw-ID	33	Name of the gateway	String	SIPIDString	Start Acc Stop Acc
26	SIP-Call-ID	34	SIP Call ID	String	abcde@ac.com	Start Acc Stop Acc

Attribute Number	Attribute Name	VSA No.	Purpose	Value Format	Example	AAA ¹
26	Call-Terminator	35	The call's terminator: PSTN-terminated call (Yes); IP-terminated call (No).	String	Yes, No	Stop Acc
30	Called-Station-ID			String	8004567145	Start Acc
			Destination phone number	String	2427456425	Stop Acc
			Calling Party Number (ANI)	String	5135672127	Start Acc Stop Acc
			Account Request Type (start or stop) Note: 'start' isn't supported on the Calling Card application.	Numeric	1: start, 2: stop	Start Acc Stop Acc
			No. of seconds tried in sending a particular record	Numeric	5	Start Acc Stop Acc
			Number of octets received for that call duration	Numeric		Stop Acc
			Number of octets sent for that call duration	Numeric		Stop Acc
			A unique accounting identifier - match start & stop	String	34832	Start Acc Stop Acc
			For how many seconds the user received the service	Numeric		Stop Acc
			Number of packets received during the call	Numeric		Stop Acc
			Number of packets sent during the call	Numeric		Stop Acc
			Physical port type of device on which the call is active	String	0: Asynchronous	Start Acc Stop Acc
Response Attributes						
26	H323-Return-Code	103	The reason for failing authentication (0 = ok, other number failed)	Numeric	0 Request accepted	Stop Acc
44	Acct-Session-ID		A unique accounting identifier – match start & stop	String		Stop Acc

Below is an example of RADIUS Accounting, where the non-standard parameters are preceded with brackets.

```
Accounting-Request (361)
user-name = 111
acct-session-id = 1
nas-ip-address = 212.179.22.213
nas-port-type = 0
```

```

acct-status-type = 2
acct-input-octets = 4841
acct-output-octets = 8800
acct-session-time = 1
acct-input-packets = 122
acct-output-packets = 220
called-station-id = 201
calling-station-id = 202

// Accounting non-standard parameters:
(4923 33) h323-gw-id =
(4923 23) h323-remote-address = 212.179.22.214
(4923 1) h323-ivr-out = h323-incoming-conf-id:02102944 600a1899
3fd61009 0e2f3cc5
(4923 30) h323-disconnect-cause = 22 (0x16)
(4923 27) h323-call-type = VOIP
(4923 26) h323-call-origin = Originate
(4923 24) h323-conf-id = 02102944 600a1899 3fd61009 0e2f3cc5

```

8.7.3 Call Detail Record

The Call Detail Record (CDR) contains vital statistic information on calls made from the device. CDRs are generated at the end and optionally, at the beginning of each call (defined by the CDRReportLevel parameter). Once generated, they are sent to a Syslog server. The destination IP address for CDR logs is defined by the CDRSyslogServerIP parameter. For CDR in RADIUS format, see "Supported RADIUS Attributes" on page 609.

8.7.3.1 CDR Fields

The following table lists the supported CDR fields.

Table 8-28: Supported CDR Fields

Field Name	Description
ReportType	Report for either Call Started, Call Connected, or Call Released
Cid	Port Number
CallId	SIP Call Identifier
Trunk	Physical Trunk Number
BChan	Selected B-Channel
ConId	SIP Conference ID
TG	Trunk Group Number
EPTyp	Endpoint Type
Orig	Call Originator (IP, Tel)
SourceIp	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

Field Name	Description
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
TrmSd	Initiator of Call Release (IP, Tel, Unknown)
TrmReason	Termination Reason (see "Release Reasons in CDR" on page 612)
Fax	Fax Transaction during the Call
InPackets	Number of Incoming Packets
OutPackets	Number of Outgoing Packets
PackLoss	Local Packet Loss
RemotePackLoss	Number of Outgoing Lost Packets
Uniqueld	unique RTP ID
SetupTime	Call Setup Time
ConnectTime	Call Connect Time
ReleaseTime	Call Release Time
RTPdelay	RTP Delay
RTPjitter	RTP Jitter
RTPssrc	Local RTP SSRC
RemoteRTPssrc	Remote RTP SSRC
RedirectReason	Redirect Reason
TON	Redirection Phone Number Type
MeteringPulses	Number of Generated Metering Pulses
NPI	Redirection Phone Number Plan
RedirectPhonNum	Redirection Phone Number

8.7.3.2 Release Reasons in CDR

The possible reasons for call termination which is represented in the CDR field **TrmReason** are listed below:

- "REASON N/A"
- "RELEASE_BECAUSE_NORMAL_CALL_DROP"
- "RELEASE_BECAUSE_DESTINATION_UNREACHABLE"

- "RELEASE_BECAUSE_DESTINATION_BUSY"
- "RELEASE_BECAUSE_NOANSWER"
- "RELEASE_BECAUSE_UNKNOWN_REASON"
- "RELEASE_BECAUSE_REMOTE_CANCEL_CALL"
- "RELEASE_BECAUSE_UNMATCHED_CAPABILITIES"
- "RELEASE_BECAUSE_UNMATCHED_CREDENTIALS"
- "RELEASE_BECAUSE_UNABLE_TO_HANDLE_REMOTE_REQUEST"
- "RELEASE_BECAUSE_NO_CONFERECE_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"

Reader's Notes

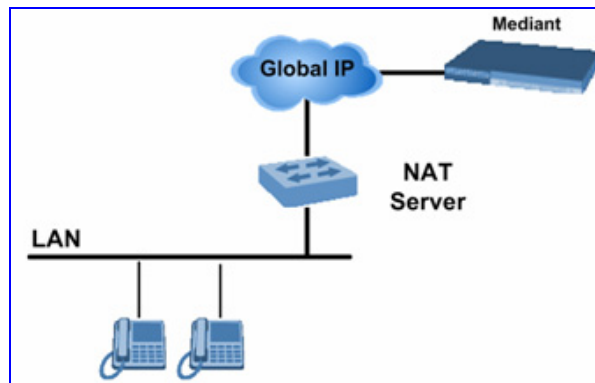
9 VoIP Networking Capabilities

This section provides an overview of the device's VoIP networking capabilities.

9.1 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:

- First Incoming Packet Mechanism (see "First Incoming Packet Mechanism" on page 617)
- RTP No-Op packets according to the avt-rtp-noop draft (see "No-Op Packets" on page 618)

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

9.1.1 First Incoming Packet Mechanism

If the remote device resides behind a NAT device, it's possible that the device can activate the RTP/RTCP/T.38 streams to an invalid IP address / UDP port. To avoid such cases, the device automatically compares the source address of the 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.

9.1.2 No-Op Packets

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

You can control the activation of No-Op packets by using the *ini* file parameter NoOpEnable. If No-Op packet transmission is activated, you can control the time interval in which No-Op packets are sent in the case of silence (i.e., no RTP or T.38 traffic). This is performed using the *ini* file parameter NoOpInterval. For a description of the RTP No-Op *ini* file parameters, see "Networking Parameters" on page 653.

- **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 653). AudioCodes' default payload type is 120.
- **T.38 No-Op:** T.38 No-Op packets are sent only while a T.38 session is activated. Sent packets are a duplication of the previously sent frame (including duplication of the sequence number).



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

9.2 Robust Receipt of Media Streams

This mechanism filters out unwanted media (i.e., RTP, RTCP, and T.38) streams that are sent to the same port number on the device. These multiple media streams can result from traces of previous calls, call control errors, and deliberate attacks. When more than one media stream reaches the device on the same port number, the device accepts only one of the media streams ("inbound media stream latch") and ignores the rest.

The "original" stream is the inbound media stream whose IP address/UDP port are configured at the channel opening. The "active" stream is the media stream to which a channel is currently latched on.

The media stream to be latched on is selected according to the following:

- InboundMediaLatchMode = 0 (Strict): only the original media stream is accepted.
- InboundMediaLatchMode = 1 (Dynamic): the active media stream choice is performed as follows. The first packet arriving on a newly opened channel sets the source IP address and the UDP port of the active stream. If a new packet with a different source IP address or UDP port arrives later, one of the following occurs:
 - The device reverts (re-latches) to the new media stream if the new packet belongs to the original media stream.
 - The device reverts to the new media stream if for a period of time there are no incoming packets belonging to the active media stream.
 - Otherwise, the packet is dropped.
 - Special cases:

- ◆ Inbound media re-latch during a silence period: If a silence compression RTP packet is received, latching new RTP streams is disabled until a silence timeout expires. Currently, RTP packets with payload types 13 and 19 are considered silence compression packets. Each new silence compression RTP packet resets the timeout's timer.
- ◆ Fax relay: No RTP re-latch is allowed if a T.38 fax relay session is underway. It is re-allowed after the T.38 session ends and timeout.

The reason for the above cases is to avoid re-latch on another RTP stream due to "missing" activity on the currently active one, if no activity is expected. If a switch from a non-original RTP stream to the original one occurs, both special cases are ignored and the original stream is accepted immediately.

If an inbound media stream latch occurs, the outbound media stream latch (redirecting outgoing media packets) is also (optionally) performed, according to the DisableNAT parameter (see First Incoming Packet Mechanism on page 617).

9.3 Multiple Routers Support

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

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



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

9.4 Simple Network Time Protocol Support

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

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

The client requests a time update from a specified NTP server at a specified update interval. In most situations, this update interval is every 24 hours based on when the system was restarted. The NTP server identity (as an IP address) and the update interval are user-defined (using the *ini* file parameters NTPServerIP and NTPUpdateInterval respectively), or an SNMP MIB object (refer to the *Product Reference Manual*).

When the client receives a response to its request from the identified NTP server, it must be interpreted based on time zone or location offset that the system is to a standard point of reference called the Universal Time Coordinate (UTC). The time offset that the NTP client uses is configurable using the *ini* file parameter NTPServerUTCOffset, or via an SNMP MIB object (refer to the *Product Reference Manual*).

If required, the clock update is performed by the client as the final step of the update process. The update is performed in such a way as to be transparent to the end users. For instance, the response of the server may indicate that the clock is running too fast on the client. The client slowly robs bits from the clock counter to update the clock to the correct time. If the clock is running too slow, then in an effort to catch the clock up, bits are added to the counter, causing the clock to update quicker and catch up to the correct time. The advantage of this method is that it does not introduce any disparity in the system time that is noticeable to an end user or that could corrupt call timeouts and timestamps.

9.5 Network Configuration

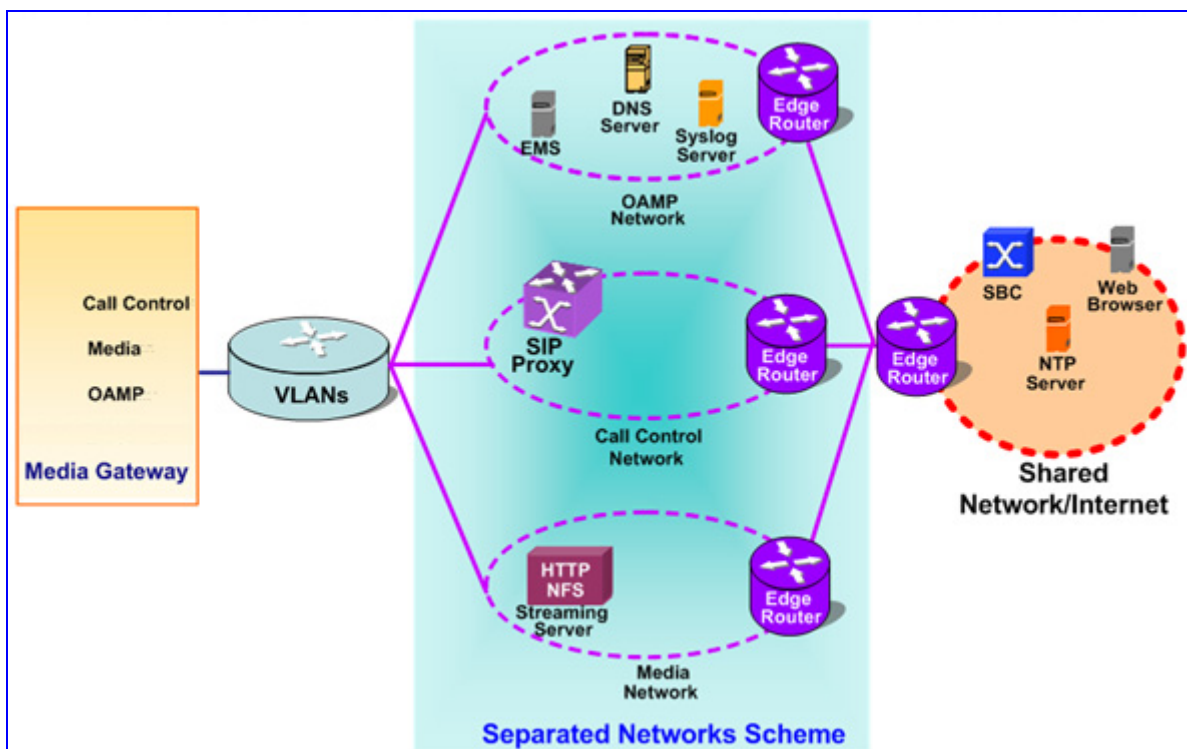
The device allows you to configure up to 12 different IP addresses with associated VLANs for the VoIP network, using the Multiple Interface table. Complementing this table is the Routing table, which allows you to define VoIP network static routing rules for non-local hosts/subnets. This section describes the various network configuration options offered by the device.

This section covers the VoIP network configuration (interfaces, static routing rules, and QoS definitions). For configuring the data-routing network (interfaces, routing, firewall, NAT, etc.), see Data Settings on page 222.

9.5.1 Multiple Network Interfaces and VLANs

A need often arises to have logically separated network segments for various applications (for administrative and security reasons). This can be achieved by employing Layer-2 VLANs and Layer-3 subnets.

Figure 9-1: 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

The Multiple Interfaces scheme allows the configuration of up to 12 different IP addresses, each associated with a unique VLAN ID. The configuration is performed using the Multiple Interface table, which is configurable using the *ini* file, Web, and SNMP interfaces.

9.5.1.1 Overview of Multiple Interface Table

The Multiple Interfaces scheme allows you to define up to 12 different IP addresses and VLANs in a table format, as shown below:

Table 9-1: Multiple Interface Table

Index Mode	Application	Interface	IP Address	Prefix Length	Default Gateway	VLAN ID	Interface Name
0	OAMP	IPv4	10.31.174.50	16	0.0.0.0	4	ManagementIF
1	Control	IPv4	10.32.174.50	16	0.0.0.0	5	ControlIF
2	Media	IPv4	10.33.174.50	16	10.33.0.1	6	Media1IF
3	Media	IPv4	10.34.174.50	16	0.0.0.0	7	Media2IF
4	Media	IPv4	10.35.174.50	16	10.35.0.1	8	Media3IF
5	Media	IPv4	10.36.174.50	16	0.0.0.0	9	Media4IF
6	Media	IPv4	10.37.174.50	16	0.0.0.0	10	Media5IF
7	Media	IPv4	10.38.174.50	16	0.0.0.0	11	Media6IF
8	Media	IPv4	10.39.174.50	16	10.39.0.1	12	Media7IF
9	Media	IPv4	10.40.174.50	16	10.40.0.1	13	Media8IF
10	Media & Control	IPv4	10.41.174.50	16	0.0.0.0	14	MediaCtrl9IF
11	Media	IPv4	10.42.174.50	16	0.0.0.0	15	Media10IF
12	Media	IPv4	10.43.174.50	16	10.43.0.1	16	Media11IF
13	Media	IPv4	10.44.174.50	16	0.0.0.0	17	Media12IF
14	Media & Control	IPv4	10.45.174.50	16	10.45.0.1	18	Media13IF

Complementing this network configuration is the On-Board Ethernet Switch configuration. This allows configuring the VLAN IDs accessible through each physical port, as well as the Native VLAN ID of each physical port. The On-Board Ethernet Switch configuration is described in LAN Switch on page 292. In addition, Layer3 (DiffServ) and Layer 2 (VLAN priority) Quality of Service parameters are also configurable.

9.5.1.2 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, 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. See "Gateway Column" on page 623 for more details.

9.5.1.2.1 Index Column

This column holds the index of each interface. Possible values are 0 to 11. Each interface index must be unique.

9.5.1.2.2 Application Types Column

This column defines the types of applications that are allowed on this interface:

- OAMP – Operations, Administration, Maintenance and Provisioning applications such as Web, Telnet, SSH, SNMP
- CONTROL – Call Control protocols (i.e., SIP)
- MEDIA – RTP streams of voice
- Various combinations of the above mentioned types

The following table shows the possible values of this column and their descriptions:

Table 9-2: Application Types

Value	Description
0	OAMP: only OAMP applications are allowed on this interface.
1	MEDIA: only Media (RTP) are allowed on this interface.
2	CONTROL: only Call Control applications are allowed on this interface.
3	OAMP & MEDIA: only OAMP and Media (RTP) applications are allowed on this interface.
4	OAMP & CONTROL: only OAMP and Call Control applications are allowed on this interface.
5	MEDIA & CONTROL: only Media (RTP) and Call Control applications are allowed on this interface.
6	OAMP, MEDIA & CONTROL: all of the application types are allowed on this interface.

For valid configuration guidelines, see "Multiple Interface Table Configuration Summary and Guidelines" on page 627 for more information.

9.5.1.2.3 Interface Mode Column

The Interface Mode column determines the method that this interface uses to acquire its IP address. For IPv4 Manual IP Address assignment, use "IPv4 Manual" (10).

IPv6 addresses may be assigned in two ways:

- "IPv6 Manual" (4)
- "IPv6 Manual Prefix" (3)

9.5.1.2.4 IP Address and Prefix Length Columns

These columns allow the user to configure an IPv4/IPv6 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. For IPv6 interfaces, the prefix length must be set to 64.

9.5.1.2.5 Gateway Column

This column defines a default gateway for each interface. A default gateway can be defined for each interface. When traffic is sent from this interface to an unknown destination (i.e., not in the same subnet and not defined for any static routing rule), it is forwarded to this default gateway. The default gateway's address must be on the same subnet as the interface address. A separate routing table allows configuring additional static routing rules. See "Routing Table" on page 628 for more details.



Note: In the example below, the default gateway for the OAMP application is 192.168.0.1, whereas for Media & Control applications it is 200.200.85.1.

Table 9-3: Configured Default Gateway Example

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

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

Table 9-4: Separate Routing Table Example

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

9.5.1.2.6 VLAN ID Column

This column defines the VLAN ID for each interface. This column must hold a unique value for each interface of the same address family. One IPv4 interface and one IPv6 interface may share the same VLAN ID, allowing hybrid networks on a single broadcast domain.

9.5.1.2.7 Interface Name Column

This column allows the configuration of a short string (up to 16 characters) to name this interface. This name is displayed in management interfaces (Web, CLI, and SNMP) and is used in the Media Realm table. This column must have a unique value for each interface (no two interfaces can have the same name) and must not be left blank.

9.5.1.3 Other Related Parameters

The Multiple Interface table allows you to configure interfaces and their related parameters such as VLAN ID, default gateway, or interface name. This section lists additional parameters complementing this table functionality.

9.5.1.3.1 Booting using DHCP

The *DHCPEnable* parameter enables the device to boot while acquiring an IP address from a DHCP server. Note that when using this method, Multiple Interface table/VLANs and other advanced configuration options are disabled.

9.5.1.3.2 Quality of Service Parameters

The device allows you to specify values for Layer-3 priorities, by assigning values to the following service classes:

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

Table 9-5: Quality of Service Parameters

Parameter	Description
Layer-2 Class Of Service Parameter (VLAN Tag Priority Field)	
DiffServ Table [DiffServToVlanPriority]	<p>This ini file table parameter allows you to configure DiffServ-to-VLAN Priority mapping. For each packet sent to the LAN, the VLAN Priority of the packet is set according to the DiffServ value in the IP header of the packet.</p> <p>The format of this ini file is as follows:</p> <pre>[DiffServToVlanPriority] FORMAT DiffServToVlanPriority_Index = DiffServToVlanPriority_DiffServ, DiffServToVlanPriority_VlanPriority; [\DiffServToVlanPriority]</pre> <p>For example:</p> <pre>DiffServToVlanPriority 1 = 46, 6; DiffServToVlanPriority 2 = 40, 6; DiffServToVlanPriority 3 = 26, 4; DiffServToVlanPriority 4 = 10, 2;</pre> <p>Notes:</p> <ul style="list-style-type: none"> ▪ You can configure up to 64 VLAN tag priorities (i.e., indices 0-63). ▪ The valid range of the parameter DiffServ is 0-63. ▪ The valid range of the parameter VlanPriority is 0-7. ▪ To set a default VLAN Priority (used for ARPs and automated ICMP packets, as well as for IP Packets without DiffServ value), set a VLAN Priority value for DiffServ 0.
Layer-3 Class Of Service Parameters (TOS/DiffServ)	
PremiumServiceClassMediaDiffServ	Defines the DiffServ value for Premium Media CoS content (media traffic).
PremiumServiceClassControlDiffServ	Defines the DiffServ value for Premium Control CoS content (Call Control applications).
GoldServiceClassDiffServ	Sets the DiffServ for the Gold service class content (streaming applications).
BronzeServiceClassDiffServ	Sets the DiffServ for the Bronze service class content (OAMP applications).

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

Table 9-6: Traffic/Network Types and Priority

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

Application	Traffic / Network Types	Class-of-Service (Priority)
Web server (HTTP)	Management	Bronze
SNMP GET/SET	Management	Bronze
Web server (HTTPS)	Management	Bronze
RTP traffic	Media	Premium media
RTCP traffic	Media	Premium media
T.38 traffic	Media	Premium media
SIP	Control	Premium control
SIP over TLS (SIPS)	Control	Premium control
Syslog	Management	Bronze
SNMP Traps	Management	Bronze
DNS client	Varies according to DNS settings (EnableDNSasOAM): <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 (EnableNTPasOAM): <ul style="list-style-type: none"> ■ OAMP ■ Control 	Depends on traffic type: <ul style="list-style-type: none"> ■ Control: Premium control ■ Management: Bronze

9.5.1.3.3 Applications with Assignable Application Type

Some applications can be associated with different application types in different setups. These application types are configurable. The applications listed below can be configured to one of two application types:

- DNS
- NTP

Table 9-7: Application Type Parameters

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

9.5.1.4 Multiple Interface Table Configuration Summary and Guidelines

Multiple Interface table configuration must adhere to the following rules:

- Up to 12 different interfaces may be defined.
- The indices used must be in the range between 0 and 11.
- Each interface must have its own subnet. Defining two interfaces with addresses in the same subnet (i.e. two interfaces with 192.168.0.1/16 and 192.168.100.1/16) is illegal.
- Subnets in different interfaces must not be overlapping in any way (i.e. defining two interfaces with 10.0.0.1/8 and 10.50.10.1/24 is invalid). Each interface must have its own address space.
- The Prefix Length replaces the dotted decimal Subnet Mask presentation. This column must have a value of 0-30 for IPv4 interfaces.
- Only one IPv4 interface with OAMP "Application Types" **must** be configured. At least one IPv4 interface with CONTROL "Application Types" **must** be configured. At least one IPv4 interface with MEDIA "Application Types" **must** be configured. These application types **may** be mixed (i.e. OAMP and CONTROL). Here are some examples for interface configuration:
 - One IPv4 interface with "Application Types" OAMP, MEDIA & CONTROL (without VLANs).
 - One IPv4 interface with "Application Types" OAMP, one other or more IPv4 interfaces with "Application Types" CONTROL, and one or more IPv4 interfaces with "Application Types" MEDIA (with VLANs).
 - One IPv4 interface with "Application Types" OAMP & MEDIA, one other or more IPv4 interfaces with "Application Types" MEDIA & CONTROL.
 - Other configurations are also possible while keeping to the above-mentioned rule.
- Each network interface may be defined with a default gateway. This default gateway address must be in the same subnet as the associated interface. Additional routing rules may be specified in the Routing table ("Routing Table" on page 628).
- The Interface Name column may have up to 16 characters. This column allows the user to name each interface with an easier name to associate the interface with. This column must have a unique value to each interface and must not be left blank.
- For IPv4 interfaces, the "Interface Mode" column must be set to "IPv4 Manual" (numeric value 10).
- Quality of Service parameters specify the DiffServ field in the IP header according to service classes. DiffServ-to-VLAN Priority mapping allows associating each DiffServ value with a VLAN priority (according to IEEE 802.1p standard).
- Network Configuration changes are offline. The new configuration should be saved and becomes available at the next startup.

Upon system start up, the Multiple Interface table is parsed and passes comprehensive validation tests. If any errors occur during this validation phase, the device sends an error message to the Syslog server and falls back to a "safe mode", using a single interface and no VLANs. Please be sure to follow the Syslog messages that the device sends in system startup to see if any errors occurred.



Note: When configuring the device using the Web interface, it is possible to perform a quick validation of the configured Multiple Interface table and VLAN definitions, by clicking the **Done** button in the Multiple Interface Table Web page. It is highly recommended to perform this when configuring Multiple Interfaces and VLANs, using the Web Interface to ensure the configuration is complete and valid.

9.5.1.5 Troubleshooting the Multiple Interface Table

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

Validation failures may be caused by one of the following:

- One of the Application Types (OAMP, CONTROL, 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.
- 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 untagged traffic when VLANs are on and Native VLAN is not configured properly.
- Routing Table is not configured properly.

9.5.2 Static Routing Table

The IP Routing table allows you to configure static routing rules for the VoIP network. You may define up to 30 different routing rules, using the *ini* file, Web interface, and SNMP.

9.5.2.1 Routing Table Overview

The IP Routing table consists of the following:

Table 9-8: IP Routing Table Layout

Destination	Prefix Length	Gateway	Interface	Metric	Status
201.201.0.0	16	192.168.0.1	0	1	Active
202.202.0.0	16	192.168.0.2	0	1	Active
203.203.0.0	16	192.168.0.3	0	1	Active
225.225.0.0	16	192.168.0.25	0	1	Inactive

9.5.2.2 Routing Table Columns

Each row of the Routing table defines a static routing rule. Traffic destined to the subnet specified in the routing rule is re-directed to the defined gateway, reachable through the specified interface.

9.5.2.2.1 Destination Column

This column defines the destination of the route rule. The destination can be a single host or a whole subnet, depending on the Prefix Length/Subnet Mask specified for this routing rule.

9.5.2.2.2 Prefix Length Column

The Prefix Length column holds the Classless Inter-Domain Routing (CIDR)-style representation of a dotted-decimal subnet notation. The CIDR-style representation uses a suffix indicating the number of bits that are set in the dotted-decimal format. For example, 16 is synonymous with subnet 255.255.0.0.

9.5.2.2.3 Gateway Column

The Gateway column defines the IP address of the next hop used for traffic destined to the subnet/host as defined in the destination/mask columns. This gateway address must be on the same subnet as the IP address of the interface configured in the Interface column.

9.5.2.2.4 Interface Column

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



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

Figure 9-2: Interface Column

The VoIP Interface Table:

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

The VoIP Static Routing Table:

Destination	Destination Subnet Mask / Prefix Length	Gateway (Next Hop) IP Address	Metric	Interface Index
10.31.174.0	24	192.168.11.1	1	0
174.96.151.15	24	10.32.174.12	1	1
10.35.174.0	24	10.34.174.240	1	3

The IP Address of the Gateway (Next Hop) must reside at the same subnet as the IP Address of the interface configured in the Interface Index column

9.5.2.2.5 Metric Column

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

9.5.2.2.6 State Column

The State column displays the state of each static route. Possible values are "Active" and "Inactive". When the destination IP address is not on the same segment with the next hop or the interface does not exist, the route state changes to "Inactive".

9.5.2.3 Routing Table Configuration Summary and Guidelines

The Routing table configurations must adhere to the following rules:

- Up to 30 different static routing rules may be defined.
- The Prefix Length replaces the dotted-decimal subnet mask presentation. This column must have a value of 0-31 for IPv4 interfaces and a value of 64 for IPv6 interfaces.
- The "Gateway" IP Address must be on the same subnet as the IP address of the interfaces configured in the Interface Index column.
- The "Metric" column must be set to 1.
- Network Configuration changes are offline. The new configuration should be saved and will be available at the next startup.

9.5.2.4 Troubleshooting the Routing Table

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

Common routing rule configuration errors may include the following:

- The IP address specified in the "Gateway" column is unreachable from the interface specified in the "Interface" column.
- The same destination is defined in two different routing rules.
- More than 30 routing rules were defined.



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

9.5.3 Setting Up VoIP Networking

9.5.3.1 Using the Web Interface

The Web interface is a convenient user interface for configuring the device's network configuration.

9.5.3.2 Using the ini File

When configuring the network configuration using the *ini* File, use a textual presentation of the Interface and Routing Tables, as well as some other parameters. The following shows an example of a full network configuration, consisting of **all** the parameters described in this section:

```
; *** TABLE InterfaceTable ***
[ InterfaceTable ]
FORMAT InterfaceTable Index = InterfaceTable ApplicationTypes,
InterfaceTable InterfaceMode, InterfaceTable IPAddress,
InterfaceTable PrefixLength, InterfaceTable Gateway,
InterfaceTable VlanID, InterfaceTable InterfaceName;
InterfaceTable 0 = 0, 10, 192.168.0.2, 16, 192.168.0.1, 501, Mgmt;
InterfaceTable 1 = 5, 10, 10.32.174.50, 24, 10.32.174.1, 2012,
MediaCntrl;
InterfaceTable 2 = 1, 10, 10.33.174.50, 24, 10.33.174.1, 2013, Media1;
InterfaceTable 3 = 2, 10, 10.34.174.50, 24, 10.34.174.1, 2014, Cntrl1;
[ \InterfaceTable ]

; Routing Table Configuration:
[ StaticRouteTable ]
```

```

FORMAT StaticRouteTable Index = StaticRouteTable InterfaceName,
StaticRouteTable_Destination, StaticRouteTable_PrefixLength,
StaticRouteTable Gateway, StaticRouteTable Description;
StaticRouteTable 0 = 0, 10.31.174.0, 24, 192.168.11.1, ;
StaticRouteTable 1 = 1, 174.96.151.15, 24, 10.32.174.12, ;
StaticRouteTable 2 = 3, 10.35.174.0, 24, 10.34.174.240, ;
[ \StaticRouteTable ]
; Layer 3 QoS parameters (DiffServ):
PremiumServiceClassMediaDiffServ = 46
PremiumServiceClassControlDiffServ = 40
GoldServiceClassDiffServ = 26
BronzeServiceClassDiffServ = 10

; *** TABLE DiffServToVlanPriority ***
[ DiffServToVlanPriority ]
FORMAT DiffServToVlanPriority Index = DiffServToVlanPriority DiffServ,
DiffServToVlanPriority VlanPriority;
DiffServToVlanPriority 0 = 0, 7;
DiffServToVlanPriority 1 = 46, 6;
DiffServToVlanPriority 2 = 40, 6;
DiffServToVlanPriority 3 = 26, 4;
DiffServToVlanPriority 4 = 10, 2;
[ \DiffServToVlanPriority ]

; Application Type for applications:
EnableDNSSasOAM = 1
EnableNTPasOAM = 1

```

This *ini* file shows the following:

- A Multiple Interface table with a an interface for OAMP applications (192.168.0.2/16), an interface for Media & Control applications (10.32.174.50/24), an interface for Media applications (10.33.174.50/24), and an interface for Control applications (10.34.174.50/24).
- Each interface is defined with its own VLAN ID, Default Gateway, and name.
- A Routing table is configured with three static routing rules:
 - Directing all traffic destined to subnet 10.31.174.0/24 to 192.168.11.1 over Interface Index 0
 - Directing all traffic destined to subnet 174.96.151.15/24 to 10.32.174.12 over Interface Index 1
 - Directing all traffic destined to subnet 10.35.174.0/24 to 10.34.174.240 over Interface Index 3
- Layer-3 QoS values are assigned:
 - For Media Service class, the default DiffServ value is set to 46
 - For Control Service class, the default DiffServ value is set to 40
 - For Gold Service class, the default DiffServ value is set to 26
 - For Bronze Service class, the default DiffServ value is set to 10
- Layer-2 QoS values are assigned:
 - For packets sent with DiffServ value of 46, set VLAN priority to 6
 - For packets sent with DiffServ value of 40, set VLAN priority to 6
 - For packets sent with DiffServ value of 26, set VLAN priority to 4

- For packets sent with DiffServ value of 10, set VLAN priority to 2
- The DNS and the NTP applications are configured to serve as OAMP applications.

**Notes:**

- Lines that begin with a semicolon are considered a remark and are ignored.
- When using the *ini* file, the Multiple Interface table and the DiffServ To VLAN Priority table must have the prefix and suffix to allow the INI File parser to correctly recognize and parse the table.

9.5.3.3 Networking Configuration Examples

This section provides examples of network configurations (and their corresponding *ini* file configuration).

Example 1 - One VoIP Interface for All Applications: Multiple Interface table with a single interface for OAMP, Media and Control applications:

Table 9-9: Multiple Interface Table - Example 1

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

Additional static routing rules:

Table 9-10: Routing Table - Example 1

Destination	Prefix Length	Gateway	Interface	Metric
201.201.0.0	16	192.168.11.10	0	1
202.202.0.0	16	192.168.11.1	0	1

The DNS/NTP applications remain with their default application types.

The corresponding *ini* file configuration is shown below:

```
; Interface Table Configuration:
[InterfaceTable]
FORMAT InterfaceTable Index = InterfaceTable ApplicationTypes,
InterfaceTable InterfaceMode, InterfaceTable IPAddress,
InterfaceTable PrefixLength, InterfaceTable Gateway,
InterfaceTable VlanID, InterfaceTable InterfaceName;
InterfaceTable 0 = 6, 10, 192.168.0.2, 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, 192.168.11.10, ;
StaticRouteTable 1 = 0, 202.202.0.0, 16, 192.168.11.1, ;
[ \StaticRouteTable ]
```

Example 2 - Three VoIP Interfaces, One for each Application Exclusively: the Multiple Interface table is configured with three interfaces, one exclusively for each application type: one interface for OAMP applications, one for Call Control applications, and one for RTP Media applications:

Table 9-11: Multiple Interface Table - Example 2

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

Additional static routing rules:

Table 9-12: Routing Table - Example2

Destination	Prefix Length	Gateway	Interface	Metric
176.85.49.0	24	192.168.11.1	0	1

All other parameters are set to their respective default values. The DNS/NTP applications are left with their default application types.

The corresponding *ini* file configuration is shown below:

```
; Interface Table Configuration:
[InterfaceTable]
FORMAT InterfaceTable Index = InterfaceTable ApplicationTypes,
InterfaceTable InterfaceMode, InterfaceTable IPAddress,
InterfaceTable PrefixLength, InterfaceTable Gateway,
InterfaceTable VlanID, InterfaceTable InterfaceName;
InterfaceTable 0 = 0, 10, 192.168.0.2, 16, 192.168.0.1, 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 ]

; 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, 192.168.11.1, ;
[ \StaticRouteTable ]
```

Example 3 - Three Interfaces: one exclusively for management (OAMP applications) and two others for Call Control and RTP (Control and Media applications) :

Table 9-13: Multiple Interface Table - Example 3

Index	Allowed Applications	Interface Mode	IP Address	Prefix Length	Default Gateway	VLAN ID	Interface Name
0	OAMP	IPv4 Manual	192.168.0.2	16	192.168.0.1	1	Mgmt
1	Media & Control	IPv4 Manual	200.200.85.14	24	200.200.85.1	201	MediaCntrl1
2	Media & Control	IPv4 Manual	200.200.86.14	24	200.200.86.1	202	MediaCntrl2

Additional static routing rules

Table 9-14: Routing Table - Example 3

Destination	Destination Subnet Mask/Prefix Length	Gateway	Interface	Metric
176.85.49.0	24	192.168.0.10	0	1

All other parameters are set to their respective default values. The DNS/NTP applications are left with their default application types.

The corresponding *ini* file configuration is shown below:

```
; Interface Table Configuration:
[InterfaceTable]
FORMAT InterfaceTable Index = InterfaceTable ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable PrefixLength, InterfaceTable Gateway,
InterfaceTable VlanID, InterfaceTable InterfaceName;
InterfaceTable 0 = 0, 10, 192.168.0.2, 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]

; 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, 192.168.11.1, ;
[ \\StaticRouteTable ]
```


Reader's Notes

10 Advanced PSTN Configuration

This section discusses advanced PSTN configurations.

10.1 Clock Settings

In a traditional TDM service network such as PSTN, both ends of the TDM connection must be synchronized. If synchronization is not achieved, voice frames are either dropped (to prevent a buffer overflow condition) or inserted (to prevent an underflow condition). In both cases, connection quality and reliability is affected.

- PSTN line clock (see "Recovering Clock from PSTN Line" on page 637)
- Internal clock (see "Configuring Internal Clock as Clock Source" on page 638)



Note: When the device is used in a 'non-span' configuration, the internal device clock must be used (as explained above).

10.1.1 Recovering Clock from PSTN Line Interface

This section provides a brief description for configuring synchronization based on recovering clock from the PSTN line (Trunk) interface. For a full description of the clock parameters, see "PSTN Parameters" on page 783.

- `TDMBusClockSource = 4` ('Network') - recovers clock from line interface
- `ClockMaster`: configures the PSTN trunk to recover/derive clock from the device or transmit the clock to the remote side of the PSTN trunk (i.e. clock slave or clock master):

`ClockMaster_x = 0/1` (where 'x' depicts the trunk number) - '0' means to recover/derive clock (i.e. slave); '1' means to transmit/drive clock (i.e. master).
- `TDMBusLocalReference`: selects the trunk from which the clock is derived.

`TDMBusLocalReference = x` (where 'x' is the trunk number and 0 is the first trunk - default)
- `TDMBusPSTNAutoClockEnable`: The device has an automatic mechanism to detect when a "local-reference" trunk (set by `TDMBusLocalReference`) is no longer capable of supplying the clock to the system, and can automatically switch to the next available trunk (according to the priority set by the `AutoClockTrunkPriority` and `TDMBusPSTNAutoClockRevertingEnable` parameters).

`TDMBusPSTNAutoClockEnable = 1` (device automatically selects one of the connected 'slave' trunks)

10.1.2 Configuring Internal Clock as Clock Source

This section describes how to configure the device to use its internal clock source. The internal clock source is a stratum 4E-compliant clock source. When the device has no line interfaces, the device should be configured in this mode.

- Set the clock source to be from the internal oscillator device:
TDMBusClockSource = 1 (internal)
- Set the line to drive the clock on all trunks:
ClockMaster = 1 (for all trunks)

10.2 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 639 and "Fixed Mapping of SIP Response to ISDN Release Reason" on page 641. 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 799) or the Web interface (see "Configuring Release Cause Mapping" on page 162).

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 799) 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.

10.2.1 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.

10.2.2 Fixed Mapping of ISDN Release Reason to SIP Response

The following table describes the mapping of ISDN release reason to SIP response.

Table 10-1: Mapping of ISDN Release Reason to SIP Response

ISDN Release Reason	Description	SIP Response	Description
1	Unallocated number	404	Not found
2	No route to network	404	Not found
3	No route to destination	404	Not found
6	Channel unacceptable	406*	Not acceptable
7	Call awarded and being delivered in an established channel	500	Server internal error
16	Normal call clearing	_*	BYE
17	User busy	486	Busy here
18	No user responding	408	Request timeout
19	No answer from the user	480	Temporarily unavailable
21	Call rejected	403	Forbidden
22	Number changed w/o diagnostic	410	Gone
26	Non-selected user clearing	404	Not found
27	Destination out of order	502	Bad gateway
28	Address incomplete	484	Address incomplete
29	Facility rejected	501	Not implemented
30	Response to status enquiry	501*	Not implemented
31	Normal unspecified	480	Temporarily unavailable
34	No circuit available	503	Service unavailable
38	Network out of order	503	Service unavailable
41	Temporary failure	503	Service unavailable
42	Switching equipment congestion	503	Service unavailable
43	Access information discarded	502*	Bad gateway
44	Requested channel not available	503*	Service unavailable
47	Resource unavailable	503	Service unavailable
49	QoS unavailable	503*	Service unavailable
50	Facility not subscribed	503*	Service unavailable
55	Incoming calls barred within CUG	403	Forbidden
57	Bearer capability not authorized	403	Forbidden
58	Bearer capability not presently available	503	Service unavailable
63	Service/option not available	503*	Service unavailable

ISDN Release Reason	Description	SIP Response	Description
65	Bearer capability not implemented	501	Not implemented
66	Channel type not implemented	480*	Temporarily unavailable
69	Requested facility not implemented	503*	Service unavailable
70	Only restricted digital information bearer capability is available	503*	Service unavailable
79	Service or option not implemented	501	Not implemented
81	Invalid call reference value	502*	Bad gateway
82	Identified channel does not exist	502*	Bad gateway
83	Suspended call exists, but this call identity does not	503*	Service unavailable
84	Call identity in use	503*	Service unavailable
85	No call suspended	503*	Service unavailable
86	Call having the requested call identity has been cleared	408*	Request timeout
87	User not member of CUG	503	Service unavailable
88	Incompatible destination	503	Service unavailable
91	Invalid transit network selection	502*	Bad gateway
95	Invalid message	503	Service unavailable
96	Mandatory information element is missing	409*	Conflict
97	Message type non-existent or not implemented	480*	Temporarily not available
98	Message not compatible with call state or message type non-existent or not implemented	409*	Conflict
99	Information element non-existent or not implemented	480*	Not found
100	Invalid information elements contents	501*	Not implemented
101	Message not compatible with call state	503*	Service unavailable
102	Recovery of timer expiry	408	Request timeout
111	Protocol error	500	Server internal error
127	Interworking unspecified	500	Server internal error

* Messages and responses were created because the 'ISUP to SIP Mapping' draft doesn't specify their cause code mapping.

10.2.3 Fixed Mapping of SIP Response to ISDN Release Reason

The following table describes the mapping of SIP response to ISDN release reason.

Table 10-2: 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
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

SIP Response	Description	ISDN Release Reason	Description
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.

10.3 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.

The device supports the interworking of ISDN overlap dialing to SIP based on RFC 3578.

- **Interworking ISDN overlap dialing to SIP (Tel to IP):** The device sends collected digits each time they are received (initially from ISDN Setup and then from subsequent Info Q.931 messages) to the IP, 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.

The device stops collecting digits when:

- Receives Sending Complete IE in the ISDN Setup or Info messages to signal that no more digits are going to be sent.
- The inter-digit timeout (configured by the TimeBetweenDigits parameter) expires.
- The maximum allowed number of digits (configured by the MaxDigits parameter) is reached.
- A match is found with the defined digit map (configured by the DigitMapping parameter).

The device can also mute in-band DTMF detection until the device receives the full destination number from the ISDN. This is configured using the MuteDTMFInOverlap parameter. With ISDN overlap dialing, DTMF digits can be sent in-band in the voice stream or out-of-band using Q.931 Info messages. If Q.931 Info messages are used, the DTMF in-band detector must be disabled. Note that when at least one digit is received from the ISDN (Setup message), the device stops playing a dial tone.

- **Interworking SIP to ISDN overlap dialing (IP to Tel):** For each received INVITE pertaining to 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 to the IP in order to maintain the current dialog session and to receive additional digits from subsequent INVITEs.

The device can optionally support ISDN overlap dialing for incoming ISDN calls for the entire device or per E1/T1 span, using the ISDNRxOverlap parameter.

To play a Dial tone to the ISDN user side when an empty called number is received, set the ISDNINCallsBehavior parameter to 65536 (bit #16). This results in the Progress Indicator being included in the SetupAck ISDN message.

Relevant parameters (described in "PSTN Parameters" on page 783):

- ISDNRxOverlap
- ISDNTxOverlap
- TimeBetweenDigits
- MaxDigits
- ISDNInCallsBehavior
- DigitMapping
- MinOverlapDigitsForRouting

For configuring ISDN overlap dialing using the Web interface, see "Configuring Trunk Settings" on page 101.

10.4 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 101).

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 101).

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 783.

10.4.1 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.

10.4.2 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
```

10.4.3 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.

10.5 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 10-3: Calling Name (Display)

NT/TE Interface	DMS-100	NI-2	4/5ESS	Euro ISDN	QSIG
NT-to-TE	Yes	Yes		Yes	Yes
TE-to-NT	Yes	Yes		No	Yes

Table 10-4: 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).

10.6 Automatic Gain Control (AGC)

Automatic Gain Control (AGC) adjusts the energy of the output signal to a required level (i.e., 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.

To configure AGC, see "Configuring the IP Media Settings" on page [107](#).

11 Tunneling Applications

This section discusses the device's support for VoIP tunneling applications.

11.1 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 138), 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]
FORMAT PREFIX Index = PREFIX DestinationPrefix,
PREFIX DestAddress, PREFIX SourcePrefix, PREFIX ProfileId,
PREFIX MeteringCode, PREFIX DestPort;
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 to 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 MWIAnalog, 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 MWIAnalog, TelProfile MWIDisplay,
TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia,
TelProfile_ProgressIndicator2IP;
TelProfile 1 = voice,$$,1,$$,,$$,,$$,,$$,,$$,,$$
TelProfile 2 = data,$$,2,$$,,$$,,$$,,$$,,$$,,$$
[\\TelProfile]
```

11.1.1 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:

- EnabledDSPIPMDetectors = 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)

11.2 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 the ECMA-355/ISO/IEC 22535 standard. This method enables all QSIG messages to be sent as raw data in corresponding SIP messages using a dedicated message body. This mechanism is useful for 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, whereas 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'. In addition, the device adds a Content-Disposition header in the following format:

```
Content-Disposition: signal; handling=required.
```

- **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 doesn't 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, use the following settings:

- Set the EnableQSIGTunneling parameter to 1 on the originating and terminating devices
- Set 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)
- Set the ISDNDuplicateQ931BuffMode parameter to 128 (duplicate all messages)
- Set the ISDNInCallsBehavior parameter to 4096
- Set the ISDNRxOverlap parameter 0 (for tunneling of QSIG overlap dialed digits - see below for description)

For a detailed description of these parameters, see "ISDN and CAS Interworking Parameters" on page [799](#).

The configuration of the ISDNInCallsBehavior and ISDNRxOverlap parameters as mentioned above, 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 to the remote party, encapsulated in SIP INFO messages.

Reader's Notes

12 Configuration Parameters Reference

The device's VoIP functionality (not data-routing functionality) 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.

12.1 Networking Parameters

This subsection describes the device's networking parameters.

12.1.1 VoIP Multiple Network Interfaces and VLAN Parameters

The IP network interfaces and VLAN parameters are described in the table below.

Table 12-1: IP Network Interfaces and VLAN Parameters

Parameter	Description
Web: Multiple Interface Table EMS: IP Interface Settings	
[InterfaceTable]	<p>This <i>ini</i> file table parameter configures the Multiple Interface table for configuring the IP addresses of the voice and/or data functionalities and 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]</pre> <p>For example:</p> <pre>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; 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;</pre> <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>ini</i> file table parameter to take effect, a device reset is required. Up to 12 logical IP addresses with associated VLANs can be defined (indices 0-11). However, only up to 8 interfaces can be used for media RTP traffic (assigned to a Media Realm in the 'SIP Media

Parameter	Description
	<p>Realm' table, which in turn is assigned to an IP Group).</p> <ul style="list-style-type: none"> 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. To configure multiple VoIP IP interfaces in the Web interface and for a detailed description of the table's parameters, see "Configuring IP Interface Settings" on page 83). For a description of configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
[EnableDNSasOAM]	<p>Determines the application type for DNS services.</p> <ul style="list-style-type: none"> [1] = OAMP (default) [0] = Control. <p>Note: For this parameter to take effect, a device reset is required.</p>
[EnableNTPasOAM]	<p>Determines the application type for NTP services.</p> <ul style="list-style-type: none"> [1] = OAMP (default) [0] = Control. <p>Note: For this parameter to take effect, a device reset is required.</p>

12.1.2 VoIP Static Routing Parameters

The static routing parameters are described in the table below.

Table 12-2: Static Routing Parameters

Parameter	Description
Static IP Routing Table	
[StaticRouteTable]	<p>You can define up to 30 static VoIP IP routing rules for the device. These rules can be associated with IP interfaces defined in the Multiple Interface table (InterfaceTable parameter). The routing decision for sending the outgoing IP packet is based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination IP address.</p> <p>When the destination of an outgoing IP packet does not match one of the subnets defined in the Multiple Interface table, the device searches this table for an entry that matches the requested destination host/network. If such an entry is found, the device sends the packet to the indicated router (i.e., next hop). If no explicit entry is found, the packet is sent to the default gateway according to the source interface of the packet (if</p>

Parameter	Description
	<p>defined).</p> <p>The format of this parameter is as follows:</p> <pre>[StaticRouteTable]</pre> <p>FORMAT StaticRouteTable_Index = StaticRouteTable_InterfaceName, StaticRouteTable_Destination, StaticRouteTable_PrefixLength, StaticRouteTable_Gateway, StaticRouteTable_Description;</p> <pre>[\StaticRouteTable]</pre> <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 VoIP network interfaces (refer to "Configuring IP Interface Settings" on page 83). ▪ The StaticRouteTable_Description parameter is a string value of up to 30 characters. ▪ The metric value (next hop) is automatically set to 1.

12.1.3 Quality of Service Parameters

The Quality of Service (QoS) parameters are described in the table below.

The device allows you to specify DiffServ (Differentiated Services) values for four predefined service classes:

- 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-3 QoS parameters enables setting the values of the DiffServ field in the IP Header of the frames related to a specific service class. 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.

Table 12-3: QoS Parameters

Parameter	Description
Layer-2 Class Of Service (CoS) Parameters (VLAN Tag Priority Field)	
Web: DiffServ Table EMS: QoS Settings – DSCP to QoS Mapping [DiffServToVlanPriority]	<p>This ini file table parameter allows you to configure DiffServ-to-VLAN Priority mapping.</p> <p>For each packet sent to the LAN, the VLAN Priority of the packet is set according to the DiffServ value in the IP header of the packet. The format of this ini file is as follows:</p> <pre>[DiffServToVlanPriority]</pre> <p>FORMAT DiffServToVlanPriority_Index = DiffServToVlanPriority_DiffServ, DiffServToVlanPriority_VlanPriority;</p> <pre>[\DiffServToVlanPriority]</pre> <p>For example:</p>

Parameter	Description
	DiffServToVlanPriority 0 = 46, 6; DiffServToVlanPriority 1 = 40, 6; DiffServToVlanPriority 2 = 26, 4; DiffServToVlanPriority 3 = 10, 2; Notes: <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. You can configure up to 64 VLAN tag priorities (i.e., indices 0-63). The valid range of the parameter DiffServ is 0-63. The valid range of the parameter VlanPriority is 0-7. To set a default VLAN Priority (used for ARPs and automated ICMP packets, as well as for IP Packets without DiffServ value), set a VLAN Priority value for DiffServ 0.
Layer-3 Class of Service (TOS/DiffServ) Parameters	
Web: Media Premium QoS EMS: Premium Service Class Media Diff Serv [PremiumServiceClassMediaDiffServ]	Defines the DiffServ value for Premium Media CoS content. The valid range is 0 to 63. The default value is 46. Notes: <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. The value for the Premium Control DiffServ is 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). The valid range is 0 to 63. The default value is 40. Notes: <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. 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. Note: For this parameter to take effect, a device reset is required.
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. Note: For this parameter to take effect, a device reset is required.

12.1.4 NAT Parameters

The Network Address Translation (NAT) parameters are described in the table below.

Table 12-4: NAT Parameters

Parameter	Description
Web/EMS: NAT Traversal [DisableNAT]	Enables or disables the NAT mechanism. <ul style="list-style-type: none">▪ [0] Enable▪ [1] Disable (default)
Web: NAT IP Address EMS: Static NAT IP Address [StaticNatIP]	Global (public) IP address of the device to enable static NAT between the device and the Internet. Note: For this parameter to take effect, a device reset is required.
Web/EMS: Inbound Media Latch Mode [InboundMediaLatchMode]	Enables or disables the receipt of media streams whose IP address/port are not configured for the channel. <ul style="list-style-type: none">▪ [0] Strict = Accepts only the media stream configured for the channel.▪ [1] Dynamic = Accepts any media stream (default).

12.1.5 NFS Parameters

The Network File Systems (NFS) configuration parameters are described in the table below.

Table 12-5: NFS Parameters

Parameter	Description
[NFSBasePort]	<p>Start of the range of numbers used for local UDP ports used by the NFS client. The maximum number of local ports is maximum channels plus maximum NFS servers.</p> <p>The valid range is 0 to 65535. The default is 47000.</p>
Web: NFS Table EMS: NFS Settings	
[NFSServers]	<p>This <i>ini</i> file table parameter defines up to 16 NFS file systems so that the device can access a remote server's shared files and directories for loading cmp, ini, and auxiliary files (using the Automatic Update mechanism). As a file system, the NFS is independent of machine types, OSs, and network architectures. Note that an NFS file server can share multiple file systems. There must be a separate row for each remote file system shared by the NFS file server that needs to be accessed by the device.</p> <p>The format of this <i>ini</i> file table parameter is as follows:</p> <pre>[NFSServers] FORMAT NFSServers_Index = NFSServers_HostOrIP, NFSServers_RootPath, NFSServers_NfsVersion, NFSServers_AuthType, NFSServers_UID, NFSServers_GID, NFSServers_VlanType; [NFSServers]</pre> <p>For example: NFSServers 1 = 101.1.13, /audio1, 3, 1, 0, 1, 1;</p> <p>Notes:</p> <ul style="list-style-type: none"> You can configure up to 16 NFS file systems (where the first index is 0). To avoid terminating current calls, a row must not be deleted or modified while the device is currently accessing files on the remote NFS file system. The combination of host/IP and Root Path must be unique for each index in the table. For example, the table must include only one index entry with a Host/IP of '192.168.1.1' and Root Path of '/audio'. This parameter is applicable only if VLANs are enabled or Multiple IPs is configured. For a detailed description of the table's parameters and to configure NFS using the Web interface, see "Configuring NFS Settings" on page 66. For a description of configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.1.6 DNS Parameters

The Domain name System (DNS) parameters are described in the table below.

Table 12-6: DNS Parameters

Parameter	Description
Web: DNS Primary Server IP EMS: DNS Primary Server [DNSPriServerIP]	The IP address of the primary DNS server. Enter the IP address in dotted-decimal notation, for example, 10.8.2.255. Notes: <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. To use Fully Qualified Domain Names (FQDN) in the 'Outbound IP Routing Table', you must define this parameter.
Web: DNS Secondary Server IP EMS: DNS Secondary Server [DNSSecServerIP]	The IP address of the second DNS server. Enter the IP address in dotted-decimal notation, for example, 10.8.2.255. Note: For this parameter to take effect, a device reset is required.
Web: Internal DNS Table EMS: DNS Information	
[DNS2IP]	This <i>ini</i> file table parameter configures the internal DNS table for resolving host names into IP addresses. Up to four different IP addresses (in dotted-decimal notation) can be assigned to a host name. The format of this parameter is as follows: <pre>[Dns2Ip] FORMAT Dns2Ip_Index = Dns2Ip_DomainName, Dns2Ip_FirstIpAddress, Dns2Ip_SecondIpAddress, Dns2Ip_ThirdIpAddress, Dns2Ip_FourthIpAddress; [Dns2Ip]</pre> For example: Dns2Ip 0 = DnsName, 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4; Notes: <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 91. For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Internal SRV Table EMS: DNS Information	
[SRV2IP]	This <i>ini</i> file table parameter defines the internal SRV table for resolving host names into DNS A-Records. Three different A-Records can be assigned to a host name. Each A-Record contains the host name, priority, weight, and port. The format of this parameter is as follows: <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 92. ▪ For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.1.7 DHCP Parameters

The Dynamic Host Control Protocol (DHCP) parameters are described in the table below.

Table 12-7: DHCP Parameters

Parameter	Description
Web: Enable DHCP EMS: DHCP Enable [DHCPEnable]	<p>Determines whether Dynamic Host Control Protocol (DHCP) is enabled.</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>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"> Enable DHCP and save the configuration. Perform a cold reset using the device's hardware reset button (soft reset using the Web interface doesn't trigger the DHCP procedure and this parameter reverts to 'Disable'). ▪ For additional 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.
EMS: DHCP Speed Factor [DHCPSpeedFactor]	<p>Determines the DHCP renewal speed.</p> <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = Normal (default)

Parameter	Description
	<ul style="list-style-type: none"> ▪ [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>
Web: Enable DHCP Lease Renewal [EnableDHCPLeaseRenewal]	<p>Enables or disables DHCP renewal support.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>This parameter is applicable only if the parameter DHCPEnable is set to 0 for cases where booting up the device using DHCP is not desirable but renewing DHCP leasing is.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>

12.1.8 NTP and Daylight Saving Time Parameters

The Network Time Protocol (NTP) and daylight saving time parameters are described in the table below.

Table 12-8: NTP and Daylight Saving Time Parameters

Parameter	Description
NTP Parameters	
Note: For detailed information on Network Time Protocol (NTP), see "Simple Network Time Protocol Support" on page 619.	
Web: NTP Server IP Address EMS: Server IP Address [NTPServerIP]	The IP address (in dotted-decimal notation) of the NTP server. The default IP address is 0.0.0.0 (i.e., internal NTP client is disabled).
Web: NTP UTC Offset EMS: UTC Offset [NTPServerUTCOffset]	Defines the Universal Time Coordinate (UTC) offset (in seconds) from the NTP server. The default offset is 0. The offset range is -43200 to 43200.
Web: NTP Update Interval EMS: Update Interval [NTPUpdateInterval]	<p>Defines the time interval (in seconds) that the NTP client requests for a time update. The default interval is 86400 (i.e., 24 hours). The range is 0 to 214783647.</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>Determines whether to enable 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. The format of the value is mo:dd:hh:mm (month, day, hour, and minutes).</p>

Parameter	Description
Web: End Time EMS: End [DayLightSavingTimeEnd]	Defines the date and time when daylight saving ends. The format of the value is mo:dd:hh:mm (month, day, hour, and minutes).
Web/EMS: Offset [DayLightSavingTimeOffset]	Daylight saving time offset (in minutes). The valid range is 0 to 120. The default is 60.

12.2 Web and Telnet Parameters

This subsection describes the device's Web and Telnet parameters.

12.2.1 General Parameters

The general Web and Telnet parameters are described in the table below.

Table 12-9: General Web and Telnet Parameters

Parameter	Description
Web: Web and Telnet Access List Table EMS: Web Access Addresses [WebAccessList_x]	<p>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).</p> <p>The default value is 0.0.0.0 (i.e., the device can be accessed from any IP address).</p> <p>For example: WebAccessList_0 = 10.13.2.66 WebAccessList_1 = 10.13.77.7</p> <p>For defining the Web and Telnet Access list using the Web interface, see "Configuring Web and Telnet Access List" on page 77.</p>
Web: Use RADIUS for Web/Telnet Login EMS: Web Use Radius Login [WebRADIUSLogin]	<p>Uses RADIUS queries for Web and Telnet interface authentication.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable. <p>When enabled, logging in to the device's Web and Telnet embedded servers is performed through a RADIUS server. The device contacts a user-defined server and verifies the given user name and password pair against a remote database, in a secure manner.</p> <p>Notes:</p> <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 HTTPOnly 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 73).

12.2.2 Web Parameters

The Web parameters are described in the table below.

Table 12-10: Web Parameters

Parameter	Description
[DisableWebTask]	<p>Disables or 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>HTTP port used for Web management (default is 80).</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 in read-only mode.</p> <ul style="list-style-type: none"> ▪ [0] = Enables modifications of parameters (default). ▪ [1] = Web interface in read-only mode. <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>Note: For this parameter to take effect, a device reset is required.</p>
[ResetWebPassword]	<p>Resets the username and password of the primary and secondary accounts to their defaults.</p> <ul style="list-style-type: none"> ▪ [0] = Password and username retain their values (default). ▪ [1] = Password and username are reset (for the default username and password, see User Accounts). <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).

Parameter	Description
[WelcomeMessage]	<p>This <i>ini</i> file table parameter configures 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 368.

12.2.3 Telnet Parameters

The Telnet parameters are described in the table below. Note: Telnet is currently supported only for debugging from the LAN interface.

Table 12-11: Telnet Parameters

Parameter	Description
Web: Embedded Telnet Server EMS: Server Enable [TelnetServerEnable]	<p>Enables or disables 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 73).</p>
Web: Telnet Server TCP Port EMS: Server Port [TelnetServerPort]	<p>Defines the port number for the embedded Telnet server. The valid range is all valid port numbers. The default port is 23.</p>
Web: Telnet Server Idle Timeout EMS: Server Idle Disconnect [TelnetServerIdleDisconnect]	<p>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.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web/EMS: WAN Telnet Server Port [WanMgmtTelnetPort]	<p>Defines the WAN management port number for the embedded Telnet server. The valid range is all valid port numbers. The default port is 23.</p>

12.3 Debugging and Diagnostics Parameters

This subsection describes the device's debugging and diagnostic parameters.

12.3.1 General Parameters

The general debugging and diagnostic parameters are described in the table below.

Table 12-12: General Debugging and Diagnostic Parameters

Parameter	Description
EMS: Enable Diagnostics [EnableDiagnostics]	<p>Checks the correct functionality of the different hardware components on the device. On completion of the check and if the test fails, the device sends information on the test results of each hardware component to the Syslog server.</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 detailed 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>Determines whether the LAN Watch-Dog feature is enabled.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable LAN Watch-Dog (default). ▪ [1] Enable = Enable LAN Watch-Dog. <p>When LAN Watch-Dog is enabled, the device's overall communication integrity is checked periodically. If no communication is detected for about three minutes, the device performs a self test:</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]	<ul style="list-style-type: none"> ▪ [0] = Disable device's watch dog. ▪ [1] = Enable device's watch dog (default). <p>Note: For this parameter to take effect, a device reset is required.</p>
[LifeLineType]	<p>Defines the scenario upon which the Lifeline phone is activated. The Lifeline phone is available on Port 1 of each FXS module. FXS Port 1 is connected to the POTS (Lifeline) phone as well as to the PSTN/PBX (using a splitter cable). Upon power outage and/or network failure, PSTN connectivity is maintained for the FXS phone user.</p>

Parameter	Description
	<ul style="list-style-type: none"> [0] = Lifeline is activated upon power failure (default). [1] = Lifeline is activated upon power failure or when the link is down (physically disconnected). [2] = Lifeline is activated upon power failure, when the link is down, or upon network failure (logical link disconnected). <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 FXS interfaces. To enable Lifeline switching on network failure, the LAN watch dog must be activated (i.e., set the parameter EnableLANWatchDog to 1). For a detailed description on cabling the device for Lifeline, refer to the Installation Manual.
Web: Delay After Reset [sec] [GWAppDelayTime]	<p>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.</p> <p>Note: This feature helps overcome connection problems caused by some LAN routers or IP configuration parameters' modifications by a DHCP server.</p>

12.3.2 Syslog, CDR and Debug Parameters

The Syslog, CDR and debug parameters are described in the table below.

Table 12-13: Syslog, CDR and Debug Parameters

Parameter	Description
Web: Enable Syslog EMS: Syslog enable [EnableSyslog]	<p>Sends the logs and error message generated by the device to the Syslog server.</p> <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. <p>Notes:</p> <ul style="list-style-type: none"> If you enable Syslog, you must enter an IP address of the Syslog server (using the SyslogServerIP parameter). Syslog messages may increase the network traffic. To configure Syslog SIP message logging levels, use the GwDebugLevel parameter. For information on the Syslog, refer to the <i>Product Reference Manual</i>. By default, logs are also sent to the RS-232 serial port. For information on establishing a serial communications link with the device, refer to the Installation Manual.

Parameter	Description
Web/EMS: Syslog Server IP Address [SyslogServerIP]	The IP address (in dotted-decimal notation) of the computer on which the Syslog server is running. The Syslog server is an application designed to collect the logs and error messages generated by the device. Default IP address is 0.0.0.0. For information on Syslog, refer to the <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 the Syslog, refer to the <i>Product Reference Manual</i> .
[MaxBundleSyslogLength]	The maximum size (in bytes) threshold of logged Syslog messages bundled into a single UDP packet, after which they are sent to a Syslog server. The valid value range is 0 to 1220 (where 0 indicates that no bundling occurs). The default is 1220. Note: This parameter is applicable only if the GWDebugLevel parameter is set to 7.
Web: CDR Server IP Address EMS: IP Address of CDR Server [CDRSyslogServerIP]	Defines the destination IP address to where CDR logs are sent. The default value is a null string, which causes CDR messages to be sent with all Syslog messages to the Syslog server. Notes: <ul style="list-style-type: none"> The CDR messages are sent to UDP port 514 (default Syslog port). This mechanism is active only when Syslog is enabled (i.e., the parameter EnableSyslog is set to 1).
Web/EMS: CDR Report Level [CDRReportLevel]	Determines whether Call Detail Records (CDR) are sent to the Syslog server and when they are sent. <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. Notes: <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]	Syslog debug logging level. <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:

Parameter	Description
	<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>Facility level (0 through 7) for the device's Syslog messages, according to RFC 3164. This allows you to identify Syslog messages generated by the device. This is useful, for example, if you collect the device's and other equipments' Syslog messages, at one single server. The device's Syslog messages can easily be identified and distinguished from other Syslog messages by its Facility level. Therefore, in addition to filtering Syslog messages according to IP address, the messages can be filtered according to Facility level.</p> <ul style="list-style-type: none"> ▪ [16] = local use 0 (local0) - default ▪ [17] = local use 1 (local1) ▪ [18] = local use 2 (local2) ▪ [19] = local use 3 (local3) ▪ [20] = local use 4 (local4) ▪ [21] = local use 5 (local5) ▪ [22] = local use 6 (local6) ▪ [23] = local use 7 (local7)
Web: Activity Types to Report via Activity Log Messages [ActivityListToLog]	<p>The Activity Log mechanism enables the device to send log messages (to a Syslog server) for reporting certain types of Web operations according to the below user-defined filters.</p> <ul style="list-style-type: none"> ▪ [pvc] Parameters Value Change = Changes made on-the-fly to parameters. ▪ [afl] Auxiliary Files Loading = Loading of auxiliary files. ▪ [dr] Device Reset = Reset of device via the 'Maintenance Actions' page. Note: For this option to take effect, a device reset is required. ▪ [fb] Flash Memory Burning = Burning of files or parameters to flash (in 'Maintenance Actions' page). ▪ [swu] Device Software Update = cmp file loading via the Software Upgrade Wizard. ▪ [ard] Access to Restricted Domains = Access to restricted domains, which include the following Web pages: <ul style="list-style-type: none"> ✓ (1) ini parameters (AdminPage)

Parameter	Description
	<ul style="list-style-type: none"> ✓ (2) 'General Security Settings' ✓ (3) 'Configuration File' ✓ ✓ (5) 'Software Upgrade Key' ✓ ✓ (7) 'Web Access List' ✓ (8) 'Web User Accounts' <ul style="list-style-type: none"> ▪ [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', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc'</p> <p>Note: For the <i>ini</i> file, values must be enclosed in single quotation marks.</p>
[FacilityTrace]	<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>

12.3.3 Remote Alarm Indication Parameters

The Remote Alarm Indication (RAI) parameters are described in the table below.

Table 12-14: RAI Parameters

Parameter	Description
[EnableRAI]	<p>Enables RAI alarm generation if the device's busy endpoints exceed a user-defined threshold.</p> <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]	<p>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> <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 Hunt Group Table).</p>

Parameter	Description
[RAILowThreshold]	Low threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints falls below this low threshold, the device sends an SNMP acBoardCallResourcesAlarm alarm trap with a 'cleared' alarm status. The range is 0 to 100%. The default value is 90%.
[RAILoopTime]	Time interval (in seconds) that the device periodically checks call resource availability. The valid range is 1 to 200. The default is 10.

12.3.4 Serial Parameters

The RS-232 serial parameters are described in the table below. (Serial interface is mainly used for debugging.)

Table 12-15: Serial Parameters

Parameter	Description
[DisableRS232]	<p>Enables or disables the device's RS-232 port.</p> <ul style="list-style-type: none"> [0] = RS-232 serial port is enabled. [1] = RS-232 serial port is disabled (default). <p>The RS-232 serial port can be used to change the networking parameters and view error/notification messages. For information on establishing a serial communications link with the device, refer to the <i>Installation Manual</i>.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: Baud Rate [SerialBaudRate]	<p>Determines the value of the RS-232 baud rate. 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>Determines the value of 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>Determines the value of 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>Determines the value of 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>

Parameter	Description
EMS: Flow Control [SerialFlowControl]	<p>Determines the value of 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>

12.4 Security Parameters

This subsection describes the device's security parameters.

12.4.1 General Parameters

The general security parameters are described in the table below.

Table 12-16: General Security Parameters

Parameter	Description
Web: Internal Firewall Parameters EMS: Firewall Settings	
[AccessList]	<p>This <i>ini</i> file table parameter configures the device's access list (firewall), which defines network traffic filtering rules. For each packet received on the network interface, the table is scanned from the top down until a matching rule is found. This rule can either deny (block) or permit (allow) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted.</p> <p>The format of this parameter is as follows: [AccessList] FORMAT AccessList_Index = AccessList_Source_IP, AccessList_PrefixLen, AccessList_Start_Port, AccessList_End_Port, AccessList_Protocol, AccessList_Use_Specific_Interface, AccessList_Interface_ID, AccessList_Packet_Size, AccessList_Byte_Rate, AccessList_Byte_Burst, AccessList_Allow_Type; [AccessList]</p> <p>For example: AccessList 10 = mgmt.customer.com, 32, 0, 80, tcp, 1, OAMP, 0, 0, 0, allow; AccessList 22 = 10.4.0.0, 16, 4000, 9000, any, 0, , 0, 0, 0, block;</p> <p>In the example above, Rule #10 allows traffic from the host 'mgmt.customer.com' destined to TCP ports 0 to 80 on interface OAMP (OAMP). Rule #22 blocks traffic from the subnet 10.4.xxx.yyy destined to ports 4000 to 9000.</p> <p>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 94. ▪ For a description of configuring with <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.4.2 HTTPS Parameters

The Secure Hypertext Transport Protocol (HTTPS) parameters are described in the table below.

Table 12-17: 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>Determines the local Secured HTTPS port of the device. The valid range is 1 to 65535 (other restrictions may apply within this range). The default port is 443.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: HTTPS Cipher String [HTTPSCipherString]	<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 HTTPSCipherString 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.
Web: HTTP Authentication Mode EMS: Web Authentication Mode [WebAuthMode]	<p>Determines the authentication mode for the Web interface.</p> <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]	<p>Requires client certificates for HTTPS connection. The client certificate must be preloaded to the device and its matching private key must be installed on the managing PC. Time and date must be correctly set on the device for the client certificate to be verified.</p> <ul style="list-style-type: none"> ▪ [0] = Client certificates are not required (default). ▪ [1] = Client certificates are required.

Parameter	Description
	Notes: <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 71.

12.4.3 SRTP Parameters

The Secure Real-Time Transport Protocol (SRTP) parameters are described in the table below.

Table 12-18: 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>Notes: 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. If negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted. (default) [1] Mandatory = The device initiates encrypted calls, but if negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected. [2] Disable = The profile does not support encrypted calls (i.e., SRTP). [3] Preferable - Single Media = The device sends SDP with a single media ('m=') line only (e.g., m=audio 6000 RTP/AVP 4 0 70 96) with RTP/AVP and crypto keys. If the remote SIP UA does not support SRTP, it ignores the crypto lines. <p>Notes:</p> <ul style="list-style-type: none"> Before configuring this parameter, set the EnableMediaSecurity parameter to 1. This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).
Web: Master Key Identifier (MKI) Size EMS: Packet MKI Size [SRTPTxPacketMKISize]	<p>Determines the size (in bytes) of the Master Key Identifier (MKI) in SRTP Tx packets. The range is 0 to 4. The default value is 0.</p>
Web/EMS: SRTP offered Suites [SRTPofferedSuites]	<p>Defines the offered crypto suites (cipher encryption algorithms) for SRTP.</p> <ul style="list-style-type: none"> [0] All = All available crypto suites (default) [1] AES_CM_128_HMAC_SHA1_80 = device uses AES-CM

Parameter	Description
	<p>encryption with a 128-bit key and HMAC-SHA1 message authentication with a 80-bit tag.</p> <ul style="list-style-type: none"> [2] AES_CM_128_HMAC_SHA1_32 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag.
Web: Disable Authentication On Transmitted RTP Packets EMS: RTP AuthenticationDisable Tx [RTPAuthenticationDisableTx]	<p>On a secured RTP session, this parameter determines whether to enable authentication on transmitted RTP packets.</p> <ul style="list-style-type: none"> [0] Enable (default) [1] Disable
Web: Disable Encryption On Transmitted RTP Packets EMS: RTP EncryptionDisable Tx [RTPEncryptionDisableTx]	<p>On a secured RTP session, this parameter determines whether to enable encryption on transmitted RTP packets.</p> <ul style="list-style-type: none"> [0] Enable (default) [1] Disable
Web: Disable Encryption On Transmitted RTCP Packets EMS: RTCP EncryptionDisable Tx [RTCPEncryptionDisableTx]	<p>On a secured RTP session, this parameter determines whether to enable encryption on transmitted RTCP packets.</p> <ul style="list-style-type: none"> [0] Enable (default) [1] Disable

12.4.4 TLS Parameters

The Transport Layer Security (TLS) parameters are described in the table below.

Table 12-19: TLS Parameters

Parameter	Description
Web/EMS: TLS Version [TLSVersion]	<p>Defines 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

Parameter	Description
	<p>the client certificate to establish the TLS connection.</p> <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 HTTPSRootFileName.
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 match, the CN value of the SubjectName field is compared with the parameter TLSRemoteSubjectName. If a match is found, the connection is established. Otherwise, the connection is terminated.</p>
Web: TLS Client Verify Server Certificate EMS: Verify Server Certificate [VerifyServerCertificate]	<p>Determines whether the device, when acting as a client for TLS connections, verifies the Server certificate. The certificate is verified with the Root CA information.</p> <ul style="list-style-type: none"> [0] Disable (default). [1] Enable. <p>Note: If Subject Name verification is necessary, the parameter PeerHostNameVerificationMode must be used as well.</p>
Web/EMS: TLS Remote Subject Name [TLSRemoteSubjectName]	<p>Defines the Subject Name that is compared with the name defined in the remote side certificate when establishing TLS connections.</p> <p>If the SubjectAltName of the received certificate is not equal to any of the defined Proxies Host names/IP addresses and is not marked as 'critical', the Common Name (CN) of the Subject field is compared with this value. If not equal, the TLS connection is not established. If the CN uses a domain name, the certificate can also use wildcards (*) to replace parts of the domain name.</p> <p>The valid range is a string of up to 49 characters.</p> <p>Note: This parameter is applicable only if the parameter PeerHostNameVerificationMode is set to 1 or 2.</p>

12.4.5 SSH Parameters

The Secure Shell (SSH) parameters are described in the table below.

Table 12-20: SSH Parameters

Parameter	Description
Web/EMS: SSH Server Enable [SSHServerEnable]	Enables or disables the device's embedded SSH server. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable
Web/EMS: SSH Server Port [SSHServerPort]	Defines the port number for the embedded SSH server. Range is any valid port number. The default port is 22.
Web/EMS: WAN SSH Server Port [WanMgmtSSHPort]	Defines the WAN management port for the embedded SSH server. Range is any valid port number. The default port is 22.
[SSHAdminKey]	Determines the RSA public key for strong authentication to logging in to the SSH interface (if enabled). The value should be a base64-encoded string. The value can be a maximum length of 511 characters. For additional information, refer to the <i>Product Reference Manual</i> .
[SSHMaxLoginAttempts]	Defines the maximum SSH login attempts allowed for entering an incorrect password by an administrator before the SSH session is rejected. The valid range is 1 to 3. the default is 3.
[SSHEnableLastLoginMessage]	Enables or disables the message display in SSH sessions of the time and date of the last SSH login. The SSH login message displays the number of unsuccessful login attempts since the last successful login. <ul style="list-style-type: none"> [0] Disable [1] Enable (default) Note: The last SSH login information is cleared when the device is reset.
[SSHMaxSessions]	Maximum number of simultaneous SSH sessions. The valid range is 1 to 2. The default is 2 sessions.
[SSHRequirePublicKey]	Enables or disables RSA public keys for SSH. <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.
[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]

12.4.6 OCSP Parameters

The Online Certificate Status Protocol (OCSP) parameters are described in the table below.

Table 12-21: OCSP Parameters

Parameter	Description
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> .
EMS: OCSP Server IP [OCSPServerIP]	Defines the IP address of the OCSP server. The default IP address is 0.0.0.0.
[OCSPSecondaryServerIP]	Defines the IP address (in dotted-decimal notation) of the secondary OCSP server (optional). The default IP address is 0.0.0.0.
EMS: OCSP Server Port [OCSPServerPort]	Defines the OCSP server's TCP port number. The default port number is 2560.
EMS: OCSP Default Response [OCSPDefaultResponse]	Determines the default OCSP behavior when the server cannot be contacted. <ul style="list-style-type: none"> [0] = Rejects peer certificate (default). [1] = Allows peer certificate.

12.5 RADIUS Parameters

The RADIUS parameters are described in the table below. For detailed information on the supported RADIUS attributes, see "Supported RADIUS Attributes" on page 609.

Table 12-22: RADIUS Parameters

Parameter	Description
Web: Enable RADIUS Access Control [EnableRADIUS]	Determines whether the RADIUS application is enabled. <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]	IP address of the RADIUS accounting server.
Web: Accounting Port [RADIUSAccPort]	Port of the RADIUS accounting server. The default value is 1646.
Web/EMS: RADIUS Accounting Type [RADIUSAccountingType]	Determines when the RADIUS accounting messages are sent to the RADIUS accounting server. <ul style="list-style-type: none"> [0] At Call Release = Sent at call release only (default).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [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 [AAAIindications]	<p>Determines the Authentication, Authorization and Accounting (AAA) indications.</p> <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]	<p>Defines the device's response upon a RADIUS timeout.</p> <ul style="list-style-type: none"> ▪ [0] Deny Access = Denies access. ▪ [1] Verify Access Locally = Checks password locally (default).
[MaxRADIUSSessions]	<p>Number of concurrent calls that can communicate with the RADIUS server (optional). The valid range is 0 to 240. The default value is 240.</p>
[RADIUSRetransmission]	<p>Number of retransmission retries. The valid range is 1 to 10. The default value is 3.</p>
[RadiusTO]	<p>Determines the time interval (measured in seconds) the device waits for a response before a RADIUS retransmission is issued. The valid range is 1 to 30. The default value is 10.</p>
Web: RADIUS Authentication Server IP Address [RADIUSAuthServerIP]	<p>IP address of the RADIUS authentication server. Note: For this parameter to take effect, a device reset is required.</p>
Web: RADIUS Authentication Server Port [RADIUSAuthPort]	<p>RADIUS Authentication Server Port. Note: For this parameter to take effect, a device reset is required.</p>
Web: RADIUS Shared Secret [SharedSecret]	<p>'Secret' used to authenticate the device to the RADIUS server. This should be a cryptically strong password.</p>
Web: Default Access Level [DefaultAccessLevel]	<p>Defines the default access level for the device when the RADIUS (authentication) response doesn't include an access level attribute. The valid range is 0 to 255. The default value is 200 (Security Administrator').</p>
Web: Local RADIUS Password Cache Mode [RadiusLocalCacheMode]	<p>Defines the device's mode of operation regarding the timer (configured by the parameter RadiusLocalCacheTimeout) that determines the validity of the user name and password (verified by the RADIUS server).</p> <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]	<p>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).</p> <ul style="list-style-type: none"> ▪ [-1] = Never expires. ▪ [0] = Each request requires RADIUS authentication.

Parameter	Description
Web: RADIUS VSA Vendor ID [RadiusVSAVendorID]	Defines the vendor ID that the device accepts when parsing a RADIUS response packet. The valid range is 0 to 0xFFFFFFFF. The default value is 5003.
Web: RADIUS VSA Access Level Attribute [RadiusVSAAccessAttribute]	Defines the code that indicates the access level attribute in the Vendor Specific Attributes (VSA) section of the received RADIUS packet. The valid range is 0 to 255. The default value is 35.

12.6 SNMP Parameters

The SNMP parameters are described in the table below.

Table 12-23: SNMP Parameters

Parameter	Description
Web: Enable SNMP [DisableSNMP]	Determines whether SNMP is enabled. <ul style="list-style-type: none"> ▪ [0] Enable = SNMP is enabled (default). ▪ [1] Disable = SNMP is disabled and no traps are sent.
[SNMPPort]	The device's local UDP port used for SNMP Get/Set commands. The range is 100 to 3999. The default port is 161. Note: For this parameter to take effect, a device reset is required.
[SNMPTrustedMGR_x]	Defines up to five IP addresses of remote trusted SNMP managers from which the SNMP agent accepts and processes SNMP Get and Set requests. Notes: <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]	This object is an 'alias' name 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]	This object is a user-assigned asset tracking identifier 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.

Parameter	Description
[ifAlias]	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]	The port to which the keep-alive traps are sent. The valid range is 0 - 65534. The default is port 162.
[SendKeepAliveTrap]	When enabled, this parameter invokes the keep-alive trap and sends it every 9/10 of the time defined in the parameter defining NAT Binding Default Timeout. <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = Enable Note: For this parameter to take effect, a device reset is required.
[SNMPSysOid]	Defines the base product system OID. The default is eSNMP_AC_PRODUCT_BASE_OID_D. Note: For this parameter to take effect, a device reset is required.
[SNMPTrapEnterpriseOid]	Defines a Trap Enterprise OID. The default is eSNMP_AC_ENTERPRISE_OID. The inner shift of the trap in the AcTrap subtree is added to the end of the OID in this parameter. Note: For this parameter to take effect, a device reset is required.
[acUserInputAlarmDescription]	Defines the description of the input alarm.
[acUserInputAlarmSeverity]	Defines the severity of the input alarm.
[AlarmHistoryTableMaxSize]	Determines the maximum number of rows in the Alarm History table. This parameter can be controlled by the Config Global Entry Limit MIB (located in the Notification Log MIB). The valid range is 50 to 1000. The default value is 500. Note: For this parameter to take effect, a device reset is required.
[SNMPEngineIDString]	Defines the SNMP engine ID for SNMPv2/SNMPv3 agents. This is used for authenticating a user attempting to access the SNMP agent on the device. The ID can be a string of up to 36 characters. The default value is 00:00:00:00:00:00:00:00:00:00:00:00:00:00 (12 Hex octets characters). The provided key must be set with 12 Hex values delimited by a colon (":") in the format xx:xx:....xx. For example, 00:11:22:33:44:55:66:77:88:99:aa:bb Notes: <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.

Parameter	Description
Web: SNMP Trap Destination Parameters EMS: Network > SNMP Managers Table Note: Up to five SNMP trap managers can be defined.	
SNMP Manager [SNMPManagerIsUsed_x]	Determines the validity of the parameters (IP address and port number) of the corresponding SNMP Manager used to receive SNMP traps. <ul style="list-style-type: none"> ▪ [0] (Check box cleared) = Disabled (default) ▪ [1] (Check box selected) = Enabled
Web: IP Address EMS: Address [SNMPManagerTableIP_x]	Defines the IP address of the remote host used as an SNMP Manager. The device sends SNMP traps to this IP address. Enter the IP address in dotted-decimal notation, e.g., 108.10.1.255.
Web: Trap Port EMS: Port [SNMPManagerTrapPort_x]	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port. The valid SNMP trap port range is 100 to 4000. The default port is 162.
Web: Trap Enable [SNMPManagerTrapSendingEnable_x]	Activates or de-activates the sending of traps to the corresponding SNMP Manager. <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: 'mngr.corp.mycompany.com'. The valid range is a 99-character string.
SNMP Community String Parameters	
Community String [SNMPReadOnlyCommunityString_x]	Defines up to five read-only SNMP community strings (up to 19 characters each). The default string is 'public'.
Community String [SNMPReadWriteCommunityString_x]	Defines up to five read/write SNMP community strings (up to 19 characters each). The default string is 'private'.
Trap Community String [SNMPTrapCommunityString]	Community string used in traps (up to 19 characters). The default string is 'trapuser'.

Parameter	Description
Web: SNMP V3 Table EMS: SNMP V3 Users	
[SNMPUsers]	<p>This <i>ini</i> file table parameter configures SNMP v3 users. The format of this parameter is as follows:</p> <pre>[SNMPUsers] FORMAT SNMPUsers_Index = SNMPUsers_Username, SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol, SNMPUsers_AuthKey, SNMPUsers_PrivKey, SNMPUsers_Group; [SNMPUsers]</pre> <p>For example: SNMPUsers 1 = v3admin1, 1, 0, myauthkey, -, 1; The example above configures user 'v3admin1' with security level authNoPriv(2), authentication protocol MD5, authentication text password 'myauthkey', and ReadWriteGroup2.</p> <p>Notes:</p> <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 81. ▪ For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368

12.7 SIP Media Realm Parameters

The SIP Media Realm parameters are described in the table below.

Table 12-24: SIP Media Realm Parameters

Parameter	Description
Web: Default CP Media Realm Name EMS: Default Realm Name [cpDefaultMediaRealmName]	For a description of this parameter, see "Configuring Media Realms" on page 109.
Web: SIP Media Realm Table EMS: Protocol Definition > Media Realm	
[CpMediaRealm]	<p>This <i>ini</i> file table parameter configures the SIP Media Realm table. The Media Realm table allows you to divide a Media-type interface (defined in the 'Multiple Interface' table) into several realms, where each realm is specified by a UDP port range.</p> <p>The format of this parameter is as follows:</p> <pre>[CpMediaRealm] FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd; [CpMediaRealm]</pre>

Parameter	Description
	<p>For example, CpMediaRealm 1 = Mrealm1, Voice, , 6600, 20, 6790; CpMediaRealm 2 = Mrealm2, Voice, , 6800, 10, 6890;</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. The parameter cpDefaultRealmName can be used to define one of the Media Realms appearing in this table as the default Media Realm. If the parameter cpDefaultRealmName is not configured, then the first Media Realm appearing in this table is set as default. If this table is not configured, then the default Media Realm includes all defined media interfaces. A Media Realm can be assigned to an IP Group (in the 'IP Group' table) or an SRD (in the 'SRD' table). If different Media Realms are assigned to both an IP Group and SRD, the IP Group's Media Realm takes precedence. 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 109. For a description on configuring ini file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.8 Control Network Parameters

12.8.1 IP Group, Proxy, Registration and Authentication Parameters

The proxy server, registration and authentication SIP parameters are described in the table below.

Table 12-25: Proxy, Registration and Authentication SIP Parameters

Parameter	Description
Web: IP Group Table EMS: Endpoints > IP Group	
[IPGroup]	<p>This <i>ini</i> file table parameter configures the IP Group table. The format of this parameter is as follows:</p> <pre>[IPGroup] FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description, IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_EnableSurvivability, IPGroup_ServingIPGroup, IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable, IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm, IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet,</pre>

Parameter	Description
	<p>IPGroup_OutboundManSet, IPGroup_ContactName; [IPGroup]</p> <p>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, ;</p> <p>Notes:</p> <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). 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 119. For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Authentication Table EMS: SIP Endpoints > Authentication	
[Authentication]	<p>This ini file table parameter defines a user name and password for authenticating each device port. The format of this parameter is as follows: [Authentication] FORMAT Authentication_Index = Authentication_UserId, Authentication_UserPassword, Authentication_Module, Authentication_Port; [Authentication]</p> <p>Where,</p> <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) <p>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)</p> <p>Notes:</p> <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 is not configured, the port's phone number (configured using the parameter TrunkGroup - Hunt Group Table) and global password (using the

Parameter	Description
	<p>individual parameter Password) are used for authentication.</p> <ul style="list-style-type: none"> 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 183. For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Account Table EMS: SIP Endpoints > Account	
[Account]	<p>This <i>ini</i> file table parameter configures the Account table for registering and/or authenticating (digest) Hunt 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:</p> <pre>[Account] FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup, Account_ServingIPGroup, Account_Username, Account_Password, Account_HostName, Account_Register, Account_ContactUser, Account_ApplicationType; [Account]</pre> <p>For example: Account 1 = 1, -1, 1, user, 1234, acl, 1, ITSP1, 0;</p> <p>Notes:</p> <ul style="list-style-type: none"> This table can include up to 32 indices (where 1 is the first index). You can define multiple table indices with the same ServedTrunkGroup but different ServingIPGroups, username, password, HostName, and ContactUser. This provides the capability for registering the same Hunt Group 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 133. For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Proxy Registration Parameters	
Web: Use Default Proxy EMS: Proxy Used [IsProxyUsed]	<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 126). <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 165).</p>

Parameter	Description
Web/EMS: Proxy Name [ProxyName]	<p>Defines the Home Proxy domain name. If specified, this name is used as the Request-URI in REGISTER, INVITE, and other SIP messages, and as the host part of the To header in INVITE messages. If not specified, the Proxy IP address is used instead.</p> <p>The value must be string of up to 49 characters.</p>
Web: Redundancy Mode EMS: Proxy Redundancy Mode [ProxyRedundancyMode]	<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>
Web: Proxy IP List Refresh Time EMS: IP List Refresh Time [ProxyIPListRefreshTime]	<p>Defines the time interval (in seconds) between each Proxy IP list refresh.</p> <p>The range is 5 to 2,000,000. The default interval is 60.</p>
Web: Enable Fallback to Routing Table EMS: Fallback Used [IsFallbackUsed]	<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). [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>

Parameter	Description
	<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 <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</p>

Parameter	Description
	<p>performed.</p> <p>Note: To enable NAPTR/SRV queries for Proxy servers only, use the parameter ProxyDNSQueryType.</p>
Web: Proxy DNS Query Type [ProxyDNSQueryType]	<p>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers.</p> <ul style="list-style-type: none"> ▪ [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.</p> <p>Note: When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNSQueryType is disabled.</p>
Web/EMS: Graceful Busy Out Timeout [sec] [GracefulBusyOutTimeout]	<p>Determines 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> <p>Note: This parameter is applicable only to digital interfaces.</p>
Web/EMS: Use Gateway Name for OPTIONS [UseGatewayNameForOptions]	<p>Determines whether the device uses its IP address or gateway name in keep-alive SIP OPTIONS messages.</p> <ul style="list-style-type: none"> ▪ [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.

Parameter	Description
	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]	<p>User name used for Registration and Basic/Digest authentication with a Proxy/Registrar server. The default value is an empty string.</p> <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 183).
Web/EMS: Password [Password]	<p>The password used for Basic/Digest authentication with a Proxy/Registrar server. A single password is used for all device ports. The default is 'Default_Passwd'.</p> <p>Note: Instead of configuring this parameter, the Authentication table can be used (see Authentication on page 183).</p>
Web/EMS: Cnonce [Cnonce]	<p>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'.</p>
Web/EMS: Mutual Authentication Mode [MutualAuthenticationMode]	<p>Determines the device's mode of operation when Authentication and Key Agreement (AKA) Digest Authentication is used.</p> <ul style="list-style-type: none"> ▪ [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]	<p>Determines the mode for Challenge Caching, which reduces the number of SIP messages transmitted through the network. The first request to the Proxy is sent without authorization. The Proxy sends a 401/407 response with a challenge. This response is saved for further uses. A new request is re-sent with the appropriate credentials. Subsequent requests to the Proxy are automatically sent with credentials (calculated from the saved challenge). If the Proxy doesn't accept the new request and sends another challenge, the old challenge is replaced with the new one.</p> <ul style="list-style-type: none"> ▪ [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. ▪ [2] Full = Caches all challenges from the proxies.

Parameter	Description
	<p>Note: Challenge Caching is used with all proxies and not only with the active one.</p>
Web: Proxy IP Table EMS: Proxy IP	
[ProxyIP]	<p>This <i>ini</i> file table parameter configures the Proxy Set table with Proxy Set IDs, each with up to five Proxy server IP addresses (or fully qualified domain name/FQDN). Each Proxy Set can be defined with a transport type (UDP, TCP, or TLS). The format of this parameter is as follows:</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 126. ▪ For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Proxy Set Table EMS: Proxy Set	
[ProxySet]	<p>This <i>ini</i> file table parameter 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>

Parameter	Description
	<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. 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 126. For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Registrar Parameters	
Web: Enable Registration EMS: Is Register Needed [IsRegisterNeeded]	<p>Enables the device to register to a Proxy/Registrar server.</p> <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]	<p>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.</p> <p>The valid range is up to 49 characters.</p>
Web: Registrar IP Address EMS: Registrar IP [RegistrarIP]	<p>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> <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.

Parameter	Description
Web/EMS: Registrar Transport Type [RegistrarTransportType]	<p>Determines the transport layer used for outgoing SIP dialogs initiated by the device to the Registrar.</p> <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]	<p>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.</p>
Web: Re-registration Timing [%] EMS: Time Divider [RegistrationTimeDivider]	<p>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).</p> <p>Note: This parameter may be overridden if the parameter RegistrationTimeThreshold is greater than 0.</p>
Web/EMS: Registration Retry Time [RegistrationRetryTime]	<p>Defines the time interval (in seconds) after which a registration request is re-sent if registration fails with a 4xx response or if there is no response from the Proxy/Registrar server. The default is 30 seconds. The range is 10 to 3600.</p>
Web: Registration Time Threshold EMS: Time Threshold [RegistrationTimeThreshold]	<p>Defines a threshold (in seconds) for re-registration timing. If this parameter is greater than 0, but lower than the computed re-registration timing (according to the parameter RegistrationTimeDivider), the re-registration timing is set to the following: timing set by the Registration server in the SIP Expires header minus the value of the parameter RegistrationTimeThreshold. The valid range is 0 to 2,000,000. The default value is 0.</p>
Web: Re-register On INVITE Failure EMS: Register On Invite Failure [RegisterOnInviteFailure]	<p>Enables immediate re-registration if no response is received for an INVITE request sent by the device.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>When enabled, the device immediately expires its re-registration timer and commences re-registration to the same Proxy upon any of the following scenarios:</p> <ul style="list-style-type: none"> ▪ 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

Parameter	Description
	<p>outbound proxy server failure).</p> <ul style="list-style-type: none"> ▪ 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]	<p>Enables the device to perform SIP re-registration upon TCP/TLS connection failure.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Web: Gateway Registration Name EMS: Name [GWRegistrationName]	<p>Defines the user name that is used in the From and To headers in SIP REGISTER messages. If no value is specified (default) for this parameter, the UserName parameter is used instead.</p> <p>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.</p>
Web/EMS: Authentication Mode [AuthenticationMode]	<p>Determines the device's registration and authentication method.</p> <ul style="list-style-type: none"> ▪ [0] Per Endpoint = Registration and authentication is performed separately for each endpoint/B-channel. ▪ [1] Per Gateway = Single registration and authentication for the entire device (default). ▪ [3] Per FXS = Registration and authentication for FXS endpoints. <p>Typically, authentication per endpoint is used for FXS interfaces, where each endpoint registers (and authenticates) separately with its own user name and password. Single registration and authentication (Authentication Mode = 1) is usually defined for FXO and digital modules.</p>

Parameter	Description
Web: Set Out-Of-Service On Registration Failure EMS: Set OOS On Registration Fail [OOSOnRegistrationFail]	<p>Enables setting an endpoint, trunk, or the entire device (i.e., all endpoints) to out-of-service if registration fails.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <p>If the registration is per endpoint (i.e., AuthenticationMode is set to 0) or per Account (see "Configuring Hunt Group Settings" on page 148) 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 Hunt Group fail registration and if the Hunt Group comprises a complete trunk, then the entire trunk is set to out-of-service.</p> <p>Note: The out-of-service method is configured using the parameter FXSOOSBehavior.</p>
[UnregistrationMode]	<p>Determines whether the device performs an explicit unregister.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable = The device sends an asterisk ("*") value in the SIP Contact header, instructing the Registrar server to remove all previous registration bindings. <p>When enabled, the device removes SIP User Agent (UA) registration bindings in a Registrar, according to RFC 3261. Registrations are soft state and expire unless refreshed, but they can also be explicitly removed. A client can attempt to influence the expiration interval selected by the Registrar. A UA requests the immediate removal of a binding by specifying an expiration interval of "0" for that contact address in a REGISTER request. UA's should support this mechanism so that bindings can be removed before their expiration interval has passed. Use of the "*" Contact header field value allows a registering UA to remove all bindings associated with an address-of-record (AOR) without knowing their precise values.</p> <p>Note: The REGISTER-specific Contact header field value of "*" applies to all registrations, but it can only be used if the Expires header field is present with a value of "0".</p>
Web/EMS: Add Empty Authorization Header [EmptyAuthorizationHeader]	<p>Determines whether the SIP Authorization header is included in initial registration (REGISTER) requests sent by the device.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <p>The Authorization header carries the credentials of a user agent (UA) in a request to a server. The sent REGISTER message populates the Authorization header with the following parameters:</p> <ul style="list-style-type: none"> username - set to the value of the private user identity realm - set to the domain name of the home network uri - set to the SIP URI of the domain name of the home network nonce - set to an empty value

Parameter	Description
	<ul style="list-style-type: none"> ▪ 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>Determines whether the SIP Route header is included 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>Determines whether the carriage-return and line-feed sequences (CRLF) Keep-Alive mechanism, according to RFC 5626 "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)" is used for reliable, connection-orientated transport types such as TCP.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>The SIP user agent/client (i.e., device) uses a simple periodic message as a keep-alive mechanism to keep their flow to the proxy or registrar alive (used for example, to keep NAT bindings open). For connection-oriented transports such as TCP/TLS this is based on CRLF. This mechanism uses a client-to-server "ping" keep-alive and a corresponding server-to-client "pong" message. This ping-pong sequence allows the client, and optionally the server, to tell if its flow is still active and useful for SIP traffic. If the client does not receive a pong in response to its ping, it declares the flow "dead" and opens a new flow in its place. In the CRLF Keep-Alive mechanism the client periodically (defined by the PingPongKeepAliveTime parameter) sends a double-CRLF (the "ping") then waits to receive a single CRLF (the "pong"). If the client does not receive a "pong" within an appropriate amount of time, it considers the flow failed.</p> <p>Note: The device sends a CRLF message to the Proxy Set only if the Proxy Keep-Alive feature (EnableProxyKeepAlive parameter) is enabled and its transport type is set to TCP or TLS. The device first sends a SIP OPTION message to establish the TCP/TLS connection and if it receives any SIP response, it continues sending the CRLF keep-alive sequences.</p>

Parameter	Description
[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>

12.8.2 Network Application Parameters

The SIP network application parameters are described in the table below.

Table 12-26: SIP Network Application Parameters

Parameter	Description
Web: Signaling Routing Domain (SRD) Table EMS: SRD Table	
[SRD]	<p>This <i>ini</i> file table parameter 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). ▪ 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 114. ▪ For a description on configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: SIP Interface Table EMS: SIP Interfaces Table	
[SIPInterface]	<p>This <i>ini</i> file table parameter configures the SIP Interface table. The SIP Interface represents a SIP signaling entity, comprising ports (UDP, TCP, and TLS) and associated with a specific IP interface and an SRD ID. The format of this parameter is as follows:</p> <pre>[SIPInterface] FORMAT SIPInterface_Index = SIPInterface_NetworkInterface, SIPInterface_ApplicationType, SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD; [SIPInterface]</pre> <p>For example:</p>

Parameter	Description
	<p>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 three different SIP Interfaces per SRD, where each SIP Interface pertains to a different application type (i.e., GW, SAS, and SBC). ▪ 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 117. ▪ For a description on configuring <i>ini</i> file table parameters, see "Format of ini File Table Parameters" on page 368.
Static NAT Table	
[NATTranslation]	<p>This <i>ini</i> file table parameter defines NAT rules for translating source IP addresses per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses. This allows, for example, the separation of VoIP traffic between different ISTP's, and topology hiding (of internal IP addresses to the "public" network). Each IP interface (configured in the Multiple Interface table - InterfaceTable parameter) can be associated with a NAT rule in this table, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range).</p> <p>The format of this parameter is as follows:</p> <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. ▪ The device's priority method for performing NAT is as follows (not relevant for SBC application): <ol 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.

Parameter	Description
	<ul style="list-style-type: none"> 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.

12.9 General SIP Parameters

The general SIP parameters are described in the table below.

Table 12-27: General SIP Parameters

Parameter	Description
Web/EMS: Max SIP Message Length [KB] [MaxSIPMessageLength]	<p>Defines the maximum size (in Kbytes) for each SIP message that can be sent over the network. The device rejects messages exceeding this user-defined size.</p> <p>The valid value range is 1 to 50. The default is 50.</p>
[SIPForceRport]	<p>Determines whether the device sends SIP responses to the UDP port from where SIP requests are received even if the 'rport' parameter is not present in the SIP Via header.</p> <ul style="list-style-type: none"> [0] (default) = Disabled - the device sends the SIP response to the UDP port defined in the Via header. If the Via header contains the 'rport' parameter, the response is sent to the UDP port from where the SIP request is received. [1] = Enabled - SIP responses are sent to the UDP port from where SIP requests are received even if the 'rport' parameter is not present in the Via header.
Web: Max Number of Active Calls EMS: Maximum Concurrent Calls [MaxActiveCalls]	<p>Defines the maximum number of simultaneous active calls supported by the device. If the maximum number of calls is reached, new calls are not established.</p> <p>The valid range is 1 to the maximum number of supported channels. The default value is the maximum available channels (i.e., no restriction on the maximum number of calls).</p>
Web: Number of Calls Limit [CallLimit]	<p>Maximum number of concurrent calls, per IP Profile. If the IP Profile is set to some limit, the device maintains the number of concurrent calls (incoming and outgoing) pertaining to the specific profile. When the number of concurrent calls is equal to the limit, the device rejects any new incoming and outgoing calls belonging to that profile.</p> <ul style="list-style-type: none"> [-1] = There is no limitation on calls for that IP Profile (default). [0] = Calls are rejected. <p>Note: This parameter can only be configured for an IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).</p>
Web: QoS statistics in SIP Release Call [QoSStatistics]	<p>Determines whether the device includes call quality of service (QoS) statistics in SIP BYE and SIP 200 OK response to BYE, using the proprietary SIP header, X-RTP-Stat.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable <p>The X-RTP-Stat header provides the following statistics:</p>

Parameter	Description
	<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,PRACK ,REFER,INFO,SUBSCRIBE,UPDATE User-Agent: Sip-Gateway-/v.6.2A.008.006 Reason: Q.850 ;cause=16 ;text="local" Content-Length: 0 </pre>
Web/EMS: PRACK Mode [PrackMode]	<p>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> <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.
Web/EMS: Enable Early Media [EnableEarlyMedia]	<p>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>For Analog interfaces: Note that to send a 183 response, you must also</p>

Parameter	Description
	<p>set the parameter ProgressIndicator2IP to 1. If it is equal to 0, 180 Ringing response is sent.</p> <p>For Digital interfaces: Sending a 183 response depends on the ISDN Progress Indicator (PI). It is sent only if PI is set to 1 or 8 in the received Proceeding or Alerting PRI messages. For CAS protocol, see the ProgressIndicator2IP parameter.</p> <p>Notes:</p> <ul style="list-style-type: none"> You can also configure early SIP 183 response immediately upon receipt of an INVITE, using the EnableEarly183 parameter. This parameter can be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143) and per Tel profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 141).
Web/EMS: Enable Early 183 [EnableEarly183]	<p>Determines whether the device sends a SIP 183 response with SDP to the IP immediately upon receipt of an INVITE message (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.
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.
Web: Session-Expires Time EMS: Sip Session Expires [SIPSessionExpires]	<p>Determines the numerical value that is sent in the Session-Expires header in the first INVITE request or response (if the call is answered). The valid range is 1 to 86,400 sec. The default is 0 (i.e., the Session-Expires header is disabled).</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>

Parameter	Description
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). [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]	<p>Determines whether the device removes the 'to' header tag from final SIP failure responses to INVITE transactions.</p> <ul style="list-style-type: none"> [0] = Do not remove tag (default). [1] = Remove tag.
[EnableRTCPAttribute]	<p>Enables or disables the use of the 'rtcp' attribute in the outgoing SDP.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable
EMS: Options User Part [OPTIONSUserPart]	<p>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.</p> <p>A special value is 'empty', indicating that no user part in the Request-URI (host part only) is used.</p> <p>The valid range is a 30-character string. The default value is an empty string ("").</p>
Web: Fax Signaling Method EMS: Fax Used [IsFaxUsed]	<p>Determines the SIP signaling method for establishing and transmitting a fax session after a fax is detected.</p> <ul style="list-style-type: none"> [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 Canceller = On ✓ Silence Compression = Off ✓ Echo Canceller Non-Linear Processor Mode = Off ✓ Dynamic Jitter Buffer Minimum Delay = 40 ✓ Dynamic Jitter Buffer Optimization Factor = 13 If the device initiates a fax session using G.711 (option 2 and possibly 3), a 'gpmd' attribute is added to the SDP in the following format: <ul style="list-style-type: none"> ✓ For A-law: 'a=gpmd:8 vbd=yes;ecan=on' ✓ For μ-law: 'a=gpmd:0 vbd=yes;ecan=on' When this parameter is set to 1, 2, or 3, the parameter FaxTransportMode is ignored.

Parameter	Description
	<ul style="list-style-type: none"> When this parameter is set to 0, T.38 might still be used without the control protocol's involvement. To completely disable T.38, set FaxTransportMode to a value other than 1. This parameter can also be configured per IP Profile (using the IPProfile parameter). For detailed information on fax transport methods, see "Fax/Modem Transport Modes" on page 443.
Web: SIP Transport Type EMS: Transport Type [SIPTransportType]	<p>Determines the default transport layer for outgoing SIP calls initiated by the device.</p> <ul style="list-style-type: none"> [0] UDP (default) [1] TCP [2] TLS (SIPS) <p>Notes:</p> <ul style="list-style-type: none"> It's recommended to use TLS for communication with a SIP Proxy and not for direct device-to-device communication. For received calls (i.e., incoming), the device accepts all these protocols. The value of this parameter is also used by the SAS application as the default transport layer for outgoing SIP calls. 50
Web: SIP UDP Local Port EMS: Local SIP Port [LocalSIPPort]	<p>Local UDP port for SIP messages. The valid range is 1 to 65534. The default value is 5060.</p>
Web: SIP TCP Local Port EMS: TCP Local SIP Port [TCPLocalSIPPort]	<p>Local TCP port for SIP messages. The valid range is 1 to 65535. The default value is 5060.</p>
Web: SIP TLS Local Port EMS: TLS Local SIP Port [TLSTLocalSIPPort]	<p>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.</p>
Web/EMS: Enable SIPS [EnableSIPS]	<p>Enables secured SIP (SIPS URI) connections over multiple hops.</p> <ul style="list-style-type: none"> [0] Disable (default). [1] Enable. <p>When the parameter SIPTransportType is set to 2 (i.e., TLS) and the parameter EnableSIPS is disabled, TLS is used for the next network hop only. When the parameter SIPTransportType is set to 2 or 1 (i.e., TCP or TLS) and EnableSIPS is enabled, TLS is used through the entire connection (over multiple hops). Note: If this parameter is enabled and the parameter SIPTransportType is set to 0 (i.e., UDP), the connection fails.</p>
Web/EMS: Enable TCP Connection Reuse [EnableTCPConnectionReuse]	<p>Enables the reuse of the same TCP connection for all calls to the same destination.</p> <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	<p>Determines whether all TCP/TLS connections are set as persistent and therefore, not released.</p>

Parameter	Description
Mode [ReliableConnectionPersistentMode]	<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. <p>While trying to send a SIP message connection, reuse policy determines whether live connections to the specific destination are re-used.</p> <p>Persistent TCP connection ensures less network traffic due to fewer setting up and tearing down of TCP connections and reduced latency on subsequent requests due to avoidance of initial TCP handshake. For TLS, persistent connection may reduce the number of costly TLS handshakes to establish security associations, in addition to the initial TCP connection set up.</p> <p>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>SIP destination port for sending initial SIP requests.</p> <p>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.

Parameter	Description											
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 last entry, and concatenates a new destination to it (if an additional request is sent). The order of the reasons is as follows: <ol style="list-style-type: none"> Q.850 Reason SIP Reason SIP Response code Upon receiving the final response (success or failure), the device searches for a Redirect reason in the History-Info (i.e., 3xx/4xx SIP reason). If found, it is passed to ISDN according to the following table: <table border="1"> <thead> <tr> <th>SIP Reason Code</th><th>ISDN Redirecting Reason</th></tr> </thead> <tbody> <tr> <td>302 - Moved Temporarily</td><td>Call Forward Universal (CFU)</td></tr> <tr> <td>408 - Request Timeout</td><td rowspan="3">Call Forward No Answer (CFNA)</td></tr> <tr> <td>480 - Temporarily Unavailable</td></tr> <tr> <td>487 - Request Terminated</td></tr> <tr> <td>486 - Busy Here</td><td rowspan="2">Call Forward Busy (CFB)</td></tr> <tr> <td>600 - Busy Everywhere</td></tr> </tbody> </table> <ul style="list-style-type: none"> 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: Tel2IP Default Redirect Reason [Tel2IPDefaultRedirectReason]	<p>Default redirect reason for Tel-to-IP calls when no redirect reason (or “unknown”) exists in the received Q931 ISDN Setup message. The device includes this default redirect reason in the SIP History-Info header of the outgoing INVITE.</p> <p>If a redirect reason exists in the received Setup message, this parameter is ignored and the device sends the INVITE message with the reason according to the received Setup message. If this parameter is not configured (-1), the outgoing INVITE is sent with the redirect reason as received in the Setup message (if none or “unknown” reason, then without a reason).</p> <ul style="list-style-type: none"> [-1] Not Configured (default) = Received redirect reason is not changed [1] Busy = Call forwarding busy 											

Parameter	Description
	<ul style="list-style-type: none"> ▪ [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: Use Tgrp Information EMS: Use SIP Tgrp [UseSIP Tgrp]	<p>Determines whether the SIP 'tgrp' parameter is used. This SIP parameter specifies the Hunt Group to which the call belongs (according to RFC 4904). For example, the SIP message below indicates that the call belongs to Hunt Group ID 1: INVITE sip::+16305550100;tgrp=1;trunk-context=example.com@10.1.0.3;user=phone SIP/2.0</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) = The 'tgrp' parameter isn't used. ▪ [1] Send Only = The Hunt Group number is added to the 'tgrp' parameter value in the Contact header of outgoing SIP messages. If a Hunt Group number is not associated with the call, the 'tgrp' parameter isn't included. If a 'tgrp' value is specified in incoming messages, it is ignored. ▪ [2] Send and Receive = The functionality of outgoing SIP messages is identical to the functionality described in option 1. In addition, for incoming SIP INVITEs, if the Request-URI includes a 'tgrp' parameter, the device routes the call according to that value (if possible). The Contact header in the outgoing SIP INVITE (Tel-to-IP call) contains "tgrp=<source trunk group ID>;trunk-context=<gateway IP address>". The <source trunk group ID> is the Hunt Group ID where incoming calls from Tel is received. For IP-Tel calls, the SIP 200 OK device's response contains "tgrp=<destination trunk group ID>;trunk-context=<gateway IP address>". The <destination trunk group ID> is the Hunt Group ID used for outgoing Tel calls. The <gateway IP address> in "trunk-context" can be configured using the parameter SIPGatewayName. ▪ [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: INVITE sip:1234567;tgrp=hotline-ccdata;trunk-context=dsn.mil@example.com ✓ 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

Parameter	Description
	<p>the Bearer Capability IE contains "Speech", the INVITE in this case does not contain tgrp and trunk-context parameters.</p> <ul style="list-style-type: none"> ▪ [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 [TGRP Routing Precedence]	<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 Hunt Group parameters for routing the call. ▪ [1] = The device first places precedence on the 'tgrp' parameter for IP-to-Tel routing. If the received INVITE Request-URI does not contain the 'tgrp' parameter or if the Hunt Group number is not defined, then the 'Inbound IP Routing Table' is used for routing the call. <p>Below is an example of an INVITE Request-URI with the 'tgrp' parameter, indicating that the IP call should be routed to Hunt Group 7:</p> <p>INVITE sip:200;tgrp=7;trunk-context=example.com@10.33.2.68;user=phone SIP/2.0</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For enabling routing based on the 'tgrp' parameter, the UseSIPtgrp parameter must be set to 2. ▪ For IP-to-Tel routing based on the 'dtg' parameter (instead of the 'tgrp' parameter), use the parameter UseBroadsoftDTG.
[UseBroadsoftDTG]	<p>Determines whether the device uses the 'dtg' parameter for routing IP-to-Tel calls to a specific Hunt 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 Hunt Group according to its value. This parameter is used instead of the 'tgrp/trunk-context' parameters. The 'dtg' parameter appears in the INVITE Request-URI (and in the To header).</p> <p>For example, the received SIP message below routes the call to Hunt</p>

Parameter	Description
	<p>Group ID 56:</p> <p>INVITE sip:123456@192.168.1.2;dtg=56;user=phone SIP/2.0</p> <p>Note: If the Hunt Group is not found based on the 'dtg' parameter, the 'Inbound IP Routing Table' is used instead for routing the call to the appropriate Hunt Group.</p>
<p>Web/EMS: Enable GRUU [EnableGRUU]</p>	<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 REGISTER request containing a Supported header field with the value "gruu". The UA includes a "+sip.instance" Contact header parameter of each contact for which the GRUU is desired. This Contact parameter contains a globally unique ID that identifies the UA instance. The global unique ID is created from one of the following: <ul style="list-style-type: none"> ✓ If the REGISTER is per the device's client (endpoint), it is the MAC address concatenated with the phone number of the client. ✓ If the REGISTER is per device, it is the MAC address only. ✓ When using TP, "User Info" can be used for registering per endpoint. Thus, each endpoint can get a unique id – its phone number. The globally unique ID in TP is the MAC address concatenated with the phone number of the endpoint. <p>If the remote server doesn't support GRUU, it ignores the parameters of the GRUU. Otherwise, if the remote side also supports GRUU, the REGISTER responses contain the "gruu" parameter in each Contact header. 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:

Parameter	Description
	INVITE request, its 2xx response, SUBSCRIBE request, its 2xx response, NOTIFY request, REFER request and its 2xx response.
EMS: Is CISCO Sce Mode [IsCiscoSCEMode]	<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 fmtp attribute in the SDP to 'no'. This logic is used if the parameter EnableSilenceCompression is set to 2 (enable without adaptation). In this case, Silence Suppression is used on the channel but not declared in the SDP.</p> <p>Note: The IsCiscoSCEMode parameter is applicable only when the selected coder is G.729.</p>
Web: User-Agent Information EMS: User Agent Display Info [UserAgentDisplayInfo]	<p>Defines the string that is used in the SIP User-Agent and Server response headers. When configured, the string '<UserAgentDisplayInfo value>/software version' is used, for example:</p> <pre>User-Agent: myproduct/v.6.00.010.006</pre> <p>If not configured, the default string, '<AudioCodes product-name>/software version' is used, for example:</p> <pre>User-Agent: Audiocodes-Sip-Gateway-Mediant 800 MSBG/v.6.00.010.006</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>
Web/EMS: SDP Session Owner [SIPSDPSessionOwner]	<p>Determines the value of the Owner line ('o' field) in outgoing SDP messages.</p> <p>The valid range is a string of up to 39 characters. The default value is 'AudiocodesGW'.</p> <p>For example:</p> <pre>o=AudiocodesGW 1145023829 1145023705 IN IP4 10.33.4.126</pre>
[EnableSDPVersionNegotiation]	<p>This feature enables the flexibility of ignoring a new SDP re-offer (from the media negotiation perspective) in certain scenarios (such as session expires). According to RFC 3264, once an SDP session is established, a new SDP offer is considered a new offer only when the SDP origin value is incremented. In scenarios such as session expires, SDP negotiation is irrelevant and thus, the origin field is not changed.</p> <p>Even though some SIP devices don't follow this behavior and don't increment the origin value even in scenarios where they want to re-negotiate, the device can assume that the remote party operates according to RFC 3264, and in cases where the origin field is not incremented, the device does not re-negotiate SDP capabilities.</p> <ul style="list-style-type: none"> [0] Disable = 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]	<p>Defines the value of the Subject header in outgoing INVITE messages. If not specified, the Subject header isn't included (default).</p> <p>The maximum length is up to 50 characters.</p>

Parameter	Description
Web: Multiple Packetization Time Format EMS: Multi Ptime Format [MultiPtimeFormat]	<p>Determines whether the 'mptime' attribute is included in the outgoing SDP.</p> <ul style="list-style-type: none"> [0] None = Disabled (default) [1] PacketCable = includes the 'mptime' attribute in the outgoing SDP - PacketCable-defined format <p>The 'mptime' attribute enables the device to define a separate Packetization period for each negotiated coder in the SDP. The 'mptime' attribute is only included if this parameter is enabled, even if the remote side includes it in the SDP offer. Upon receipt, each coder receives its 'ptime' value in the following precedence: from 'mptime' attribute, from 'ptime' attribute, and then from default value.</p>
EMS: Enable P Time [EnablePtime]	<p>Determines whether the 'ptime' attribute is included in the SDP.</p> <ul style="list-style-type: none"> [0] = Remove the 'ptime' attribute from SDP. [1] = Include the 'ptime' attribute in SDP (default).
Web/EMS: 3xx Behavior [3xxBehavior]	<p>Determines the device's behavior regarding call identifiers when a 3xx response is received for an outgoing INVITE request. The device can either use the same call identifiers (Call-ID, Branch, To, and From tags) or change them in the new initiated INVITE.</p> <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]	<p>Enables the inclusion of the P-Charging-Vector header to all outgoing INVITE messages.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable
Web/EMS: Retry-After Time [RetryAfterTime]	<p>Determines the time (in seconds) used in the Retry-After header when a 503 (Service Unavailable) response is generated by the device. The time range is 0 to 3,600. The default value is 0.</p>
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.</p> <p>The Retry-After header is used with the 503 (Service Unavailable) response to indicate how long the service is expected to be unavailable to the requesting SIP client. The device maintains a list of available proxies, by using the Keep-Alive mechanism. The device checks the availability of proxies by sending SIP OPTIONS every keep-alive timeout to all proxies.</p> <p>If the device receives a SIP 503 response to an INVITE, it also marks that the proxy is out of service for the defined "Retry-After" period.</p>

Parameter	Description
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 the SIP header used for the source number in incoming INVITE messages.</p> <ul style="list-style-type: none"> ▪ " = (empty string) Use the device's internal logic for header preference (default). The logic for filling the calling party parameters is as follows: the SIP header is selected first from which the calling party parameters are obtained: first priority is P-Asserted-Identity, second is Remote-Party-ID, and third is the From header. Once a URL is selected, all the calling party parameters are set from this header. If P-Asserted-Identity is selected, the Privacy header is checked and if the Privacy is set to 'id', the calling number is assumed restricted. ▪ 'FROM' = Use the source number received in the From header.
[SelectSourceHeaderForCalledNumber]	<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 to-tag than the previous 18x response. Those responses usually are generated by Proxy/Application servers that perform call forking, sending the device's originating INVITE to several destinations, using the same CallID.</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>

Parameter	Description
Web: Forking Timeout [ForkingTimeout]	<p>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/EMS: Enable Reason Header [EnableReasonHeader]	<p>Enables or disables the usage of the SIP Reason header.</p> <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default)
Web/EMS: Gateway Name [SIPGatewayName]	<p>Assigns a name to the device (e.g., 'device123.com'). Ensure that the name you choose is the one with which the Proxy is configured to identify the device.</p> <p>Note: If specified, the device name is used as the host part of the SIP URI in the From header. If not specified, the device's IP address is used instead (default).</p>
[ZeroSDPHandling]	<p>Determines the device's response to an incoming SDP that includes an IP address of 0.0.0.0 in the SDP's Connection Information field (i.e., "c=IN IP4 0.0.0.0").</p> <ul style="list-style-type: none"> ▪ [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]	<p>Determines whether the device sends the initial INVITE message with or without an SDP. Sending the first INVITE without SDP is typically done by clients for obtaining the far-end's full list of capabilities before sending their own offer. (An alternative method for obtaining the list of supported capabilities is by using SIP OPTIONS, which is not supported by every SIP agent.)</p> <ul style="list-style-type: none"> ▪ [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]	<p>Determines whether the device sets the Contact header of outgoing INVITE requests to 'anonymous' for restricted calls.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
[AnonymousMode]	<p>Determines whether the device's IP address is used as the URI host part instead of "anonymous.invalid" in the INVITE's From header for Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [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>

Parameter	Description
	<ul style="list-style-type: none"> [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 1, the device replaces the "anonymous.invalid" with its IP address.</p>
EMS: P Asserted User Name [PAssertedUserName]	<p>Defines a 'representative number' (up to 50 characters) that is used as the user part of the Request-URI in the P-Asserted-Identity header of an outgoing INVITE (for Tel-to-IP calls). The default value is null.</p>
EMS: Use URL In Refer To Header [UseAORInReferToHeader]	<p>Defines the source for the SIP URI set in the Refer-To header of outgoing REFER messages.</p> <ul style="list-style-type: none"> [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]	<p>Enables or disables the usage of the User Information, which is loaded to the device in the User Information auxiliary file. (For a description on User Information, see "Loading Auxiliary Files" on page 337.)</p> <ul style="list-style-type: none"> [0] Disable (default). [1] Enable
[HandleReasonHeader]	<p>Determines whether the device uses the value of the incoming SIP Reason header for Release Reason mapping.</p> <ul style="list-style-type: none"> [0] Disregard Reason header in incoming SIP messages. [1] Use the Reason header value for Release Reason mapping (default).
[EnableSilenceSuppInSDP]	<p>Determines the device's behavior upon receipt of SIP Re-INVITE messages that include the SDP's 'silencesupp:off' attribute.</p> <ul style="list-style-type: none"> [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]	<p>Enables or disables the usage of the 'rport' parameter in the Via header.</p> <ul style="list-style-type: none"> [0] = Enabled. [1] = Disabled (default). <p>The device adds an 'rport' parameter to the Via header of each outgoing SIP message. The first Proxy that receives this message sets the 'rport' value of the response to the actual port from where the request was received. This method is used, for example, to enable the device to identify its port mapping outside a NAT.</p> <p>If the Via header doesn't include the 'rport' parameter, the destination port of the response is obtained from the host part of the Via header.</p>

Parameter	Description
	<p>If the Via header includes the 'rport' parameter without a port value, the destination port of the response is the source port of the incoming request.</p> <p>If the Via header includes 'rport' with a port value (e.g., rport=1001), the destination port of the response is the port indicated in the 'rport' parameter.</p>
Web: Enable X-Channel Header EMS: X Channel Header [XChannelHeader]	<p>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.</p> <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, and the device's IP address. For example, 'x-channel: DS/DS1-5/8;IP=192.168.13.1', where: <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
Web/EMS: Progress Indicator to IP [ProgressIndicator2IP]	<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>

Parameter	Description
[EnableRekeyAfter181]	<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>
[NumberOfActiveDialogs]	<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 520. The default value is 520.</p>
[TransparentCoderOnDataCall]	<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).</p> <p>The initiated INVITE includes the following SDP attribute:</p> <pre>a=rtpmap:97 CLEARMODE/8000</pre> <p>The default payload type is set according to the CodersGroup parameter. If the Transparent coder is not defined, the default value is set to 56. The payload type is negotiated with the remote side, i.e., the selected payload type is according to the remote side selection. The receiving device must include the 'Transparent' coder in its coder list.</p>
Web: Enable RFC 4117 Transcoding [EnableRFC4117Transcoding]	<p>Enables transcoding of calls according to RFC 4117.</p> <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 a detailed description of this transcoding feature, see Transcoding using Third-Party Call Control on page 608.
Web/EMS: Default Release Cause [DefaultReleaseCause]	<p>Defines the default Release Cause (sent to IP) for IP-to-Tel calls when the device initiates a call release and an explicit matching cause for this release is not found. The default release cause is NO_ROUTE_TO_DESTINATION (3). Other common values include NO_CIRCUIT_AVAILABLE (34), DESTINATION_OUT_OF_ORDER (27), etc.</p> <p>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 an explanation on mapping PSTN release causes to SIP responses, see Mapping PSTN Release Cause to SIP Response on page 478. ▪ 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 162.

Parameter	Description
	<ul style="list-style-type: none"> For a list of SIP responses-Q.931 release cause mapping, see "Release Reason Mapping" on page 638.
[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 included 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. When disabled, the device sends additional 18x responses as a result of receiving an Alerting message whether or not a 18x response was already sent.</p>
Web: Enable Microsoft Extension [EnableMicrosofExt]	<p>Modifies the called number for numbers received with Microsoft's proprietary "ext=xxx" parameter in the SIP INVITE URI user part. Microsoft Office Communications Server sometimes uses this proprietary parameter to indicate the extension number of the called party.</p> <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 (see "Number Manipulation and Routing Parameters" on page 836) 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 before this timer expires, the call is disconnected. The valid range is 0 to 32,000. The default value is 0 (i.e., no timeout).</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

Parameter	Description
[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 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 [FirstCallRBTId]	<p>Determines the index of the first Ringback Tone in the CPT file. This option enables an Application server to request the device to play a distinctive Ringback tone to the calling party according to the destination of the call. The tone is played according to the Alert-Info header received in the 180 Ringing SIP response (the value of the Alert-Info header is added to the value of this parameter). The valid range is -1 to 1,000. The default value is -1 (i.e., play standard Ringback tone).</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).

Parameter	Description
Web: Reanswer Time EMS: Regret Time [RegretTime]	<p>For Analog interfaces: 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: Determines 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. 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. 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.
Web: RTP Only Mode [RTPOnlyMode]	<p>Enables the device to start sending and/or receiving RTP packets to and from remote endpoints without the need to establish a SIP session. The remote IP address is determined according to the Outbound IP Routing table (Prefix parameter). The port is the same port as the local RTP port (configured by the BaseUDPPort parameter and the channel on which the call is received).</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Transmit & Receive = Send and receive RTP

Parameter	Description
	<ul style="list-style-type: none"> ▪ [2] Transmit Only= Send RTP only ▪ [3] Receive Only= Receive RTP only <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Enables the device to start sending and/or receiving RTP packets to and from remote endpoints without the need to establish a SIP session. This is configured per trunk - the ID in the parameter name depicts the trunk number (where 0 is the first trunk).</p> <p>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"> ▪ [-1] Not Configured = use the global parameter (RTPOnlyMode) value for all channels (default) ▪ [0] Disable ▪ [1] Transmit & Receive = send and receive RTP packets ▪ [2] Transmit Only = send RTP packets only ▪ [3] Receive Only = receive RTP packets only <p>Note: The ID in the ini file parameter depicts the trunk number, where 0 is the first trunk.</p>
Web/EMS: Media IP Version Preference [MediaIPVersionPreference]	<p>Determines the preferred RTP media IP addressing version for outgoing SIP calls. This is indicated in the "c=" field (Connection Information) of the SDP.</p> <ul style="list-style-type: none"> ▪ [0] Only IPv4 = offer includes only IPv4 media IP addresses (default). ▪ [1] Only IPv6 = offer includes only IPv6 media IPs addresses. ▪ [2] Prefer IPv4 = offer includes both IPv4 and IPv6 media IP addresses, but the first media is IPv4. ▪ [3] Prefer IPv6 = offer includes both IPv4 and IPv6 media IP addresses, but the first media is IPv6. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only when the device offers an SDP. ▪ The IP addressing version is determined according to the first SDP "m=" field. ▪ This parameter can be configured per IP Profile, using the parameter IPProfile (see Configuring IP Profiles on page 143).
Web/EMS: SIT Q850 Cause [SITQ850Cause]	<p>Determines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when a Special Information Tone (SIT) is detected on an IP-to-Tel call. The valid range is 0 to 127. The default value is 34.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For mapping specific SIT tones, you can use the SITQ850CauseForNC, SITQ850CauseForIC, SITQ850CauseForVC,

Parameter	Description
	and SITQ850CauseForRO parameters.
Web/EMS: SIT Q850 Cause For NC [SITQ850CauseForNC]	<p>Determines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-NC (No Circuit Found Special Information Tone) is detected from the PSTN for IP-to-Tel calls. The valid range is 0 to 127. The default value is 34.</p> <p>Note: When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
Web/EMS: SIT Q850 Cause For IC [SITQ850CauseForIC]	<p>Determines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-IC (Operator Intercept Special Information Tone) is detected from the PSTN for IP-to-Tel calls. The valid range is 0 to 127. The default value is -1 (not configured).</p> <p>Note: When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
Web/EMS: SIT Q850 Cause For VC [SITQ850CauseForVC]	<p>Determines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-VC (Vacant Circuit - non-registered number Special Information Tone) is detected from the PSTN for IP-to-Tel calls. The valid range is 0 to 127. The default value is -1 (not configured).</p> <p>Note: When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
Web/EMS: SIT Q850 Cause For RO [SITQ850CauseForRO]	<p>Determines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-RO (Reorder - System Busy Special Information Tone) is detected from the PSTN for IP-to-Tel calls. The valid range is 0 to 127. The default value is -1 (not configured).</p> <p>Note: When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
Out-of-Service (Busy Out) Parameters	
Web/EMS: Enable Busy Out [EnableBusyOut]	<p>Determines whether the Busy Out feature is enabled.</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:</p> <p>For analog interfaces: A reorder tone (configured by the parameter FXSOOSBehavior) is played when the phone is off-hooked.</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.

Parameter	Description
	<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 Hunt Group. If there is no connectivity to the Serving IP Group of a specific Hunt Group (defined in the 'Hunt Group Settings' table), all the physical trunks pertaining to that Hunt Group are set to the Busy-Out condition. Each trunk uses the proper Out-Of-Service method according to the selected ISDN/CAS variant. 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>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 and is multiplied by two until SipT2Rtx. For example (assuming that 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.

Parameter	Description
Web: SIP T2 Retransmission Timer [msec] EMS: T2 RTX [SipT2Rtx]	The maximum interval (in msec) between retransmissions of SIP messages. The default is 4000. Note: The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.
Web: SIP Maximum RTX EMS: Max RTX [SIPMaxRtx]	Maximum number of UDP transmissions (first transmission plus retransmissions) of SIP messages. The range is 1 to 30. The default value is 7.
Web: Number of RTX Before Hot-Swap EMS: Proxy Hot Swap Rtx [HotSwapRtx]	Number of retransmitted INVITE/REGISTER messages before the call is routed (hot swap) to another Proxy/Registrar. The valid range is 1 to 30. The default value is 3. Note: This parameter is also used for alternative routing using the '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.

12.10 Coders and Profile Parameters

The profile parameters are described in the table below.

Table 12-28: Profile Parameters

Parameter	Description
Web: Coders Table/Coder Group Settings EMS: Coders Group	
[CodersGroup0] [CodersGroup1] [CodersGroup2] [CodersGroup3] [CodersGroup4]	<p>This <i>ini</i> file table parameter defines the device's coders. Up to five groups of coders can be defined, where each group can consist of up to 10 coders. The first Coder Group is the default coder list and the default Coder Group. These Coder Groups can later be assigned to IP or Tel Profiles.</p> <p>The format of this parameter is as follows:</p> <pre>[CodersGroup0] FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime, CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce; [\CodersGroup0]</pre> <p>Where,</p> <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:

Parameter	Description																																																		
	<div>✓ [0] Disabled (default)</div> <div>✓ [1] Enabled</div> <div>For example, below are defined two Coder Groups (0 and 1):</div> <div><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></div> <div>The table below lists the supported coders:</div> <table><tr><th>Coder Name</th><th>Packetization Time (msec)</th><th>Rate (kbps)</th><th>Payload Type</th><th>Silence Suppression</th></tr><tr><td>G.711 A-law [g711Alaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 8</td><td>Disable [0] Enable [1]</td></tr><tr><td>G.711 U-law [g711Ulaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 0</td><td>Disable [0] Enable [1]</td></tr><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)</td><td>16 [0] (default), 24 [1], 40 [3]</td><td>Dynamic (0-127) Default is 23</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>AMR-WB [Amr-WB]</td><td>20 (default)</td><td>6.6 [0], 8.85 [1], 12.65 [2], 14.25 [3], 15.85 [4], 18.25 [5], 19.85 [6], 23.05 [7], 23.85 [8] (default)</td><td>Dynamic (0-127)</td><td>Disable [0] Enable [1]</td></tr><tr><td>T.38 [t38fax]</td><td>N/A</td><td>N/A</td><td>N/A</td><td>N/A</td></tr><tr><td>T.38 Version 3 [t38fax]</td><td>-</td><td>-</td><td>-</td><td>-</td></tr></table> <div>Notes:</div> <div>▪ The coder name is case-sensitive.</div>	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.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)	16 [0] (default), 24 [1] , 40 [3]	Dynamic (0-127) Default is 23	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]	AMR-WB [Amr-WB]	20 (default)	6.6 [0] , 8.85 [1] , 12.65 [2] , 14.25 [3] , 15.85 [4] , 18.25 [5] , 19.85 [6] , 23.05 [7] , 23.85 [8] (default)	Dynamic (0-127)	Disable [0] Enable [1]	T.38 [t38fax]	N/A	N/A	N/A	N/A	T.38 Version 3 [t38fax]	-	-	-	-
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.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)	16 [0] (default), 24 [1] , 40 [3]	Dynamic (0-127) Default is 23	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]																																															
AMR-WB [Amr-WB]	20 (default)	6.6 [0] , 8.85 [1] , 12.65 [2] , 14.25 [3] , 15.85 [4] , 18.25 [5] , 19.85 [6] , 23.05 [7] , 23.85 [8] (default)	Dynamic (0-127)	Disable [0] Enable [1]																																															
T.38 [t38fax]	N/A	N/A	N/A	N/A																																															
T.38 Version 3 [t38fax]	-	-	-	-																																															

Parameter	Description
	<ul style="list-style-type: none"> Each coder type can appear only once per Coder Group. Only the packetization time of the first coder in the defined coder list is declared in INVITE/200 OK SDP, even if multiple coders are defined. The device always uses the packetization time requested by the remote side for sending RTP packets. If not specified, the packetization time is assigned the default value. The value of several fields is hard-coded according to common standards (e.g., payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored. If silence suppression is not defined for a specific coder, the value defined by the parameter EnableSilenceCompression is used. If G.729 is selected and silence suppression is enabled (for this coder), the device includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception is when the remote device is a Cisco gateway (IsCiscoSCEMode). The coder G.722 provides Packet Loss Concealment (PLC) capabilities, ensuring higher voice quality. A Coder Group can be assigned to an IP Profile (using the IPProfile parameter) and/or to a Tel Profile (using the TelProfile parameter). For an explanation on V.152 support (and implementation of T.38 and VBD coders), see "V.152 Support" on page 452. For a description of using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: IP Profile Settings Table EMS: Protocol Definition > IP Profile	
[IPProfile]	<p>This <i>ini</i> file table parameter configures the IP Profile table. Each IP Profile ID includes a set of parameters (which are typically configured separately using their individual "global" parameters). You can later assign these IP Profiles to 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:</p> <pre>[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,</pre>

Parameter	Description																																	
	<p>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_SBCDiversioMode, IpProfile_SBCHistoryInfoMode; [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><tr><th>IPProfile Field</th><th>Web Name</th><th>Global Parameter</th></tr><tr><td>IpProfile_Index</td><td>Profile ID</td><td>-</td></tr><tr><td>IpProfile_ProfileName</td><td>Profile Name</td><td>-</td></tr><tr><td>IpProfile_IpPreference</td><td>Profile Preference</td><td>-</td></tr><tr><td>IpProfile_CodersGroupID</td><td>Coder Group</td><td>CodersGroup</td></tr><tr><td>IpProfile_IsFaxUsed</td><td>Fax Signaling Method</td><td>IsFaxUsed</td></tr><tr><td>IpProfile_JitterBufMinDelay</td><td>Dynamic Jitter Buffer Minimum Delay</td><td>DJBufMinDelay</td></tr><tr><td>IpProfile_JitterBufOptFactor</td><td>Dynamic Jitter Buffer Optimization Factor</td><td>DJBufOptFactor</td></tr><tr><td>IpProfile_IPDiffServ</td><td>RTP IP DiffServ</td><td>PremiumServiceClassMediaDiffServ</td></tr><tr><td>IpProfile_SigIPDiffServ</td><td>Signaling DiffServ</td><td>PremiumServiceClassControlDiffServ</td></tr><tr><td>IpProfile_SCE</td><td>-</td><td>EnableSilenceCom</td></tr></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_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	-	EnableSilenceCom
IPProfile Field	Web Name	Global Parameter																																
IpProfile_Index	Profile ID	-																																
IpProfile_ProfileName	Profile Name	-																																
IpProfile_IpPreference	Profile Preference	-																																
IpProfile_CodersGroupID	Coder Group	CodersGroup																																
IpProfile_IsFaxUsed	Fax Signaling Method	IsFaxUsed																																
IpProfile_JitterBufMinDelay	Dynamic Jitter Buffer Minimum Delay	DJBufMinDelay																																
IpProfile_JitterBufOptFactor	Dynamic Jitter Buffer Optimization Factor	DJBufOptFactor																																
IpProfile_IPDiffServ	RTP IP DiffServ	PremiumServiceClassMediaDiffServ																																
IpProfile_SigIPDiffServ	Signaling DiffServ	PremiumServiceClassControlDiffServ																																
IpProfile_SCE	-	EnableSilenceCom																																

Parameter	Description		
			pression
	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
	IpProfile_RxDTMFOption	Declare RFC 2833 in SDP	RxDTMFOption
	IpProfile_EnableHold	Enable Hold	EnableHold

Parameter	Description		
	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 Mode	-
	IpProfile_SBCAllowedCodersMode	Allowed Coders Group ID	AllowedCodersGroupID
	IpProfile_SBCMediaSecurityBehaviour	-	SBCMediaSecurityBehaviour
	IpProfile_SBCRFC2833Behavior	-	-
	IpProfile_SBCAlternativeDTMFMethod	-	-
	IpProfile_SBCAssertIdentity	-	SBCAssertIdentity
	IpProfile_AMDSensitivityParameterSuit	AMD Sensitivity Level	AMDSensitivityLevel
	IpProfile_AMDSensitivityLevel	AMD Sensitivity Level	AMDSensitivityLevel
	IpProfile_AMDMaxGreetingTime	AMD Max Greeting Time	AMDMaxGreetingTime
	IpProfile_AMDMaxPostSilenceGreetingTime	AMD Max Post Silence Greeting Time	AMDMaxPostGreetingSilenceTime
	IpProfile_SBCDiversionMode	Diversion Mode	-
	IpProfile_SBCHistoryInfoMode	History Info Mode	-
<ul style="list-style-type: none"> The parameter IpPreference determines the priority of the IP Profile (1 to 20, where 20 is the highest preference). If both IP and Tel Profiles apply to the same call, the coders and common 			

Parameter	Description
	<p>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.</p> <ul style="list-style-type: none"> ▪ The parameter CallLimit defines the maximum number of concurrent calls allowed for that Profile. If the Profile is set to some limit, the device maintains the number of concurrent calls (incoming and outgoing) pertaining to the specific Profile. A limit value of [-1] indicates that there is no limitation on calls (default). A limit value of [0] indicates that all calls are rejected. When the number of concurrent calls is equal to the limit, the device rejects any new incoming and outgoing calls pertaining to that profile. ▪ RxDTMFOption configures the received DTMF negotiation method: [-1] not configured, use the global parameter; [0] don't declare RFC 2833; [1] declare RFC 2833 payload type is SDP. ▪ FirstTxDtmfOption and SecondTxDtmfOption configures the transmit DTMF negotiation method: [-1] not configured, use the global parameter; for the remaining options, see the global parameter. ▪ The VxxTransportType parameter configures the modem transport type per IP Profile for the following parameters: V21ModemTransportType, V22ModemTransportType, V23ModemTransportType, V32ModemTransportType, and V34ModemTransportType. ▪ IP Profiles can also be used when operating with a Proxy server (set the parameter AlwaysUseRouteTable to 1). ▪ The following parameters are not applicable: IsDTMFUsed (deprecated), ▪ For a description of using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Tel Profile Settings Table EMS: Protocol Definition > Telephony Profile	
[TelProfile]	<p>This <i>ini</i> file table parameter configures the Tel Profile table. Each Tel Profile ID includes a set of parameters (which are typically configured separately using their individual, "global" parameters). You can later assign these Tel Profile IDs to other elements such as in the Hunt Group Table (TrunkGroup parameter). Therefore, Tel Profiles allow you to apply the same settings of a group of parameters to multiple channels, or apply specific settings to different channels.</p> <p>The format of this parameter is as follows:</p> <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,</pre>

Parameter	Description																																							
	<div>TelProfile_EnableEarlyMedia, TelProfile_ProgressIndicator2IP, TelProfile_TimeForReorderTone, TelProfile_EnableDIDWink, TelProfile_IsTwoStageDial, TelProfile_DisconnectOnBusyTone, TelProfile_EnableVoiceMailDelay, TelProfile_DialPlanIndex, TelProfile_Enable911PSAP, TelProfile_SwapTelToIpPhoneNumbers, TelProfile_EnableAGC, TelProfile_ECNIpMode; TelProfile_DigitalCutThrough; [TelProfile]</div> <div>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;</div> <div>Notes:</div> <div><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:</div> <div><table><tr><th>TelProfile Field</th><th>Web Name</th><th>Global Parameter</th></tr><tr><td>TelProfile_ProfileName</td><td>Profile Name</td><td>-</td></tr><tr><td>TelProfile_TelPreference</td><td>Profile Preference</td><td>-</td></tr><tr><td>TelProfile_CodersGroupID</td><td>Coder Group</td><td>CodersGroup0</td></tr><tr><td>TelProfile_IsFaxUsed</td><td>Fax Signaling Method</td><td>IsFaxUsed</td></tr><tr><td>TelProfile_JitterBufMinDelay</td><td>Dynamic Jitter Buffer Minimum Delay</td><td>DJBufMinDelay</td></tr><tr><td>TelProfile_JitterBufOptFactor</td><td>Dynamic Jitter Buffer Optimization Factor</td><td>DJBufOptFactor</td></tr><tr><td>TelProfile_IPDiffServ</td><td>RTP IP DiffServ</td><td>PremiumServiceClassMediaDiffServ</td></tr><tr><td>TelProfile_SigIPDiffServ</td><td>Signaling DiffServ</td><td>PremiumServiceClassControlDiffServ</td></tr><tr><td>TelProfile_DtmfVolume</td><td>DTMF Volume</td><td>DTMFVolume</td></tr><tr><td>TelProfile_InputGain</td><td>Input Gain</td><td>InputGain</td></tr><tr><td>TelProfile_VoiceVolume</td><td>Voice Volume</td><td>VoiceVolume</td></tr><tr><td>TelProfile_EnableReversePolarity</td><td>Enable Polarity Reversal</td><td>EnableReversalPolarity</td></tr></table></div>	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 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																																						

Parameter	Description		
	TelProfile_EnableCurrentDisconnect	Enable Current Disconnect	EnableCurrentDisconnect
	TelProfile_EnableDigitDelivery	Enable Digit Delivery	EnableDigitDelivery
	TelProfile_EnableEC	Echo Canceler	EnableEchoCanceler
	TelProfile_MWIAAnalog	MWI Analog Lamp	MWIAAnalogLamp
	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, MWIAAnalog, MWIDisplay, EnableDIDWink, IsTwoStageDial, 			

Parameter	Description
	<p>DisconnectOnBusyTone, and Enable911PSAP.</p> <ul style="list-style-type: none">▪ 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 368.

12.11 Channel Parameters

This subsection describes the device's channel parameters.

12.11.1 Voice Parameters

The voice parameters are described in the table below.

Table 12-29: Voice Parameters

Parameter	Description
Web/EMS: Input Gain [InputGain]	<p>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 143) and per Tel Profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 141).</p>
Web: Voice Volume EMS: Volume (dB) [VoiceVolume]	<p>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 143) and per Tel Profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 141).</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>Determines (in 100-msec resolution) the time 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.

Parameter	Description
Web: Answer Detector Redirection [AnswerDetectorRedirection]	Currently, not supported.
Web: Answer Detector Sensitivity EMS: Sensitivity [AnswerDetectorSensitivity]	Determines the Answer Detector sensitivity. The range is 0 (most sensitive) to 2 (least sensitive). The default is 0.
Web: Silence Suppression EMS: Silence Compression Mode [EnableSilenceCompression]	<p>Silence Suppression is a method for conserving bandwidth on VoIP calls by not sending packets when silence is detected.</p> <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 fmp 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 143).</p>
Web: Echo Canceler EMS: Echo Canceller Enable [EnableEchoCanceller]	<p>Enables or disables echo cancellation (i.e., echo from voice calls is removed).</p> <ul style="list-style-type: none"> [0] Off = Echo Canceler is disabled. [1] On = Echo Canceler is enabled (default). <p>Notes:</p> <ul style="list-style-type: none"> This parameter is used to maintain backward compatibility. This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143) and per Tel Profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 141).
EMS: Echo Canceller Hybrid Loss [ECHybridLoss]	<p>Sets the four wire to two wire worst-case Hybrid loss, the ratio between the signal level sent to the hybrid and the echo level returning from the hybrid.</p> <ul style="list-style-type: none"> [0] = 6 dB (default) [1] = N/A [2] = 0 dB [3] = 3 dB
[ECNLPMODE]	<p>Defines the echo cancellation Non-Linear Processing (NLP) mode.</p> <ul style="list-style-type: none"> [0] = NLP adapts according to echo changes (default). [1] = Disables NLP. [2] = Silence output NLP.

Parameter	Description
	Note: This parameter can also be configured per Tel Profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 141).
[EchoCancellerAggressiveNLP]	Enables or disables the Aggressive NLP at the first 0.5 second of the call. When enabled, the echo is removed only in the first half of a second of the incoming IP signal. <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = Enable (default) Note: For this parameter to take effect, a device reset is required.
[RTPSIDCoeffNum]	Determines the number of spectral coefficients added to an SID packet being sent according to RFC 3389. The valid values are [0] (default), [4] , [6] , [8] and [10] .

12.11.2 Coder Parameters

The coder parameters are described in the table below.

Table 12-30: Coder Parameters

Parameter	Description
[EnableEVRCVAD]	Enables or disables 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 [VBRCoderHeaderFormat]	Defines 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 3558 Header Free format (default). ▪ [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]	Determines 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.

12.11.3 Fax and Modem Parameters

The fax and modem parameters are described in the table below.

Table 12-31: Fax and Modem Parameters

Parameter	Description
Web: Fax Transport Mode EMS: Transport Mode [FaxTransportMode]	<p>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 <code>IsFaxUsed</code>. If the parameter <code>IsFaxUsed</code> is set to 1 (T.38 Relay) or 3 (Fax Fallback), then <code>FaxTransportMode</code> is always set to 1 (T.38 relay).</p>
EMS: V34 Transport Method [V34FaxTransportType]	<p>Determines the V.34 fax transport method (whether V34 fax falls back to T.30 or pass over Bypass).</p> <ul style="list-style-type: none"> ▪ [0] = Transparent ▪ [1] = Relay (default) ▪ [2] = Bypass ▪ [3] = Transparent with Events <p>Note: To configure <code>V34FaxTransportType</code> to 1 (i.e., fax relay), you also need to configure <code>FaxTransportMode</code> to 1 (fax relay).</p>
Web: Fax Relay Enhanced Redundancy Depth EMS: Enhanced Relay Redundancy Depth [FaxRelayEnhancedRedundancyDepth]	<p>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.</p>
Web: Fax Relay Redundancy Depth EMS: Relay Redundancy Depth [FaxRelayRedundancyDepth]	<p>Number of times that each fax relay payload is retransmitted to the network.</p> <ul style="list-style-type: none"> ▪ [0] = No redundancy (default). ▪ [1] = One packet redundancy. ▪ [2] = Two packet redundancy. <p>Note: This parameter is applicable only to non-V.21 packets.</p>
Web: Fax Relay Max Rate (bps) EMS: Relay Max Rate [FaxRelayMaxRate]	<p>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) ▪ [6] 16800bps = 16.8 kbps ▪ [7] 19200bps = 19.2 kbps ▪ [8] 21600bps = 21.6 kbps ▪ [9] 24000bps = 24 kbps

Parameter	Description
	<ul style="list-style-type: none"> ▪ [10] 26400bps = 26.4 kbps ▪ [11] 28800bps = 28.8 kbps ▪ [12] 31200bps = 31.2 kbps ▪ [13] 33600bps = 33.6 kbps <p>Notes:</p> <ul style="list-style-type: none"> ▪ The rate is negotiated between both sides (i.e., the device adapts to the capabilities of the remote side). Negotiation of the T.38 maximum supported fax data rate is provided in SIP's SDP T38MaxBitRate parameter. The negotiated T38MaxBitRate is the minimum rate supported between the local and remote endpoints. ▪ Configuration above 14.4 kbps is truncated to 14.4 kbps for non-T.38 V.34 supporting devices.
Web: Fax Relay ECM Enable EMS: Relay ECM Enable [FaxRelayECMEnable]	<p>Determines whether the Error Correction Mode (ECM) mode is used during fax relay.</p> <ul style="list-style-type: none"> ▪ [0] Disable = ECM mode is not used during fax relay. ▪ [1] Enable = ECM mode is used during fax relay (default).
Web: Fax/Modem Bypass Coder Type EMS: Coder Type [FaxModemBypassCoderType]	<p>Coder used by the device when performing fax/modem bypass. Usually, 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/EMS: CNG Detector Mode [CNGDetectorMode]	<p>Determines whether the device detects the fax Calling tone (CNG).</p> <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. <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).</p>

Parameter	Description
Web: Fax/Modem Bypass Packing Factor EMS: Packetization Period [FaxModemBypassM]	Number of (20 msec) coder payloads that are used to generate a fax/modem bypass packet. The valid range is 1, 2, or 3 coder payloads. The default value is 1 coder payload.
[FaxModemNTEMode]	Determines whether the device sends RFC 2833 ANS/ANSam events upon detection of fax and/or modem Answer tones (i.e., CED tone). <ul style="list-style-type: none"> [0] = Disabled (default). [1] = Enabled. Note: This parameter is applicable only when the fax or modem transport type is set to bypass or Transparent-with-Events.
Web/EMS: Fax Bypass Payload Type [FaxBypassPayloadType]	Determines the fax bypass RTP dynamic payload type. The valid range is 96 to 120. The default value is 102.
EMS: Modem Bypass Payload Type [ModemBypassPayloadType]	Modem Bypass dynamic payload type. The range is 0-127. The default value is 103.
EMS: Relay Volume (dBm) [FaxModemRelayVolume]	Determines the fax gain control. The range is -18 to -3, corresponding to -18 dBm to -3 dBm in 1-dB steps. The default is -6 dBm fax gain control.
Web/EMS: Fax Bypass Output Gain [FaxBypassOutputGain]	Defines the fax bypass output gain control. The range is -31 to +31 dB, in 1-dB steps. The default is 0 (i.e., no gain).
Web/EMS: Modem Bypass Output Gain [ModemBypassOutputGain]	Defines the modem bypass output gain control. The range is -31 dB to +31 dB, in 1-dB steps. The default is 0 (i.e., no gain).
EMS: NTE Max Duration [NTEMaxDuration]	Maximum time for sending Named Telephony Events (NTEs) to the IP side regardless of the time range when the TDM signal is detected. The range is -1 to 200,000,000 msec (i.e., 55 hours). The default is -1 (i.e., NTE stops only upon detection of an End event).
EMS: Basic Packet Interval [FaxModemBypassBasicRTPPacketInterval]	Determines the basic frame size that is used during fax/modem bypass sessions. <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) [FaxModemBypassDJBufMinDelay]	Determines the Jitter Buffer delay (in milliseconds) during fax and modem bypass session. The range is 0 to 150 msec. The default is 40.

Parameter	Description
EMS: Enable Inband Network Detection [EnableFaxModemInbandNetworkDetection]	<p>Enables or disables in-band network detection related to fax/modem.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable <p>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.</p>
EMS: NSE Mode [NSEMode]	<p>Cisco compatible fax and modem bypass mode.</p> <ul style="list-style-type: none"> [0] = NSE disabled (default) [1] = NSE enabled <p>In NSE bypass mode, the device starts using G.711 A-Law (default) or G.711μ-Law according to the FaxModemBypassCoderType parameter. The payload type used with these G.711 coders is a standard one (8 for G.711 A-Law and 0 for G.711 μ-Law). The parameters defining payload type for the 'old' Bypass mode FaxBypassPayloadType and ModemBypassPayloadType are not used with NSE Bypass. The bypass packet interval is selected according to the FaxModemBypassBasicRtpPacketInterval parameter.</p> <p>Notes:</p> <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=rtpmap: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 143).
EMS: NSE Payload Type [NSEPayloadType]	<p>NSE payload type for Cisco Bypass compatible mode. The valid range is 96-127. The default value is 105.</p> <p>Note: Cisco gateways usually use NSE payload type of 100.</p>
Web: V.21 Modem Transport Type EMS: V21 Transport [V21ModemTransportType]	<p>V.21 Modem Transport Type used by the device.</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

Parameter	Description
	<p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).</p>
Web: V.22 Modem Transport Type EMS: V22 Transport [V22ModemTransportType]	<p>V.22 Modem Transport Type used by the device.</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 143).</p>
Web: V.23 Modem Transport Type EMS: V23 Transport [V23ModemTransportType]	<p>V.23 Modem Transport Type used by the device.</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 143).</p>
Web: V.32 Modem Transport Type EMS: V32 Transport [V32ModemTransportType]	<p>V.32 Modem Transport Type used by the device.</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 143).
Web: V.34 Modem Transport Type EMS: V34 Transport [V34ModemTransportType]	<p>V.90/V.34 Modem Transport Type used by the device.</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 143).</p>
EMS: Bell Transport Type [BellModemTransportType]	<p>Determines the Bell modem transport method.</p> <ul style="list-style-type: none"> [0] = Transparent (default) [2] = Bypass [3] = Transparent with events

12.11.4 DTMF Parameters

The dual-tone multi-frequency (DTMF) parameters are described in the table below.

Table 12-32: 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>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>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>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>

12.11.5 RTP, RTCP and T.38 Parameters

The RTP, RTCP and T.38 parameters are described in the table below.

Table 12-33: RTP/RTCP and T.38 Parameters

Parameter	Description
Web: Dynamic Jitter Buffer Minimum Delay EMS: Minimal Delay (dB) [DJBufMinDelay]	Minimum delay (in msec) for the Dynamic Jitter Buffer. The valid range is 0 to 150. The default delay is 10. Notes: <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 412.
Web: Dynamic Jitter Buffer Optimization Factor EMS: Opt Factor [DJBufOptFactor]	Dynamic Jitter Buffer frame error/delay optimization factor. The valid range is 0 to 12. The default factor is 10. Notes: <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 412.
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]	Determines whether the device generates redundant packets. This can be used for packet loss where the missing information (audio) can be reconstructed at the receiver end from the redundant data that arrives in the subsequent packet(s). <ul style="list-style-type: none"> [0] 0 = Disable the generation of redundant packets (default). [1] 1 = Enable the generation of RFC 2198 redundancy packets (payload type defined by the parameter RFC2198PayloadType). Notes: <ul style="list-style-type: none"> The RTP redundancy dynamic payload type can be included in the SDP, by using the parameter EnableRTPRedundancyNegotiation. This parameter can also be configured per IP Profile, using the IPProfile parameter.
Web: Enable RTP Redundancy Negotiation [EnableRTPRedundancyNegotiation]	Determines whether the device includes the RTP redundancy dynamic payload type in the SDP, according to RFC 2198. <ul style="list-style-type: none"> [0] Disable (default)

Parameter	Description
	<ul style="list-style-type: none"> ▪ [1] Enable <p>When enabled, the device includes in the SDP message the RTP payload type "RED" and the payload type configured by the parameter <code>RFC2198PayloadType</code>.</p> <pre>a=rtpmap:<PT> RED/8000</pre> <p>Where <code><PT></code> is the payload type as defined by <code>RFC2198PayloadType</code>. 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 <code>RTPRedundancyDepth</code> to 1 (i.e., enabled). ▪ Currently, the negotiation of "RED" payload type is not supported and therefore, it should be configured to the same PT value for both parties.
Web: RFC 2198 Payload Type EMS: Redundancy Payload Type [RFC2198PayloadType]	<p>RTP redundancy packet payload type according to RFC 2198.</p> <p>The range is 96 to 127. The default is 104.</p> <p>Note: This parameter is applicable only if the parameter <code>RTPRedundancyDepth</code> is set to 1.</p>
Web: Packing Factor EMS: Packetization Factor [RTPPackFactor]	N/A. Controlled internally by the device according to the selected coder.
Web/EMS: Basic RTP Packet Interval [BasicRTPPacketInterval]	N/A. Controlled internally by the device according to the selected coder.
Web: RTP Directional Control [RTPDirectionControl]	N/A. Controlled internally by the device according to the selected coder.
Web/EMS: RFC 2833 TX Payload Type [RFC2833TxPayloadType]	N/A. Use the <i>ini</i> file parameter <code>RFC2833PayloadType</code> instead.
Web/EMS: RFC 2833 RX Payload Type [RFC2833RxPayloadType]	N/A. Use the <i>ini</i> file parameter <code>RFC2833PayloadType</code> instead.
[EnableDetectRemoteMACChange]	<p>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.

Parameter	Description
	<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>Lower boundary of the UDP port used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2). The upper boundary of the UDP port range is the Base UDP Port + 10 * number of the device's channels.</p> <p>The range of possible UDP ports is 6,000 to 64,000. The default base UDP port is 6000.</p> <p>For example, if the Base UDP Port is set to 6000, then 1) one channel may use the ports RTP 6000, RTCP 6001, and T.38 6002, 2) another channel may use RTP 6010, RTCP 6011, and T.38 6012, etc.</p> <p>The UDP port range is 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 109). If RTP Base UDP Port is not a factor of 10, the following message is generated: 'invalid local RTP port'. For detailed information on the default RTP/RTCP/T.38 port allocation, refer to the <i>Product Reference Manual</i>.
EMS: No Op Enable [NoOpEnable]	<p>Enables or disables 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.</p> <p>The valid range is 20 to 65,000 msec. The default is 10,000.</p> <p>Note: To enable No-Op packet transmission, use the NoOpEnable parameter.</p>
EMS: No Op Payload Type [RTPNoOpPayloadType]	<p>Determines the payload type of No-Op packets.</p> <p>The valid range is 96 to 127 (for the range of Dynamic RTP Payload Type for all types of non hard-coded RTP Payload types, refer to RFC 3551). The default value is 120.</p> <p>Note: When defining this parameter, ensure that it doesn't cause collision with other payload types.</p>

12.12 Gateway and IP-to-IP Parameters

12.12.1 Fax and Modem Parameters

The fax and modem parameters are described in the table below.

Table 12-34: Fax and Modem Parameters

Parameter	Description
EMS: T38 Use RTP Port [T38UseRTPPort]	<p>Defines the port (with relation to RTP port) for sending and receiving T.38 packets.</p> <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. <p>Notes:</p> <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]	<p>Defines the maximum size of a T.38 datagram that the device can receive. This value is included in the outgoing SDP when T.38 is used.</p> <p>The valid range is 120 to 600. The default value is 560.</p>
Web/EMS: T38 Fax Max Buffer [T38FaxMaxBufferSize]	<p>Defines the maximum size (in bytes) of the device's T.38 buffer. This value is included in the outgoing SDP when T.38 is used for fax relay over IP.</p> <p>The valid range is 500 to 3000. The default value is 3000.</p>
Web/EMS: Enable Fax Re-Routing [EnableFaxReRouting]	<p>Enables or disables re-routing of Tel-to-IP calls that are identified as fax calls.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enabled. <p>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. 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> <p>Notes:</p> <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.

Parameter	Description
Web/EMS: Fax CNG Mode [FaxCNGMode]	<p>Determines the device's behavior upon detection of a CNG tone.</p> <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: Detect Fax on Answer Tone EMS: Enables Detection of FAX on Answer Tone [DetFaxOnAnswerTone]	<p>Determines when the device initiates a T.38 session for fax transmission.</p> <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. <p>Notes:</p> <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 set to 1 (T.38 Relay) or 3 (Fax Fallback).
[T38FaxSessionImmediateStart]	<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>
Web: T38 Version [SIPT38Version]	<p>Selects the T.38 fax relay version.</p> <ul style="list-style-type: none"> [-1] Not Configured = No T.38 (default) [0] T.38 version 0 (default) [3] T.38 version 3 = T.38 Version 3 (V.34 over T.38 support) <p>Note: For a description on V.34 over T.38 fax relay, see V.34 Fax Support on page 449.</p>

12.12.2 DTMF and Hook-Flash Parameters

The DTMF and hook-flash parameters are described in the table below.

Table 12-35: 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: Determines 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 occurred and sends a SIP INFO message if the parameter HookFlashOption is set to 1, indicating 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).</p> <ul style="list-style-type: none"> ▪ [0] Not Supported = Hook-Flash indication isn't sent (default). ▪ [1] INFO = Sends proprietary INFO message with Hook-Flash indication. ▪ [4] RFC 2833 ▪ [5] INFO (Lucent) = Sends proprietary SIP INFO message with Hook-Flash indication. ▪ [6] INFO (NetCentrex) = Sends proprietary SIP INFO message with Hook-Flash indication. The device sends the INFO message as follows: Content-Type: application/dtmf-relay Signal=16 Where 16 is the DTMF code for hook flash ▪ [7] INFO (HUAWEI) = 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 parameter EnableHold is set to 0.

Parameter	Description
Web: Min. Flash-Hook Detection Period [msec] EMS: Min Flash Hook Time [MinFlashHookTime]	<p>Defines the minimum time (in msec) for detection of a hook-flash event. Detection is guaranteed for hook-flash periods of at least 60 msec (when setting the minimum time to 25). Hook-flash signals that last a shorter period of time are ignored. The valid range is 25 to 300. The default value is 300.</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 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]	<p>Defines the hook-flash period (in msec) for both Tel and IP sides (per device). For the IP side, it defines the hook-flash period that is reported to the IP.</p> <p>For the analog side, it defines the following:</p> <ul style="list-style-type: none"> 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. <p>The valid range is 25 to 3,000. The default value is 700.</p> <p>Notes:</p> <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 hook-flash, set this parameter to 550. This parameter can also be configured per Tel Profile, using the TelProfile parameter.
DTMF Parameters	
EMS: Use End of DTMF [MGCPDTMFDetectionPoint]	<p>Defines when the detection of DTMF events is notified.</p> <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]	<p>Defines the supported receive DTMF negotiation method.</p> <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>

Parameter	Description
Web/EMS: Tx DTMF Option [TxDTMFOption]	<p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).</p> <p>Determines a single or several preferred transmit DTMF negotiation methods.</p> <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>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: <ul style="list-style-type: none"> a. Negotiates RFC 2833 payload type using local and remote SDPs. b. Sends DTMF packets using RFC 2833 payload type according to the payload type in the received SDP. c. Expects to receive RFC 2833 packets with the same payload type as configured by the parameter RFC2833PayloadType. d. Removes DTMF digits in transparent mode (as part of the voice stream). ▪ When TxDTMFOption is set to 0, the RFC 2833 payload type is set according to the parameter RFC2833PayloadType for both transmit and receive. ▪ 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 143).

Parameter	Description
Web/EMS: Tx DTMF Option Table	
[TxDTMFOption]	<p>This <i>ini</i> file table parameter configures up to two preferred transmit DTMF negotiation methods. The format of this parameter is as follows:</p> <pre>[TxDTMFOption] FORMAT TxDTMFOption_Index = TxDTMFOption_Type; [TxDTMFOption]</pre> <p>For example: TxDTMFOption 0 = 1; TxDTMFOption 1 = 3;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter can include up to two indices. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143). ▪ For a description on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
[DisableAutoDTMFMute]	<p>Enables/disables 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>
Web/EMS: Enable Digit Delivery to IP [EnableDigitDelivery2IP]	<p>The Digit Delivery feature enables sending DTMF digits 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.

Parameter	Description
Web: Enable Digit Delivery to Tel EMS: Enable Digit Delivery [EnableDigitDelivery]	<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 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 <code>IsWaitForDialTone</code> (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 <code>TelProfile</code> parameter.
Web/EMS: RFC 2833 Payload Type [RFC2833PayloadType]	<p>The RFC 2833 DTMF relay dynamic payload type. The valid range is 96 to 99, and 106 to 127. The default is 96. The 100, 102 to 105 range is allocated for proprietary usage.</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 <code>TxDTMFOption</code> is set to 4), this payload type is

Parameter	Description
	used for the received DTMF packets. If negotiation isn't used, this payload type is used for receive and for transmit.
[ReplaceNumberSignWithEscapeChar]	<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.
Web: Special Digit Representation EMS: Use Digit For Special DTMF [UseDigitForSpecialDTMF]	<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.

12.12.3 Digit Collection and Dial Plan Parameters

The digit collection and dial plan parameters are described in the table below.

Table 12-36: Digit Collection and Dial Plan Parameters

Parameter	Description
Web/EMS: Dial Plan Index [DialPlanIndex]	<p>Determines the Dial Plan index to use in the external Dial Plan file. The Dial Plan file is loaded to the device as a *.dat file (converted using the DConvert utility). The Dial Plan index can be defined globally or per Tel Profile.</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

Parameter	Description
	<p>the TelProfile parameter.</p> <ul style="list-style-type: none"> For a detailed description of the Dial Plan file, see "External Dial Plan File" on page 415.
[Tel2IPSourceNumberMapping DialPlanIndex]	<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 a detailed description of this feature, see "Modifying ISDN-to-IP Calling Party Number" on page 417.</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 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>An example of a digit map is shown below: 11xS 00T [1-7]xxx 8xxxxxxx #xxxxxxx *xx 91xxxxxxxxxx 9011x.T In the example above, the last rule can apply to International numbers: 9 for dialing tone, 011 Country Code, and then any number of digits for the local number ('x.').</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 a detailed description of digit mapping, see "Digit Mapping" on page 414.

Parameter	Description
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>

12.12.4 Voice Mail Parameters

The voice mail parameters are described in the table below. For detailed information on the Voice Mail application, refer to the *CPE Configuration Guide for Voice Mail*.

Table 12-37: 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 enable voice mail per Hunt Group, you can use a Tel Profile ID (using the TelProfile parameter) that is configured with voice mail interface enabled. This eliminates the phenomenon of call delay on 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 or disables 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 = Disable (default).▪ [1] Enable = 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> <table><tr><th>Redirecting Reason</th><th>>></th><th>SIP Response Code</th></tr><tr><td>Unknown</td><td>>></td><td>404</td></tr><tr><td>User busy</td><td>>></td><td>486</td></tr><tr><td>No reply</td><td>>></td><td>408</td></tr><tr><td>Deflection</td><td>>></td><td>487/480</td></tr></table>	Redirecting Reason	>>	SIP Response Code	Unknown	>>	404	User busy	>>	486	No reply	>>	408	Deflection	>>	487/480
Redirecting Reason	>>	SIP Response Code														
Unknown	>>	404														
User busy	>>	486														
No reply	>>	408														
Deflection	>>	487/480														

Parameter	Description
	<p>Unconditional >> 302</p> <p>Others >> 302</p> <p>If the device receives a Request-URI that includes a 'target' and 'cause' parameter, the 'target' is mapped to the Redirect phone number and the 'cause' is mapped to the Redirect number reason.</p>
Web/EMS: Line Transfer Mode [LineTransferMode]	<p>Determines the call transfer method used by the device.</p> <ul style="list-style-type: none"> ▪ [0] None = IP (default). ▪ [1] Blind = PBX blind transfer. After receiving a REFER message from the IP side, the FXO sends a hook-flash to the PBX, dials the digits (that are received in the Refer-To header), and then immediately drops the line (on-hook). The PBX performs the transfer internally. ▪ [2] Semi Supervised = PBX Semi-Supervised transfer. After receiving a REFER message from the IP side, the FXO sends a hook-flash to the PBX, and then dials the digits (that are received in the Refer-To header). If no Busy or Reorder tones are detected (within approximately 2 seconds), the device completes the call transfer by releasing the line; otherwise, the transfer is cancelled, the device sends a SIP NOTIFY message with a failure reason in the NOTIFY body (such as 486 if busy tone detected), and generates an additional hook-flash towards the FXO line to restore connection to the original call. ▪ [3] Supervised = PBX Supervised transfer. After receiving a REFER message from the IP side, the FXO sends a hook-flash to the PBX, and then dials the digits (that are received in the Refer-To header). The FXO waits for connection of the transfer call and if speech is detected (e.g., "hello") within approximately 2 seconds, the device completes the call transfer by releasing the line; otherwise, the transfer is cancelled, the device sends a SIP NOTIFY message with a failure reason in the NOTIFY body (such as 486 if busy tone detected) and generates an additional hook-flash towards the FXO line to restore connection to the original call.
Message Waiting Indication (MWI) Parameters	
Web: MWI Off Digit Pattern EMS: MWI Off Code [MWIOffCode]	<p>Determines the digit code used by the device to notify the PBX that there aren't any messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string.</p>
Web: MWI On Digit Pattern EMS: MWI On Code [MWIONCode]	<p>Determines the digit code used by the device to notify the PBX of messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string.</p>
Web: MWI Suffix Pattern EMS: MWI Suffix Code [MWISuffixCode]	<p>Determines the digit code used by the device as a suffix for 'MWI On Digit Pattern' and 'MWI Off Digit Pattern'. This suffix is added to the generated DTMF string after the extension number. The valid range is a 25-character string.</p>

Parameter	Description
Web: MWI Source Number EMS: MWI Source Name [MWISourceNumber]	Determines the calling party's phone number used in the Q.931 MWI Setup message to PSTN. If not configured, the channel's phone number is used as the calling number.
Digit Patterns The following digit pattern parameters apply only to voice mail applications that use the DTMF communication method. For the available pattern syntaxes, refer to the <i>CPE Configuration Guide for Voice Mail</i> .	
Web: Forward on Busy Digit Pattern (Internal) EMS: Digit Pattern Forward On Busy [DigitPatternForwardOnBusy]	Determines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an internal extension. The valid range is a 120-character string.
Web: Forward on No Answer Digit Pattern (Internal) EMS: Digit Pattern Forward On No Answer [DigitPatternForwardOnNoAnswer]	Determines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an internal extension. The valid range is a 120-character string.
Web: Forward on Do Not Disturb Digit Pattern (Internal) EMS: Digit Pattern Forward On DND [DigitPatternForwardOnDND]	Determines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an internal extension. The valid range is a 120-character string.
Web: Forward on No Reason Digit Pattern (Internal) EMS: Digit Pattern Forward No Reason [DigitPatternForwardNoReason]	Determines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an internal extension. The valid range is a 120-character string.
Web: Forward on Busy Digit Pattern (External) EMS: VM Digit Pattern On Busy External [DigitPatternForwardOnBusyExt]	Determines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Web: Forward on No Answer Digit Pattern (External) EMS: VM Digit Pattern On No Answer Ext [DigitPatternForwardOnNoAnswerExt]	Determines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Web: Forward on Do Not Disturb Digit Pattern (External) EMS: VM Digit Pattern On DND External [DigitPatternForwardOnDNDExt]	Determines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Web: Forward on No Reason Digit Pattern (External) EMS: VM Digit Pattern No Reason External [DigitPatternForwardNoReasonExt]	Determines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.

Parameter	Description
Web: Internal Call Digit Pattern EMS: Digit Pattern Internal Call [DigitPatternInternalCall]	Determines the digit pattern used by the PBX to indicate an internal call. The valid range is a 120-character string.
Web: External Call Digit Pattern EMS: Digit Pattern External Call [DigitPatternExternalCall]	Determines the digit pattern used by the PBX to indicate an external call. The valid range is a 120-character string.
Web: Disconnect Call Digit Pattern EMS: Tel Disconnect Code [TelDisconnectCode]	Determines a digit pattern that when received from the Tel side, indicates the device to disconnect the call. The valid range is a 25-character string.
Web: Digit To Ignore Digit Pattern EMS: Digit To Ignore [DigitPatternDigitToIgnore]	A digit pattern that if received as Src (S) or Redirect (R) numbers is ignored and not added to that number. The valid range is a 25-character string.

12.12.5 Supplementary Services Parameters

This subsection describes the device's supplementary telephony services parameters.

12.12.5.1 Caller ID Parameters

The caller ID parameters are described in the table below.

Table 12-38: Caller ID Parameters

Parameter	Description
Web: Caller ID Permissions Table EMS: SIP Endpoints > Caller ID	
[EnableCallerID]	<p>This ini file table parameter configures Caller ID permissions. It allows you to enable or disable (per port) Caller ID generation (for FXS interfaces) and detection (for FXO interfaces). The format of this parameter is as follows:</p> <pre>[EnableCallerID] FORMAT EnableCallerID_Index = EnableCallerID_IsEnabled, EnableCallerID_Module, EnableCallerID_Port; [EnableCallerID]</pre> <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 188. For an explanation on using ini file table parameters, see Configuring ini File Table Parameters on page 368.
Web: Caller Display Information Table EMS: SIP Endpoints > Caller ID	
[CallerDisplayInfo]	<p>This ini file table parameter enables the device to send Caller ID information to IP when a call is made. The called party can use this information for caller identification. The information configured in this table is sent in the SIP INVITE message's</p>

Parameter	Description
	<p>From header. The format of this parameter is as follows:</p> <pre>[CallerDisplayInfo] FORMAT CallerDisplayInfo_Index = CallerDisplayInfo_DisplayString, CallerDisplayInfo_IsCidRestricted, CallerDisplayInfo_Module, CallerDisplayInfo_Port; [\CallerDisplayInfo]</pre> <p>Where,</p> <ul style="list-style-type: none"> DisplayString = Caller ID string (up to 18 characters). 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 185. For an explanation on using ini file table parameters, see Configuring ini File Table Parameters on page 368.

Parameter	Description
Web/EMS: Enable Caller ID [EnableCallerID]	<p>Determines whether Caller ID is enabled.</p> <ul style="list-style-type: none"> [0] Disable = Disable the Caller ID service (default). [1] Enable = Enable the Caller ID service. <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 185. To disable/enable caller ID generation per port, see Configuring Call Forward on page 186.</p>
Web: Caller ID Type EMS: Caller id Types [CallerIDType]	<p>Defines one of the following standards for detection (FXO) and generation (FXS) of Caller ID, and detection (FXO) generation (FXS) of MWI (when specified) signals:</p> <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 [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.

Parameter	Description																											
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 = Interworking of CPC is performed <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> <p style="padding-left: 40px;">From:<sip:+551137077801;cpc=payphone@10.20.7.35>;tag=53700</p> <p>The calling number manipulation removes "+55" (leaving 10 digits), and then adds the prefix 7, the cpc code for payphone user. Therefore, the Caller ID number that is sent to the FXS port, in this example is 71137077801.</p> <p>If the incoming INVITE message doesn't contain the 'cpc' parameter, nothing is added to the Caller ID number.</p> <table><tr><th>CPC Value in Received INVITE</th><th>CPC Code Prefixed to Caller ID (Sent to FXS Endpoint)</th><th>Description</th></tr><tr><td>cpc=unknown</td><td>1</td><td>Unknown user</td></tr><tr><td>cpc=subscribe</td><td>1</td><td>-</td></tr><tr><td>cpc=ordinary</td><td>1</td><td>Ordinary user</td></tr><tr><td>cpc=priority</td><td>2</td><td>Pre-paid user</td></tr><tr><td>cpc=test</td><td>3</td><td>Test user</td></tr><tr><td>cpc=operator</td><td>5</td><td>Operator</td></tr><tr><td>cpc=data</td><td>6</td><td>Data call</td></tr><tr><td>cpc=payphone</td><td>7</td><td>Payphone user</td></tr></table> <p>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 Value in Received INVITE	CPC Code Prefixed to Caller ID (Sent to FXS Endpoint)	Description	cpc=unknown	1	Unknown user	cpc=subscribe	1	-	cpc=ordinary	1	Ordinary user	cpc=priority	2	Pre-paid user	cpc=test	3	Test user	cpc=operator	5	Operator	cpc=data	6	Data call	cpc=payphone	7	Payphone user
CPC Value in Received INVITE	CPC Code Prefixed to Caller ID (Sent to FXS Endpoint)	Description																										
cpc=unknown	1	Unknown user																										
cpc=subscribe	1	-																										
cpc=ordinary	1	Ordinary user																										
cpc=priority	2	Pre-paid user																										
cpc=test	3	Test user																										
cpc=operator	5	Operator																										
cpc=data	6	Data call																										
cpc=payphone	7	Payphone user																										
[EnableCallerIDTypeTwo]	<p>Disables the generation of Caller ID type 2 when the phone is off-hooked. Caller ID type 2 (also known as off-hook Caller ID) is sent to a currently busy telephone to display the caller ID of the waiting call.</p> <ul style="list-style-type: none">[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																											

Parameter	Description
	<p>generate the Caller ID according to the selected Caller ID type.</p> <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>Selects 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>Selects 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 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</p>

Parameter	Description
	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.
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"> ▪ 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>

12.12.5.2 Call Waiting Parameters

The call waiting parameters are described in the table below.

Table 12-39: 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>

Parameter	Description
	<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 ini file table parameter CallWaitingPerPort to enable Call Waiting per port. For information on the Call Waiting feature, see "Call Waiting" on page 460. For information on the Call Progress Tones file, see Configuring the Call Progress Tones File.
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.
Web: Call Waiting Table EMS: SIP Endpoints > Call Waiting	
[CallWaitingPerPort]	<p>This ini file table parameter 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. Module = Module number. <p>For example: CallWaitingPerPort 0 = 0,1,1; (call waiting disabled for Port 1 of Module 1) CallWaitingPerPort 1 = 1,1,2; (call waiting enabled for Port 2 of Module 1)</p> <p>Notes:</p> <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

Parameter	Description
	<p>EnableCallWaiting.</p> <ul style="list-style-type: none"> 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 189. For a description on using ini file table parameters, see Configuring ini File Table Parameters on page 368.
Web: Number of Call Waiting Indications EMS: Call Waiting Number of Indications [NumberOfWaitingIndications]	<p>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.</p> <p>Note: This parameter is applicable only to FXS ports.</p>
Web: Time Between Call Waiting Indications EMS: Call Waiting Time Between Indications [TimeBetweenWaitingIndications]	<p>Time (in seconds) between consecutive call waiting indications for call waiting. The valid range is 1 to 100. The default value is 10.</p> <p>Note: This parameter is applicable only to FXS ports.</p>
Web/EMS: Time Before Waiting Indications [TimeBeforeWaitingIndication]	<p>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.</p> <p>Note: This parameter is applicable only to FXS ports.</p>
Web/EMS: Waiting Beep Duration [WaitingBeepDuration]	<p>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.</p> <p>Note: This parameter is applicable only to FXS ports.</p>
EMS: First Call Waiting Tone ID [FirstCallWaitingToneID]	<p>Determines the index of the first Call Waiting Tone in the CPT file. This feature enables the called party to distinguish between different call origins (e.g., external versus internal calls).</p> <p>There are three ways to use the distinctive call waiting tones:</p> <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 ini file table parameter. Playing the call waiting tone according to the parameter "CallWaitingTone#" of a SIP INFO message. <p>The device plays the tone received in the 'play tone CallWaitingTone#' parameter of an INFO message plus the value of this parameter minus 1. 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

Parameter	Description
	<p>sequence in the CPT file.</p> <ul style="list-style-type: none"> 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>

12.12.5.3 Call Forwarding Parameters

The call forwarding parameters are described in the table below.

Table 12-40: Call Forwarding Parameters

Parameter	Description
Web: Enable Call Forward [EnableForward]	<p>Determines whether Call Forward is enabled.</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.</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 ini file table parameter forwards (redirects) IP-to-Tel calls (using SIP 302 response) to other device ports or an IP destination, based on the device's port to which the call was originally routed. The format of this parameter is as follows:</p> <pre>[FwdInfo] FORMAT FwdInfo_Index = FwdInfo_Type, FwdInfo_Destination, FwdInfo_NoReplyTime, FwdInfo_Module, FwdInfo_Port; [FwdInfo]</pre> <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).

Parameter	Description
	<ul style="list-style-type: none"> ✓ [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 186. ▪ For an explanation on using ini file table parameters, see Configuring ini File Table Parameters on page 368.
Call Forward Reminder Ring Parameters <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 458. 	
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

Parameter	Description
Web: AS Subscribe IPGroupID [ASSubscribeIPGroupID]	Defines the IP Group ID that contains the Application server for Subscription. The valid value range is 1 to 8. The default is -1 (i.e., not configured).
Web: NRT Retry Subscription Time [NRTRetrySubscriptionTime]	Defines the Retry period (in seconds) for Dialog subscription if a previous request failed. The valid value range is 10 to 7200. The default is 120.
Web: Call Forward Ring Tone ID [CallForwardRingToneID]	Defines the ringing tone type played when call forward notification is accepted. The valid value range is 1 to 5. The default is 1.

12.12.5.4 Message Waiting Indication Parameters

The message waiting indication (MWI) parameters are described in the table below.

Table 12-41: 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 detailed information on MWI, see "Message Waiting Indication" on page 461.
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]	Determines whether MWI information is sent 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

Parameter	Description
	the TelProfile parameter).
Web: Subscribe to MWI EMS: Enable MWI Subscription [EnableMWISubscription]	<p>Enables subscription to an MWI server.</p> <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). <p>Note: To configure whether the device subscribes per endpoint or per the entire device, use the parameter SubscriptionMode.</p>
Web: MWI Server IP Address EMS: MWI Server IP [MWIServerIP]	MWI server's IP address. If provided, the device subscribes to this IP address. The MWI server address can be configured as a numerical IP address or as a domain name. If not configured, the Proxy IP address is used instead.
Web/EMS: MWI Server Transport Type [MWIServerTransportType]	<p>Determines the transport layer used for outgoing SIP dialogs initiated by the device to the MWI server.</p> <ul style="list-style-type: none"> [-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: MWI Subscribe Expiration Time EMS: MWI Expiration Time [MWIExpirationTime]	<p>The MWI subscription expiration time in seconds.</p> <p>The default is 7200 seconds. The range is 10 to 2,000,000.</p>
Web: MWI Subscribe Retry Time EMS: Subscribe Retry Time [SubscribeRetryTime]	<p>Subscription retry time (in seconds) after last subscription failure.</p> <p>The default is 120 seconds. The range is 10 to 2,000,000.</p>
Web: Subscription Mode [SubscriptionMode]	<p>Determines the method the device uses to subscribe to an MWI server.</p> <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]	<p>Selects the ETSI Visual Message Waiting Indication (VMWI) Type 1 sub-standard.</p> <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 <p>Note: For this parameter to take effect, a device reset is</p>

Parameter	Description
	required.
EMS: Bellcore VMWI Type One Standard [BellcoreVMWITypeOneStandard]	<p>Selects the Bellcore VMWI 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>

12.12.5.5 Call Hold Parameters

The call hold parameters are described in the table below.

Table 12-42: Call Hold Parameters

Parameter	Description
Web/EMS: Enable Hold [EnableHold]	<p>For digital interfaces:</p> <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default) <p>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 143).
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>Determines the time interval that the device allows for a call to remain on hold. If a Resume (un-hold Re-INVITE) message is received before the timer expires, the call is renewed. If this timer expires, the call is released (terminated).</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.

Parameter	Description
Web: Call Hold Reminder Ring Timeout EMS: CHRR Timeout [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]	<p>Disables the reminder ring, which notifies the FXS user of a call on hold or a waiting call when the phone is returned to on-hook position.</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>Enables playing DTMF signals to the Tel side when a call is on hold.</p> <ul style="list-style-type: none"> [0] = Disable (default) - if the call is in Hold (inactive) state, the device does not play DTMF signals to the Tel if it receives SIP INFO DTMF messages. [1] = Enable - the device stops playing the Held tone (if it was played) and starts playing DTMF digits according to received SIP INFO message(s). (The stopped Held tone is not played again.)

12.12.5.6 Call Transfer Parameters

The call transfer parameters are described in the table below.

Table 12-43: Call Transfer Parameters

Parameter	Description
Web/EMS: Enable Transfer [EnableTransfer]	<p>Determines whether call transfer is enabled.</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.

Parameter	Description
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 applicable to FXO/CAS Blind Transfer modes (LineTransferMode = 1, 2 or 3 for FXO; TrunkTransferMode = 3 for CAS). 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.
[KeyBlindTransfer]	<p>Keypad sequence that activates blind transfer for Tel-to-IP calls. There are two possible scenarios:</p> <ul style="list-style-type: none"> Option 1: After this sequence is dialed, the current call is put on hold (using Re-INVITE), a dial tone is played to the B-channel, and then phone number collection starts. Option 2: A Hook-Flash is pressed, the current call is put on hold, a dial tone is played to the B-channel, and then digit collection starts. After this sequence is identified, the device continues the collection of the destination phone number. <p>For both options, after the phone number is collected, it's sent to the transferee in a SIP REFER request (without a Replaces header). The call is then terminated and a confirmation tone is played to the B-channel. If the phone number collection fails due to a mismatch, a reorder tone is played to the B-channel.</p> <p>Note: 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>

Parameter	Description
EMS: Blind Transfer Add Prefix [KeyBlindTransferAddPrefix]	<p>Determines whether the device adds the Blind Transfer code (KeyBlindTransfer) 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.</p> <p>The valid range is 0 to 1,000,000. The default is 0.</p>

12.12.5.7 Three-Way Conferencing Parameters

The three-way conferencing parameters are described in the table below.

Table 12-44: Three-Way Conferencing Parameters

Parameter	Description
Web: Enable 3-Way Conference EMS: Enable 3 Way [Enable3WayConference]	<p>Enables or disables the 3-Way Conference feature.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default) ▪ [1] Enable = Enables 3-way conferencing <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>Defines 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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to FXS interfaces. ▪ When using an external conference server (i.e., options [0] or [1]),

Parameter	Description
	more than one three-way conference may be supported (up to six).
Web: Establish Conference Code EMS: Establish Code [ConferenceCode]	Defines the digit pattern, which upon detection, generates the Conference-initiating INVITE when 3-way conferencing is enabled (Enable3WayConference is set to 1). The valid range is a 25-character string. The default is "!" (Hook-Flash).
Web/EMS: Conference ID [ConferenceID]	Defines the Conference Identification string (up to 16 characters). The default value is 'conf'. The device uses this identifier in the Conference-initiating INVITE that is sent to the media server when Enable3WayConference is set to 1. For example: ConferenceID = MyConference.

12.12.5.8 Emergency Call Parameters

The emergency call parameters are described in the table below.

Table 12-45: Emergency Call Parameters

Parameter	Description
EMS: Enable 911 PSAP [Enable911PSAP]	<p>If enabled, the device supports E911 DID protocol according to 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>When one of these numbers is dialed, the outgoing INVITE message includes the SIP Priority and Resource-Priority headers. If the user places the phone on-hook, the call is not disconnected. Instead, a Hold Re-INVITE request is sent to the remote party. Only if the remote party disconnects the call (i.e., a BYE is received) or a timer expires (set by the EmergencyRegretTimeout parameter) is the call terminated. This scenario is applicable only to FXS interfaces.</p> <p>These emergency numbers can also be used for pre-emption of E911 IP-to-Tel calls when there are unavailable (busy) channels. In this scenario, the device terminates one of the busy channels and sends the E911 call to this channel. This feature is enabled by setting the CallPriorityMode parameter to 2 ("Emergency") and by defining an emergency number value of "911" for the EmergencyNumbers parameter. For a description of this feature, see "Pre-empting Existing Call for E911 IP-to-Tel Call" on page 427. This scenario is applicable to FXS/FXO, CAS, and ISDN interfaces.</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>

Parameter	Description
Web: Emergency Calls Regret Timeout EMS: Emergency Regret Timeout [EmergencyRegretTimeout]	<p>Determines the time (in minutes) that the device waits before tearing-down an emergency call (defined by the parameter EmergencyNumbers). Until this time expires, an emergency call can only be disconnected by the remote party, typically, by a Public Safety Answering Point (PSAP).</p> <p>The valid range is 1 to 30. The default value is 10.</p> <p>Note: This parameter is applicable only to FXS interfaces.</p>

12.12.5.9 Call Cut-Through Parameters

The call cut-through parameters are described in the table below.

Table 12-46: 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-channel. 2 The device receives a SIP BYE (i.e., IP side ends the call) and plays a reorder tone to the PSTN side for the duration set by the CutThroughTimeForReOrderTone parameter. The device releases the call towards the IP side (sends a SIP 200 OK). 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.

Parameter	Description
	<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 TelProfile parameter) and therefore, assigned to specific B-channels that use specific CAS tables.

12.12.5.10 Automatic Dialing Parameters

The automatic dialing upon off-hook parameters are described in the table below.

Table 12-47: Automatic Dialing Parameters

Parameter	Description
Web: Automatic Dialing Table EMS: SIP Endpoints > Auto Dial	
[TargetOfChannel]	<p>This <i>ini</i> file table parameter defines telephone numbers that are automatically dialed when a specific FXS or FXO port is used (i.e., telephone is off-hooked). The format of this parameter is as follows:</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 HotLineToneDuration), the destination phone number is automatically dialed. ▪ Module = Module number (where 1 depicts the module in Slot 1). ▪ 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-</p>

Parameter	Description
	<p>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 184. ▪ For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.12.5.11 Direct Inward Dialing Parameters

The Direct Inward Dialing (DID) parameters are described in the table below.

Table 12-48: DID Parameters

Parameter	Description
Web/EMS: Enable DID Wink [EnableDIDWink]	<p>Enables Direct Inward Dialing (DID) using Wink-Start signaling.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disables DID Wink(default). ▪ [1] Enable = Enables DID Wink. <p>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> <p>Note: This parameter can also be configured per Tel Profile, using the TelProfile parameter.</p>
Web/EMS: Delay Before DID Wink [DelayBeforeDIDWink]	<p>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> <p>Note: This parameter is applicable only to FXS interfaces.</p>
EMS: NTT DID Signalling Form [NTTDIDSignallingForm]	<p>Determines the type of DID signaling support for NTT (Japan) modem: DTMF- or Frequency Shift Keying (FSK)-based signaling. The devices can be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX.</p> <ul style="list-style-type: none"> ▪ [0] = FSK-based signaling (default) ▪ [1] = DTMF-based signaling <p>Note: This parameter is applicable only to FXS interfaces.</p>

Parameter	Description
EMS: Enable DID [EnableDID]	<p>This <i>ini</i> file table parameter enables support for Japan NTT 'Modem' DID. FXS interfaces can be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX. The DID signal can be sent alone or combined with an NTT Caller ID signal.</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 an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
[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.

12.12.5.12 MLPP Parameters

The Multilevel Precedence and Preemption (MLPP) parameters are described in the table below.

Table 12-49: MLPP Parameters

Parameter	Description
Web/EMS: Call Priority Mode [CallPriorityMode]	<p>Enables priority call handling.</p> <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 congestion occurs in a network.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [2] Emergency = Preemption of IP-to-Tel E911 emergency calls. If the device receives an E911 call and there are unavailable channels to receive the call, the device terminates one of the channel calls and sends the E911 call to that channel. The preemption is done only on a channel pertaining to the same Hunt Group for which the E911 call was initially destined and if the channel select mode (configured by the ChannelSelectMode parameter) is set to other than "By Dest Number" (0). The preemption is done only if the incoming IP-to-Tel call is identified as an emergency call. The device identifies emergency calls by one of the following: <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 a detailed description, see "Pre-empting Existing Call for E911 IP-to-Tel Call" on page 427.
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]	Defines the default call priority for MLPP calls. <ul style="list-style-type: none"> ▪ [0] 0 = ROUTINE (default) ▪ [2] 2 = PRIORITY ▪ [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.</p>

Parameter	Description
	In this scenario, the character string is sent without translation to a numerical value.
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]	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 [MLPPDefaultServiceDomain]	MLPP default service domain string. If the device receives a non-MLPP ISDN incoming call (without a Precedence IE), it uses the parameter (if different than "FFFFFF") as a Service domain in the SIP Resource-Priority header in outgoing (Tel-to-IP calls) INVITE messages. This parameter is used in conjunction with the parameter SIPDefaultCallPriority. 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. The valid value is a 6 hexadecimal digits. The default is

Parameter	Description														
	"000000". Note: This parameter is applicable only to the MLPP NI-2 ISDN variant with CallPriorityMode set to 1.														
EMS: E911 MLPP Behavior [E911MLPPBehavior]	Defines the E911 (or Emergency Telecommunication Services/ETS) MLPP Preemption mode: <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. Note: This parameter is applicable only to analog interfaces.														
Web/EMS: Precedence Ringing Type [PrecedenceRingingType]	Defines the index of the Precedence Ringing tone in the Call Progress Tones (CPT) file. This tone is used when the parameter CallPriorityMode is set to 1 and a Precedence call is received from the IP side. The valid range is -1 to 16. The default value is -1 (i.e., plays standard Ringing tone). Note: This parameter is applicable only to analog interfaces.														
Multiple Differentiated Services Code Points (DSCP) per MLPP Call Priority Level (Precedence) Parameters <p>The MLPP service allows placement of priority calls, where properly validated users can preempt (terminate) lower-priority phone calls with higher-priority calls. For each MLPP call priority level, the DSCP can be set to a value from 0 to 63. The Resource Priority value in the Resource-Priority SIP header can be one of the following:</p> <table> <thead> <tr> <th>MLPP Precedence Level</th><th>Precedence Level in Resource-Priority SIP Header</th></tr> </thead> <tbody> <tr> <td>0 (lowest)</td><td>routine</td></tr> <tr> <td>2</td><td>priority</td></tr> <tr> <td>4</td><td>immediate</td></tr> <tr> <td>6</td><td>flash</td></tr> <tr> <td>8</td><td>flash-override</td></tr> <tr> <td>9 (highest)</td><td>flash-override-override</td></tr> </tbody> </table>		MLPP Precedence Level	Precedence Level in Resource-Priority SIP Header	0 (lowest)	routine	2	priority	4	immediate	6	flash	8	flash-override	9 (highest)	flash-override-override
MLPP Precedence Level	Precedence Level in Resource-Priority SIP Header														
0 (lowest)	routine														
2	priority														
4	immediate														
6	flash														
8	flash-override														
9 (highest)	flash-override-override														
Web/EMS: RTP DSCP for MLPP Routine [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).														

Parameter	Description
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).

12.12.5.13 ISDN BRI Parameters

The automatic dialing upon off-hook parameters are described in the table below.

Table 12-50: Automatic Dialing Parameters

Parameter	Description
Web: ISDN Supp Services Table	
[ISDNSuppServ]	<p>This <i>ini</i> file table parameter defines BRI phone extension numbers per BRI port and configures various ISDN supplementary services per BRI endpoint. The format of this parameter is as follows:</p> <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:</p> <pre>ISDNSuppServ 0 = 400, 1, 1, user, pass, callerid, 0, 1; ISDNSuppServ 1 = 401, 1, 1, user, pass, callerid, 0, 1;</pre>

Parameter	Description
	<p>Notes:</p> <ul style="list-style-type: none"> For an explanation on each of the table's parameters and for configuring the table using the Web interface, see "Configuring ISDN Supplementary Services" on page 191. For an explanation on using ini file table parameters, see "Configuring ini File Table Parameters" on page 368.
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 a detailed description of BRI call forwarding, see "BRI Call Forwarding" on page 460.</p>	
Call Forward Unconditional [SuppServCodeCFU]	<p>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>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>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>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>
Call Forward on No Reply [SuppServCodeCFNR]	<p>Prefix code for activating Call Forward on No Reply sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p>Note: The string must be enclosed in single apostrophe (e.g., '*72').</p>
Call Forward on No Reply Deactivation [SuppServCodeCFNRDeact]	<p>Prefix code for deactivating Call Forward on No Reply Deactivation sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p>Note: The string must be enclosed in single apostrophe (e.g., '*72').</p>

12.12.6 PSTN Parameters

This subsection describes the device's PSTN parameters.

12.12.6.1 General Parameters

The general PSTN parameters are described in the table below.

Table 12-51: General PSTN Parameters

Parameter	Description
Web/EMS: Protocol Type [ProtocolType]	<p>Defines the PSTN protocol for a 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] T1 HKT ISDN = ISDN PRI protocol for the Hong Kong - HKT.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [19] E1 KOR ISDN = ISDN PRI protocol for Korean Operator (similar to ETSI). ▪ [20] T1 HKT ISDN = ISDN PRI protocol for the Hong Kong - HKT. ▪ [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 ▪ [32] 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>Note: For supported protocols, please contact your AudioCodes representative.</p>
[ProtocolType_x]	Same as the description for the parameter ProtocolType, but for a specific trunk ID (where x denotes the Trunk ID and 0 is the first trunk).
[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).

Parameter	Description
[ISDNJapanNTTTimerT3JA]	<p>T3_JA timer (in seconds). This parameter overrides the internal PSTN T301 timeout on the Users Side (TE side). If an outgoing call from the device to ISDN is not answered during this timeout, the call is released. The valid range is 10 to 240. The default value is 50.</p> <p>Notes:</p> <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]	<p>Defines the trace level:</p> <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]	<p>Determines the physical framing method for the trunk.</p> <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) <p>Note: This parameter is not configurable for BRI interfaces; the device automatically uses the BRI framing method.</p>
[FramingMethod_x]	<p>Same as the description for parameter FramingMethod, but for a specific trunk ID (where x denotes the Trunk ID and 0 is the first Trunk).</p>

Parameter	Description
Web/EMS: Clock Master [ClockMaster]	<p>Determines the Tx clock source of the E1/T1 line.</p> <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. <p>Notes:</p> <ul style="list-style-type: none"> The source of the internal TDM bus clock is determined by the parameter TDMBusClockSource. For detailed information on configuring the device's clock settings, see "Clock Settings" on page 637.
[ClockMaster_x]	<p>Same as the description for parameter ClockMaster, but for a specific Trunk ID (where x denotes the Trunk ID and 0 is the first Trunk).</p>
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).
[LineCode_x]	<p>Same as the description for parameter LineCode, but for a specific trunk ID (where 0 depicts the first trunk).</p>
[TrunkAdministrativeState]	<p>Defines the administrative state of a trunk.</p> <ul style="list-style-type: none"> [0] = Lock the trunk; stops trunk traffic to configure the trunk protocol type. [2] = Unlock the trunk (default); enables trunk traffic.
[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 '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 647.

12.12.6.2 TDM Bus and Clock Timing Parameters

The TDM Bus parameters are described in the table below.

Table 12-52: TDM Bus and Clock Timing Parameters

Parameter	Description
TDM Bus Parameters	
Web/EMS: PCM Law Select [PCMLawSelect]	<p>Determines the type of PCM companding law in input/output TDM bus.</p> <ul style="list-style-type: none"> ▪ [1] Alaw = Alaw (default) ▪ [3] MuLaw = MuLaw <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>Selects 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. <p>For detailed information on configuring the device's clock settings, see "Clock Settings" on page 637.</p>
EMS/Web: TDM Bus Local Reference [TDMBusLocalReference]	<p>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]	Selects 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]	Determines 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 or disables 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 or disables 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>

12.12.6.3 CAS Parameters

The Common Channel Associated (CAS) parameters are described in the table below. Note that CAS is not applicable to BRI interfaces.

Table 12-53: CAS Parameters

Parameter	Description
Web: CAS Transport Type EMS: CAS Relay Transport Mode [CASTransportType]	<p>Controls 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>Determines if delimiters are added to the received address or received ANI digits string.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable <p>When this parameter is enabled, delimiters such as '*', '#', and 'ST' are added to the received address or received ANI digits string. When it is disabled, the address and ANI strings remain without delimiters.</p>
[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>

Parameter	Description
Web: Dial Plan EMS: Dial Plan Name [CASTrunkDialPlanName_x]	<p>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 DialPlanFileName = 'DialPlan_USA.dat' CASTrunkDialPlanName_5 = 'AT_T'</pre>
[CASFileName_x]	<p>CAS file name (e.g., 'E_M_WinkTable.dat') that defines the CAS protocol, where x denotes the CAS file ID (0-7). It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the device's trunks, using the parameter CASTableIndex_x.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: CAS Table per Channel [CASChannelIndex]	<p>Defines the loaded CAS protocol table index per B-channel pertaining to a CAS trunk. This parameter is assigned a string value and can be set in one of the following two formats:</p> <ul style="list-style-type: none"> 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>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>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> <p>Notes:</p> <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.

Parameter	Description
[CASTablesNum]	Indicates 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 99.	
Web: Generate Digit On Time [CASStateMachineGenerateDigitOnTime]	Generates digit on-time (in msec). The value must be a positive value. The default value is -1.
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 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.
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.

12.12.6.4 ISDN Parameters

The ISDN parameters are described in the table below.

Table 12-54: ISDN Parameters

Parameter	Description
Web: ISDN Termination Side EMS: Termination Side [TerminationSide]	<p>Selects the ISDN termination side.</p> <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'. The BRI module supports the ITU-T I.430 standard, which defines the ISDN-BRI layer 1 specification. The BRI 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]	<p>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).</p>
BRI Layer 2 Mode [BriLayer2Mode]	<p>Determines whether Point-to-Point or Point-to-Multipoint mode for BRI ports.</p> <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]	<p>Determines the ISDN B-Channel negotiation mode.</p> <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.

Parameter	Description
NFAS Parameters	
Note: These parameters are applicable to PRI interfaces.	
Web: NFAS Group Number EMS: Group Number [NFASGroupNumber_x]	<p>Indicates the NFAS group number (NFAS member) for the selected trunk, where x depicts the Trunk ID.</p> <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 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 a detailed description on NFAS, see "ISDN Non-Facility Associated Signaling (NFAS)" on page 643.
Web/EMS: D-channel Configuration [DChConfig_x]	<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>
Web: NFAS Interface ID EMS: ISDN NFAS Interface ID [ISDNNFASInterfaceID_x]	<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 a detailed description on NFAS, see "ISDN Non-Facility Associated Signaling (NFAS)" on page 643.
Web: Enable ignoring ISDN Disconnect with PI [KeepISDNCallOnDisconnectWithPI]	<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).
Web: PI For Setup Message [PIForSetupMsg]	<p>Determines whether and which Progress Indicator (PI) information element (IE) is added to the sent ISDN Setup message. Some ISDN protocols such as Euro ISDN can optionally contain PI = 1 or PI = 3 in the Setup message.</p> <ul style="list-style-type: none"> [0] = PI is not added (default).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [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.
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.	
Web/EMS: Incoming Calls Behavior [ISDNInCallsBehavior]	<p>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 (answer) message on incoming Tel calls. ▪ [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. ▪ [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</p>

Parameter	Description
	ISDNInCallsBehavior = 67584 (i.e., 2048 + 65536).
[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 unknown/unrecognized Facility IE. Otherwise, the Q.931 message that contains the unknown Facility IE is rejected (default). Note: This option is applicable only to ISDN variants where a complete ASN1 decoding is performed on Facility IE. ▪ [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 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).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [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 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 = Use the National mode of AT&T 5ESS for B-channel maintenance. <p>Notes:</p> <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]	<p>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).</p> <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

Parameter	Description
	<p>remote user has cleared the call, especially in the case of a long distance voice call.</p> <ul style="list-style-type: none"> ▪ [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. ▪ [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 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>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>
Web/EMS: Outgoing Calls Behavior [ISDNOutCallsBehavior]	<p>This parameter 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.

Parameter	Description
	<p>Note: This option is applicable only to the Korean variant.</p> <ul style="list-style-type: none"> ▪ [128] DIAL WITH KEYPAD = The device uses the Keypad IE to store the called number digits instead of the CALLED_NB IE. <p>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.</p> <ul style="list-style-type: none"> ▪ [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'. ▪ [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. <p>Note: This option is applicable only to the E10 variant.</p> <ul style="list-style-type: none"> ▪ [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. <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.

Parameter	Description
[PSTNExtendedParams]	<p>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>Note: If you want to use both the above options, then set this parameter to 3.</p>

12.12.7 ISDN and CAS Interworking Parameters

The ISDN and CAS interworking parameters are described in the table below.

Table 12-55: 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. ▪ [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	Minimum number of overlap digits to collect (for ISDN overlap dialing) before sending the first SIP message for routing Tel-to-

Parameter	Description
[MinOverlapDigitsForRouting]	<p>IP calls. The valid value range is 0 to 49. The default is 1.</p> <p>Note: This parameter is applicable when the ISDNRxOverlap parameter is set to [2].</p>
Web/EMS: ISDN Overlap IP to Tel Dialing [ISDNTxOverlap]	<p>Enables ISDN overlap dialing for IP-to-Tel calls. This feature is part of ISDN-to-SIP overlap dialing according to RFC 3578.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>When enabled, for each received INVITE of the same dialog session, the device sends an ISDN Setup (and subsequent ISDN Info Q.931 messages) with the collected digits to the Tel side. For all subsequent INVITEs received, the device sends a SIP 484 Address Incomplete response in order to maintain the current dialog session and receive additional digits from subsequent INVITEs.</p> <p>Note: When IP-to-Tel overlap dialing is enabled, to send ISDN Setup messages without the Sending Complete IE, the ISDNOutgoingCallsBehavior parameter must be set to USER SENDING COMPLETE (2).</p>
Web: Enable Receiving of Overlap Dialing [ISDNRxOverlap_x]	<p>Determines the receiving (Rx) type of ISDN overlap dialing for Tel-to-IP calls.</p> <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 SIP message for routing the call, using the MinOverlapDigitsForRouting parameter. ▪ 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

Parameter	Description
	<p>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.</p> <ul style="list-style-type: none"> For enabling ISDN overlap dialing for IP-to-Tel calls, use the ISDNTxOverlap parameter. For detailed information on ISDN overlap dialing, see "ISDN Overlap Dialing" on page 642.
[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>Notes:</p> <ul style="list-style-type: none"> When enabled and at least one digit is received from the ISDN (Setup message), the device stops playing a dial tone. This parameter is applicable only to ISDN Overlap mode when dialed numbers are sent using Q.931 Info messages.
[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 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>

Parameter	Description
	<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.
Web/EMS: Enable ISDN Tunneling IP to Tel [EnableISDNTunnelingIP2Tel]	<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 (<code>X-ISDNTunnelingInfo</code>) or a dedicated message body (<code>application/isdn</code>) in the SIP messages and sends the data as ISDN messages to the PSTN side.</p>
Web/EMS: Enable QSIG Tunneling [EnableQSIGTunneling]	<p>Enables QSIG tunneling-over-SIP according to the IETF Internet-Draft <code>draft-elwell-sipping-qsig-tunnel-03</code> and ECMA-355 and ETSI TS 102 345 standards.</p> <ul style="list-style-type: none"> [0] Disable = Disable (default). [1] Enable = Enable QSIG tunneling from QSIG to SIP and vice versa. <p>When QSIG tunneling is enabled, all QSIG messages are sent as raw data in corresponding SIP messages using a dedicated message body.</p> <p>Notes:</p> <ul style="list-style-type: none"> 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 also to all ISDN variants (in addition to the QSIG protocol). For a detailed description on QSIG tunneling, see "QSIG Tunneling" on page 650.
[QSIGTunnelingMode]	<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>
Web: Enable Hold to ISDN EMS: Enable Hold 2 ISDN [EnableHold2ISDN]	<p>Enables SIP-to-ISDN interworking of the Hold/Retrieve supplementary service.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable

Parameter	Description
	<p>Notes:</p> <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]	<p>Controls the activation/deactivation of delivering raw Q.931 messages.</p> <ul style="list-style-type: none"> ▪ [0] = ISDN messages aren't duplicated (default). ▪ [128] = All ISDN messages are duplicated. <p>Note: For this parameter to take effect, a device reset is required.</p>
Web/EMS: ISDN SubAddress Format [ISDNSubAddressFormat]	<p>Determines the encoding format of the SIP Tel URI parameter 'isub', which carries the encoding type of ISDN subaddresses. This is used to identify different remote ISDN entities under the same phone number (ISDN Calling and Called numbers) for interworking between ISDN and SIP networks.</p> <ul style="list-style-type: none"> ▪ [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 <p>For IP-to-Tel calls, if the incoming SIP INVITE message includes subaddress values in the 'isub' parameter for the Called Number (in the Request-URI) and/or the Calling Number (in the From header), these values are mapped to the outgoing ISDN Setup message.</p> <p>If the incoming ISDN Setup message includes 'subaddress' values for the Called Number and/or the Calling Number, these values are mapped to the outgoing SIP INVITE message's 'isub' parameter in accordance with RFC 4715.</p>
[IgnoreISDNSubaddress]	<p>Determines whether the device ignores the Subaddress from the incoming ISDN Called and Calling numbers when sending to IP.</p> <ul style="list-style-type: none"> ▪ [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>Specifies 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)]

Parameter	Description
	<p>before it reaches the Connect state; otherwise, the Disconnect message is sent immediately and no tones are played.</p>
<p>Web: Play Ringback Tone to Trunk [PlayRBTone2Trunk_ID]</p>	<p>Enables 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). Note: Receipt of a 183 response does not cause the device configured with CAS to play an RBT (unless SIP183Behaviour is set to 1). The device configured with ISDN protocol type operates according to the parameter LocalISDNRBSrcSource: <ul style="list-style-type: none"> ✓ If the device receives a 180 Ringing response (with or without SDP) and the parameter LocalISDNRBSrcSource 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 LocalISDNRBSrcSource 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. 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. ▪ [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 LocalISDNRBSrcSource: <ul style="list-style-type: none"> ✓ If LocalISDNRBSrcSource 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 LocalISDNRBSrcSource is set to 0, the device doesn't

Parameter	Description
	<p>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 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 LocalISDNRBSrc is set to 1.</p>
Web: Digital Out-Of-Service Behavior EMS: Digital OOS Behavior For Trunk Value [DigitalOOSBehaviorForTrunk_ID]	<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.

Parameter	Description
Web: Digital Out-Of-Service Behavior [DigitalOOSBehavior]	Determines the method for setting digital trunks to Out-Of-Service state per device. For a description, refer to the parameter DigitalOOSBehaviorForTrunk_ID. Note: To configure the method for setting Out-Of-Service state per trunk, use the parameter DigitalOOSBehaviorForTrunk_ID.
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).
Web: Release Cause Mapping Table EMS: ISDN to SIP Cause Mapping	
[CauseMapISDN2SIP]	<p>This <i>ini</i> file table parameter maps ISDN Q.850 Release Causes to SIP responses.</p> <p>The format of this parameter is as follows:</p> <pre>[CauseMapISDN2SIP] FORMAT CauseMapISDN2SIP_Index = CauseMapISDN2SIP_IsdnReleaseCause, CauseMapISDN2SIP_SipResponse; [CauseMapISDN2SIP]</pre> <p>Where,</p> <ul style="list-style-type: none"> IsdnReleaseCause = Q.850 Release Cause SipResponse = SIP Response <p>For example: CauseMapISDN2SIP 0 = 50,480; CauseMapISDN2SIP 0 = 6,406;</p> <p>When a Release Cause is received (from the PSTN side), the device searches this mapping table for a match. If the Q.850 Release Cause is found, the SIP response assigned to it is sent to the IP side. If no match is found, the default static mapping is used.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter can appear up to 12 times. For an explanation on <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Release Cause Mapping Table EMS: SIP to ISDN Cause Mapping	
[CauseMapSIP2ISDN]	<p>This <i>ini</i> file table parameter maps SIP responses to Q.850 Release Causes. The format of this parameter is as follows:</p> <pre>[CauseMapSIP2ISDN] FORMAT CauseMapSIP2ISDN_Index = CauseMapSIP2ISDN_SipResponse, CauseMapSIP2ISDN_IsdnReleaseCause; [CauseMapSIP2ISDN]</pre> <p>Where,</p>

Parameter	Description
	<ul style="list-style-type: none"> SipResponse = SIP Response IsdnReleaseCause = Q.850 Release Cause <p>For example: CauseMapSIP2ISDN 0 = 480,50; CauseMapSIP2ISDN 0 = 404,3; When a SIP response is received (from the IP side), the device searches this mapping table for a match. If the SIP response is found, the Q.850 Release Cause assigned to it is sent to the PSTN. If no match is found, the default static mapping is used.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter can appear up to 12 times. For an explanation on <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
[UserToUserHeaderFormat]	<p>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.</p> <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]	<p>Determines (for IP-to-Tel calls) whether the Calling Number and Calling Name IEs are removed from the ISDN Setup message if the presentation is set to Restricted.</p> <ul style="list-style-type: none"> [0] No = IE's are not removed (default). [1] Yes = IE's are removed.
Web/EMS: Remove Calling Name [RemoveCallingName]	<p>Enables the device to remove the Calling Name from SIP-to-ISDN calls for all trunks.</p> <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_ID]	<p>Enables the device to remove the Calling Name per trunk (where ID denotes the trunk number) for SIP-to-ISDN calls.</p> <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]	<p>Progress Indicator (PI) to ISDN. The ID in the <i>ini</i> file parameter depicts the trunk number, where 0 is the first trunk.</p> <ul style="list-style-type: none"> [-1] Not Configured = The PI in ISDN messages is set

Parameter	Description
	<p>according to the parameter PlayRBTone2Tel (default).</p> <ul style="list-style-type: none"> ▪ [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]	<p>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.</p> <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]	<p>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.</p> <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]	<p>Determines whether the Ringback tone is played to the ISDN by the PBX/PSTN or by the device.</p> <ul style="list-style-type: none"> ▪ [0] PBX = PBX/PSTN (default). ▪ [1] Gateway = device plays the Ringback tone. <p>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.</p>
Web: PSTN Alert Timeout EMS: Trunk PSTN Alert Timeout [PSTNAlertTimeout]	<p>For digital interfaces: Alert Timeout (in seconds) (ISDN T301 timer) for calls to 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.</p> <p>For analog interfaces: Alert Timeout (in seconds) for calls to the Tel side. This timer is used between the time ring is generated (FXS) or line is seized (FXO) until the call is connected. The range is 1 to 600. The default is 180 seconds.</p> <p>Note: If per trunk configuration (using TrunkPSTNAlertTimeout) is set to other than default, the PSTNAlertTimeout parameter value is overridden.</p>
Web/EMS: PSTN Alert Timeout	<p>Alert Timeout (ISDN T301 timer) in seconds for outgoing calls to PSTN. This timer is used between the time that an ISDN</p>

Parameter	Description
[TrunkPSTNAlertTimeout_ID]	<p>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.</p> <p>In the <i>ini</i> file parameter, <i>ID</i> depicts the trunk number, where 0 is the first trunk.</p> <p>The range is 1 to 600. The default is 180.</p>
Web: B-Channel Negotiation EMS: B-Channel Negotiation For Trunk Mode [BChannelNegotiationForTrunk_ID]	<p>Determines the ISDN B-channel negotiation mode.</p> <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. <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 <i>ID</i> in the <i>ini</i> file parameter name represents the trunk number, where 0 is the first trunk.
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 <i>ini</i> file parameter) a rule to route the redirected call (using the user part from the 302 Contact header) to the same Trunk Group from where the incoming Tel-to-IP call was received.</p>
EMS: Enable CIC [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

Parameter	Description
	<p>Selection (TNS) IE.</p> <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-Tel calls.
EMS: Enable AOC [EnableAOC]	<p>Determines whether ISDN Advice of Charge (AOC) messages are interworked to SIP.</p> <ul style="list-style-type: none"> [0] = Not used (default). [1] = AOC messages are interworked to SIP. <p>The device supports the receipt of ISDN (Euro ISDN) AOC messages. 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.</p>
Web: IPMedia Detectors EMS: DSP Detectors Enable [EnableDSPIPMDetectors]	<p>Enables or disables the device's DSP detectors.</p> <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. 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]	<p>Adds an optional Information Element (IE) data (in hex format) to ISDN Setup messages. For example, to add IE '0x20,0x02,0x00,0xe1', enter the value "200200e1".</p> <p>Notes:</p> <ul style="list-style-type: none"> This IE is sent from the Hunt Group IDs that are defined by the parameter SendIEonTG. You can configure different IE data for Hunt 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]	<p>Defines Hunt Group IDs (up to 50 characters) from where the optional ISDN IE (defined by the parameter AddIEinSetup) is sent. For example: '1,2,4,10,12,6'.</p> <p>Notes:</p> <ul style="list-style-type: none"> You can configure different IE data for Hunt Groups by defining this parameter for different IP Profile IDs (using the parameter IPProfile), and then assigning the required IP

Parameter	Description
	<p>Profile ID in the 'Inbound IP Routing Table' (PSTNPrefix).</p> <ul style="list-style-type: none"> When IP Profiles are used for configuring different IE data for Hunt Groups, this parameter is ignored.
<p>Web: Enable User-to-User IE for Tel to IP EMS: Enable UUI Tel 2 Ip [EnableUUITel2IP]</p>	<p>Enables ISDN PRI-to-SIP interworking.</p> <ul style="list-style-type: none"> [0] Disable = Disabled (default). [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. 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>
<p>Web: Enable User-to-User IE for IP to Tel EMS: Enable UUI Ip 2 Tel [EnableUUIIP2Tel]</p>	<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). The valid range is 0 to 600. The default value is 0 (i.e., disabled).</p>

Parameter	Description												
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"> <thead> <tr> <th>PSTN Protocol</th><th>Transfer Method (Described Below)</th></tr> </thead> <tbody> <tr> <td>E1 Euro ISDN [1]</td><td>ECT [2] or InBand [5]</td></tr> <tr> <td>E1 QSIG [21], T1 QSIG [23]</td><td>Single Step Transfer [4], Path Replacement Transfer [2], or InBand [5]</td></tr> <tr> <td>T1 NI2 ISDN [10], T1 4ESS ISDN [11], T1 5ESS 9 ISDN [12]</td><td>TBCT [2] or InBand [5]</td></tr> <tr> <td>T1 DMS100 ISDN [14]</td><td>RTL [2] or InBand [5]</td></tr> <tr> <td>T1 RAW CAS [3], T1 CAS [2], E1 CAS [8], E1 RAW CAS [9]</td><td>[1] CAS NFA DMS-100 or [3] CAS Normal transfer</td></tr> </tbody> </table> <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 SendISDNTransferOnConnect must be set to 1. ✓ The parameter SendISDNTransferOnConnect 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 (SendISDNTransferOnConnect is set to 1). ✓ This transfer can be performed between B-channels from different trunks or Hunt Groups, by using the parameter EnableTransferAcrossTrunkGroups. ✓ The device initiates the ECT process after receiving a SIP REFER message only for trunks that are configured to User side. 	PSTN Protocol	Transfer Method (Described Below)	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 DMS100 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
PSTN Protocol	Transfer Method (Described Below)												
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 DMS100 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												

Parameter	Description
	<ul style="list-style-type: none"> [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 device performs a transfer by sending a Facility message to the PBX, initiating Single Step transfer. Once a success return result is received, the transfer is completed. Tel-to-IP: When a Facility message initiating Single Step transfer is received from the PBX, a SIP REFER message is sent to the IP side. [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. If the hostpart of the Refer-To sip:URI contains the device's IP address, and if the Hunt Group selected according to the IP to Tel Routing table is the same Hunt Group as the original call, then the device performs the in-band DTMF transfer; otherwise, the device sends the INVITE according to regular transfer rules. After completing the in-band transfer, the device waits for the ISDN Disconnect message. If the Disconnect message is received during the first 5 seconds, the device sends a SIP NOTIFY with 200 OK message; otherwise, the device sends a NOTIFY with 4xx message. <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]	Determines whether the device allows ISDN ECT, RLT or TBCT IP-to-Tel call transfers between B-channels of different Hunt Groups. <ul style="list-style-type: none"> [0] = Disable - ISDN call transfer is only between B-channels of the same Hunt Group (default). [1] = Enable - the device performs ISDN transfer between any two PSTN calls (between any Hunt Group) handled by the device. <p>Note: The ISDN transfer also requires that you configure the parameter TrunkTransferMode_x to 2.</p>

Parameter	Description
Web: ISDN Transfer Capabilities EMS: Transfer Capability To ISDN [ISDNTransferCapability_ID]	<p>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.</p> <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]	<p>This parameter is used for the ECT/TBCT/RLT/Path Replacement ISDN transfer methods. Usually, the device requests the PBX to connect an incoming and outgoing call. This parameter determines if the outgoing call (from the device to the PBX) must be connected before the transfer is initiated.</p> <ul style="list-style-type: none"> ▪ [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 (TrunkTransferMode = 2 and ProtocolType = 14 DMS-100), this parameter must be set to 1.</p>
[ISDNTransferCompleteTimeout]	<p>The timeout (in seconds) for determining ISDN call transfer (ECT, RLT, or TBCT) failure. If the device does not receive any response to an ISDN transfer attempt within this user-defined time, the device identifies this as an ISDN transfer failure and subsequently performs a hairpin TDM connection or sends a SIP NOTIFY message with a SIP 603 response (depending whether hairpin is enabled or disabled, using the parameter DisableFallbackTransferToTDM).</p> <p>The valid range is 1 to 10. The default is 4.</p>
Web/EMS: Enable Network ISDN Transfer [EnableNetworkISDNTransfer]	<p>Determines whether the device allows interworking of network-side received ECT/TBCT Facility messages (ETSI ECT - Explicit Call Transfer) to SIP REFER.</p> <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 Facility messages are received from the ISDN side (e.g., from a PBX).
[DisableFallbackTransferToTDM]	<p>Enables or disables "hairpin" TDM transfer upon ISDN (ECT, RLT, or TBCT) call transfer failure. When this feature is enabled and an ISDN call transfer failure occurs, the device sends a SIP NOTIFY message with a SIP 603 Decline response.</p> <ul style="list-style-type: none"> ▪ [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> 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>

12.12.8 Answer and Disconnect Supervision Parameters

The answer and disconnect supervision parameters are described in the table below.

Table 12-56: Answer and Disconnect Parameters

Parameter	Description
Web: Answer Supervision EMS: Enable Voice Detection [EnableVoiceDetection]	<p>Enables the sending of SIP 200 OK upon detection of speech, fax, or modem.</p> <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). <p>Typically, this feature is used only when early media (enabled using the EnableEarlyMedia parameter) is used to establish the voice path before the call is answered.</p> <p>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 EnableDSIPMDetectors parameter to 1. Digital interfaces: This feature is applicable only when the protocol type is CAS.
Web/EMS: Max Call Duration (min) [MaxCallDuration]	<p>Defines the maximum call duration (in minutes). If this time expires, both sides of the call are released (IP and Tel). The valid range is 0 to 35,791. The default is 0 (i.e., no limitation).</p>
Web/EMS: Disconnect on Dial Tone [DisconnectOnDialTone]	<p>Determines whether the device disconnects a call when a dial tone is detected from the PBX.</p> <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]	<p>Defines a digit pattern to send to the Tel side after a SIP 200 OK is received from the IP side. The digit pattern is a user-defined DTMF sequence that is used to indicate an answer signal (e.g., for billing). The valid range is 1 to 8 characters.</p> <p>Note: This parameter is applicable to FXO/CAS.</p>
Web: Disconnect on Broken Connection EMS: Disconnect Calls on Broken Connection	<p>Determines whether the device releases the call if RTP packets are not received within a user-defined timeout.</p> <ul style="list-style-type: none"> [0] No

Parameter	Description
[DisconnectOnBrokenConnection]	<ul style="list-style-type: none"> [1] Yes (default) <p>Notes:</p> <ul style="list-style-type: none"> The timeout is configured by the BrokenConnectionEventTimeout parameter. This feature is applicable only if the RTP session is used without Silence Compression. If Silence Compression is enabled, the device doesn't detect a broken RTP connection. During a call, if the source IP address (from where the RTP packets are received) is changed without notifying the device, the device filters these RTP packets. To overcome this, set the DisconnectOnBrokenConnection parameter to 0; the device doesn't detect RTP packets arriving from the original source IP address and switches (after 300 msec) to the RTP packets arriving from the new source IP address. This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).
Web: Broken Connection Timeout EMS: Broken Connection Event Timeout [BrokenConnectionEventTimeout]	<p>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).</p> <p>Notes:</p> <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]	<p>Determines whether calls are disconnected after detection of silence.</p> <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). <p>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.</p>
Web: Silence Detection Period [sec] EMS: Silence Detection Time Out [FarEndDisconnectSilencePeriod]	<p>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.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: Silence Detection Method [FarEndDisconnectSilenceMethod]	<p>Silence detection method.</p> <ul style="list-style-type: none"> [0] None = Silence detection option is disabled. [1] Packets Count = According to packet count.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [2] Voice/Energy Detectors = N/A. ▪ [3] All = N/A. <p>Note: For this parameter to take effect, a device reset is required.</p>
[FarEndDisconnectSilenceThresh old]	<p>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%.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only if silence is detected according to packet count (FarEndDisconnectSilenceMethod is set to 1). ▪ For this parameter to take effect, a device reset is required.
[BrokenConnectionDuringSilence]	<p>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.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable.
Web: Disconnect Call on Busy Tone Detection (ISDN) EMS: Isdn Disconnect On Busy Tone [ISDNDisconnectOnBusyTone]	<p>Determines whether a call is disconnected upon detection of a busy tone (for ISDN).</p> <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). <p>Notes:</p> <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 EMS: Disconnect On Detection End Tones [DisconnectOnBusyTone]	<p>Determines whether a call is disconnected upon detection of a busy tone (for CAS).</p> <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). <p>Notes:</p> <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.

Parameter	Description
Polarity (Current) Reversal for Call Release (Analog Interfaces) Parameters	
Web: Enable Polarity Reversal EMS: Enable Reversal Polarity [EnableReversalPolarity]	<p>Enables the polarity reversal feature for call release.</p> <ul style="list-style-type: none"> [0] Disable = Disable the polarity reversal service (default). [1] Enable = Enable the polarity reversal service. <p>If the polarity reversal service is enabled, the FXS interface changes the line polarity on call answer and then changes it back on call release.</p> <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>
Web/EMS: Enable Current Disconnect [EnableCurrentDisconnect]	<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>
EMS: Polarity Reversal Type [PolarityReversalType]	<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.

Parameter	Description
EMS: Current Disconnect Duration [CurrentDisconnectDuration]	<p>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.
[CurrentDisconnectDefaultThreshold]	<p>Determines the line voltage threshold at which a current disconnect detection is considered. The valid range is 0 to 20 Volts. The default value is 4 Volts.</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.
[TimeToSampleAnalogLineVoltage]	<p>Determines the frequency at which the analog line voltage is sampled (after offhook), for detection of the current disconnect threshold. The valid range is 100 to 2500 msec. The default value is 1000 msec.</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.

12.12.9 Tone Parameters

This subsection describes the device's tone parameters.

12.12.9.1 Telephony Tone Parameters

The telephony tone parameters are described in the table below.

Table 12-57: Tone Parameters

Parameter	Description
[PlayHeldToneForIP2IP]	<p>Enables playing a Held tone to an IP-to-IP leg instead of putting it on hold.</p> <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. <p>Note: This parameter is applicable only to the IP-to-IP application (enables using the parameter EnableIP2IPApplication).</p>
Web/EMS: Dial Tone Duration	Duration (in seconds) that the dial tone is played (for digital

Parameter	Description
[sec] [TimeForDialTone]	<p>interfaces, to an ISDN terminal).</p> <p>For digital interfaces: This parameter is applicable for overlap dialing when ISDNInCallsBehavior is set to 65536. The dial tone is played if the ISDN Setup message doesn't include the called number.</p> <p>The valid range is 0 to 60. The default is 5.</p> <p>For analog interfaces: FXS interfaces play the dial tone after the phone is picked up (off-hook). FXO interfaces play the dial tone after the port is seized in response to ringing (from PBX/PSTN). The valid range is 0 to 60. The default time is 16.</p> <p>Notes for analog interfaces:</p> <ul style="list-style-type: none"> 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]	<p>Duration (in msec) of the Confirmation tone. A Stutter tone is played (instead of a regular dial tone) when a Message Waiting Indication (MWI) is received. The Stutter tone is composed of a Confirmation tone (Tone Type #8), which is played for the defined duration (StutterToneDuration) followed by a Stutter Dial tone (Tone Type #15). Both these tones are defined in the CPT file. The range is 1,000 to 60,000. The default is 2,000 (i.e., 2 seconds).</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 detailed information on MWI, see Message Waiting Indication on page 461.
Web: FXO AutoDial Play BusyTone EMS: Auto Dial Play Busy Tone [FXOAutoDialPlayBusyTone]	<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>
Web: Hotline Dial Tone Duration EMS: Hot Line Tone Duration [HotLineToneDuration]	<p>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 184).</p> <p>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.

Parameter	Description
Web/EMS: Reorder Tone Duration [sec] [TimeForReorderTone]	<p>For Analog: 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: 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).
Web: Time Before Reorder Tone [sec] EMS: Time For Reorder Tone [TimeBeforeReorderTone]	<p>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>
Web: Cut Through Reorder Tone Duration [sec] [CutThroughTimeForReOrderTone]	<p>Defines the duration (in seconds) of the Reorder tone played to the PSTN side after the IP call party releases the call, for the Cut-Through feature. After the tone stops playing, an incoming call is immediately answered if the FXS is off-hooked (for analog interfaces) or the PSTN is connected (for digital interfaces).</p> <p>The valid values are 0 to 30. The default is 0 (i.e., no Reorder tone is played).</p> <p>Note: To enable the Cut-Through feature, use the DigitalCutThrough (for CAS channels) or CutThrough (for FXS channels) parameters.</p>
Web/EMS: Enable Comfort Tone [EnableComfortTone]	<p>Determines whether the device plays a Comfort Tone (Tone Type #18) to the FXS/FXO endpoint after a SIP INVITE is sent and before a SIP 18x response is received.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note: This parameter is applicable to FXS and FXO interfaces.</p>
[WarningToneDuration]	<p>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.</p> <p>Notes:</p> <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]	<p>Enables the play of the ringback tone (RBT) to the Tel side and determines the method for playing the RBT.</p> <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

Parameter	Description
	<p>when a SIP 180/183 response is received.</p> <ul style="list-style-type: none"> ▪ [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. <p>Note: For ISDN trunks, this option is applicable only if the parameter LocalISDNRBSrc is set to 1.</p>
Web: Play Ringback Tone to IP EMS: Play Ring Back Tone To IP [PlayRBTone2IP]	<p>Determines whether or not the device plays a ringback tone (RBT) to the IP side for IP-to-Tel calls.</p> <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. <p>For digital modules: If configured to 1 ('Play') and EnableEarlyMedia is set to 1, the device plays a ringback tone according to the following:</p> <ul style="list-style-type: none"> ▪ 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 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>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 143).
Web: Play Local RBT on ISDN Transfer EMS: Play RBT On ISDN Transfer [PlayRBTOnISDNTransfer]	<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).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [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.
Web: MFC R2 Category EMS: R2 Category [R2Category]	Determines 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.
Tone Index Table	
[ToneIndex]	<p>This ini file table parameter configures the Tone Index table, which allows you to define Distinctive Ringing and Call Waiting tones per FXS endpoint (or for a range of FXS endpoints). This is based on calling number (source number prefix) and/or called (destination number/prefix) for IP-to-Tel calls. This allows different tones to be played for an FXS endpoint depending on the source or destination number of the IP-to-Tel call.</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. ▪ 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.</p>

Parameter	Description
	<p>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.

12.12.9.2 Tone Detection Parameters

The signal tone detection parameters are described in the table below.

Table 12-58: Tone Detection Parameters

Parameter	Description
EMS: DTMF Enable [DTMFDetectorEnable]	<p>Enables or disables the detection of DTMF signaling.</p> <ul style="list-style-type: none"> [0] = Disable [1] = Enable (default)
EMS: MF R1 Enable [MFR1DetectorEnable]	<p>Enables or disables the detection of MF-R1 signaling.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable
EMS: R1.5 Detection Standard [R1DetectionStandard]	<p>Determines the MF-R1 protocol used for detection.</p> <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 [UserDefinedToneDetectorEnable]	<p>Enables or disables the detection of User Defined Tones signaling, applicable for Special Information Tone (SIT) detection.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable
EMS: SIT Enable [SITDetectorEnable]	<p>Enables or disables 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

Parameter	Description
	<ul style="list-style-type: none"> 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. 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. 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>

12.12.9.3 Metering Tone Parameters

The metering tone parameters are described in the table below.

Table 12-59: 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 internal table configured by the parameter ChargeCode. Notes: <ul style="list-style-type: none"> This parameter is applicable only to FXS interfaces. If you select 'Internal Table', you must configure the 'Charge Codes Table' (see "Configuring Charge Codes Table" on page 181).
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.
Web: Charge Codes Table EMS: Charge Codes	
[ChargeCode]	This <i>ini</i> file table parameter configures metering tones (and their time intervals) that the device's FXS interface generates to the Tel side. The format of this parameter is as follows: [ChargeCode] FORMAT ChargeCode_Index = ChargeCode_EndTime1, ChargeCode_PulseInterval1, ChargeCode_PulsesOnAnswer1, ChargeCode_EndTime2, ChargeCode_PulseInterval2, ChargeCode_PulsesOnAnswer2, ChargeCode_EndTime3, ChargeCode_PulseInterval3, ChargeCode_PulsesOnAnswer3, ChargeCode_EndTime4, ChargeCode_PulseInterval4, ChargeCode_PulsesOnAnswer4; [ChargeCode] Where, <ul style="list-style-type: none"> EndTime = Period (1 - 4) end time.

Parameter	Description
	<ul style="list-style-type: none"> ▪ PulseInterval = Period (1 - 4) pulse interval. ▪ PulsesOnAnswer = Period (1 - 4) pulses on answer. <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). ▪ This parameter is applicable only to FXS interfaces. ▪ 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 181. ▪ For an explanation on configuration using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.12.10 Telephone Keypad Sequence Parameters

The telephony keypad sequence parameters are described in the table below.

Table 12-60: 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</p>

Parameter	Description
	<p>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>
Hook Flash Parameters	
Web: Flash Keys Sequence Style [FlashKeysSequenceStyle]	<p>Hook flash keys sequence style for FXS interfaces.</p> <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). Note that the settings of the ConferenceCode parameter are ignored. ✓ Flash + 4: makes a call transfer.
Web: Flash Keys Sequence Timeout [FlashKeysSequenceTimeout]	<p>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.</p>
Keypad Feature - Call Forward Parameters	
Web: Unconditional EMS: Call Forward Unconditional [KeyCFUnCond]	<p>Keypad sequence that activates the immediate call forward option.</p>
Web: No Answer EMS: Call Forward No Answer [KeyCFNoAnswer]	<p>Keypad sequence that activates the forward on no answer option.</p>
Web: On Busy EMS: Call Forward Busy [KeyCFBusy]	<p>Keypad sequence that activates the forward on busy option.</p>

Parameter	Description
Web: On Busy or No Answer EMS: CF Busy Or No Answer [KeyCFBusyOrNoAnswer]	Keypad sequence that activates the forward on 'busy or no answer' option.
Web: Do Not Disturb EMS: CF Do Not Disturb [KeyCFDoNotDisturb]	Keypad sequence that activates the Do Not Disturb option (immediately reject incoming calls).
<p>To activate the required forward method from the telephone:</p> <ol style="list-style-type: none"> 1 Dial the user-defined sequence number on the keypad; a dial tone is heard. 2 Dial the telephone number to which the call is forwarded (terminate the number with #); a confirmation tone is heard. 	
Web: Deactivate EMS: Call Forward Deactivation [KeyCFDeact]	Keypad sequence that deactivates any of the call forward options. After the sequence is pressed, a confirmation tone is heard.
Keypad Feature - Caller ID Restriction Parameters	
Web: Activate EMS: CLIR [KeyCLIR]	Keypad sequence that activates the restricted Caller ID option. After the sequence is pressed, a confirmation tone is heard.
Web: Deactivate EMS: CLIR Deactivation [KeyCLIRDeact]	Keypad sequence that deactivates the restricted Caller ID option. After the sequence is pressed, a confirmation tone is heard.
Keypad Feature - Hotline Parameters	
Web: Activate EMS: Hot Line [KeyHotLine]	<p>Keypad sequence that activates the delayed hotline option. To activate the delayed hotline option from the telephone, perform the following:</p> <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]	Keypad sequence that deactivates the delayed hotline option. After the sequence is pressed, a confirmation tone is heard.
Keypad Feature - Transfer Parameters	
Web: Blind EMS: Blind Transfer [KeyBlindTransfer]	<p>Keypad sequence that activates blind transfer for Tel-to-IP calls. There are two possible scenarios:</p> <ul style="list-style-type: none"> ▪ Option 1: After this sequence is dialed, the current call is put on hold (using Re-INVITE), a dial tone is played to the phone and then phone number collection starts. ▪ Option 2: A Hook-Flash is pressed, the current call is put on hold, a dial tone is played to the phone, and then digit collection starts. After this sequence is identified, the device continues the collection of the destination phone number. <p>For both options, after the phone number is collected, it's sent to the transferee in a SIP REFER request (without a Replaces header). The call is then terminated and a confirmation tone is played to the phone. If the phone number collection fails due to</p>

Parameter	Description
	<p>a mismatch, a reorder tone is played to the phone.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable to FXO and FXS interfaces (but for FXO the Web interface does not display this parameter). It is possible to configure whether the KeyBlindTransfer code is added as a prefix to the dialed destination number, by using the parameter KeyBlindTransferAddPrefix.
Keypad Feature - Call Waiting Parameters	
Web: Activate EMS: Keypad Features CW [KeyCallWaiting]	Keypad sequence that activates the Call Waiting option. After the sequence is pressed, a confirmation tone is heard.
Web: Deactivate EMS: Keypad Features CW Deact [KeyCallWaitingDeact]	Keypad sequence that deactivates the Call Waiting option. After the sequence is pressed, a confirmation tone is heard.
Keypad Feature - Reject Anonymous Call Parameters	
Web: Activate EMS: Reject Anonymous Call [KeyRejectAnonymousCall]	Keypad sequence that activates the reject anonymous call option, whereby the device rejects incoming anonymous calls. After the sequence is pressed, a confirmation tone is heard.
Web: Deactivate EMS: Reject Anonymous Call Deact [KeyRejectAnonymousCallDeact]	Keypad sequence that de-activates the reject anonymous call option. After the sequence is pressed, a confirmation tone is heard.
[RejectAnonymousCallPerPort]	<p>This <i>ini</i> file table parameter determines whether the device rejects incoming anonymous calls on FXS interfaces. The format of this parameter is as follows:</p> <pre>[RejectAnonymousCallPerPort] FORMAT RejectAnonymousCallPerPort_Index = RejectAnonymousCallPerPort_Enable, RejectAnonymousCallPerPort_Port, RejectAnonymousCallPerPort_Module; [RejectAnonymousCallPerPort]</pre> <p>Where,</p> <ul style="list-style-type: none"> Enable = accept [0] (default) or reject [1] incoming anonymous calls. Port = Port number. Module = Module number. <p>For example: RejectAnonymousCallPerPort 0 = 0,1,1; RejectAnonymousCallPerPort 1 = 1,2,1;</p> <p>If enabled, when a device's FXS interface receives an anonymous call, it responds with a 433 (Anonymity Disallowed) SIP response.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only to FXS interfaces. This parameter is per FXS port. For an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.12.11 General FXO Parameters

The general FXO parameters are described in the table below.

Table 12-61: General FXO Parameters

Parameter	Description
Web: FXO Coefficient Type EMS: Country Coefficients [CountryCoefficients]	<p>Determines the FXO line characteristics (AC and DC) according to USA or TBR21 standard.</p> <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>
[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>

Parameter	Description
	<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.
Web: Time to Wait before Dialing [msec] EMS: Time Before Dial [WaitForDialTime]	<p>For digital interfaces: Determines 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: Determines 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).

Parameter	Description
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.

12.12.12 FXS Parameters

The general FXS parameters are described in the table below.

Table 12-62: General FXS Parameters

Parameter	Description
Web: FXS Coefficient Type EMS: Country Coefficients [FXSCountryCoefficients]	<p>Determines the FXS line characteristics (AC and DC) according to USA or Europe (TBR21) standards.</p> <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>

12.12.13 Hunt Groups, Number Manipulation and Routing Parameters

This subsection describes the device's number manipulation and routing parameters.

12.12.13.1 Hunt Groups and Routing Parameters

The routing parameters are described in the table below.

Table 12-63: Routing Parameters

Parameter	Description
Web: Hunt Group Table EMS: SIP Endpoints > Phones	
[TrunkGroup]	<p>This <i>ini</i> file table parameter is used to define and activate the device's endpointsTrunk channels, by defining telephone numbers and assigning them to Hunt 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 BRI channels 1 through 4 of Module 2 to Hunt Group ID 2 with phone numbers 208 to 211:</p> <pre>TrunkGroup 1 = 2, 0, 1, 4, 208, 0, 0 ,2;</pre> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The first entry in this table starts at index 0. ▪ Hunt Group ID 1 is depicted as 0 in the table. ▪ This parameter can appear up to four times per module. ▪ For configuring this table in the Web interface, see Configuring Hunt Group Table on page 146. ▪ For a description of <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Hunt Group Settings EMS: SIP Routing > Hunt Group	
[TrunkGroupSettings]	<p>This <i>ini</i> file table parameter defines rules for channel allocation per Hunt Group. If no rule exists, the rule defined by the global parameter ChannelSelectMode takes effect. The format of this parameter is as follows:</p> <pre>[TrunkGroupSettings] FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId, TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode, TrunkGroupSettings_GatewayName,TrunkGroupSettings_ContactUser, TrunkGroupSettings_ServingIPGroup, TrunkGroupSettings_MWIInterrogationType; [TrunkGroupSettings]</pre>

Parameter	Description
	<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 24 indices. ▪ The parameter MWIInterrogationType is not applicable. ▪ For configuring Hunt Group Settings using the Web interface, see "Configuring Hunt Group Settings" on page 148. ▪ For a description on using <i>ini</i> file table parameters, see to "Configuring ini File Table Parameters" on page 368.
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 device's channel according to the called number (default.) ▪ [1] Cyclic Ascending = Selects the next available channel in an ascending cyclic order. Always selects the next higher channel number in the Hunt Group. When the device reaches the highest channel number in the Hunt Group, it selects the lowest channel number in the Hunt Group and then starts ascending again. ▪ [2] Ascending = Selects the lowest available channel. It always starts at the lowest channel number in the Hunt Group and if that channel is unavailable, selects the next higher channel. ▪ [3] Cyclic Descending = Selects the next available channel in descending cyclic order. It always selects the next lower channel number in the Hunt Group. When the device reaches the lowest channel number in the Hunt Group, it selects the highest channel number in the Hunt Group and then starts descending again. ▪ [4] Descending = Selects the highest available channel. It always starts at the highest channel number in the Hunt Group and if that channel is unavailable, selects the next lower channel. ▪ [5] Dest Number + Cyclic Ascending = The device first selects the channel according to the called number. If the called number isn't found, it then selects the next available channel in ascending cyclic order. Note that if the called number is found but the port associated with this number is busy, the call is released. ▪ [6] By Source Phone Number = The device selects the channel according to the calling number. ▪ [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 Hunt Group) and then selects the B-channel of this trunk according to the

Parameter	Description
	<p>cyclic ascending method (i.e., selects the channel after the last allocated channel). This option is applicable only to digital interfaces.</p> <p>For example, if the Hunt 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 an IP-to-Tel call is received by the device for a specific Hunt Group, all telephones connected to the FXS ports belonging to the Hunt Group start ringing. The call is eventually received by whichever telephone answers the call first (and the other phones then stop ringing). This option is applicable only to FXS interfaces. ▪ [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 ISDNSuppServ parameter), allowing the routing of IP-to-Tel calls to specific BRI endpoints. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For defining the channel select mode per Hunt Group, see "Configuring Hunt Group Settings" on page 148. ▪ The logical (for digital interfaces) phone numbers of the device's B-channels are defined by the TrunkGroup parameter.
Web: Default Destination Number [DefaultNumber]	<p>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 'Hunt Group Table' (see Configuring the Hunt Group Table on page 146). This parameter is used as a starting number for the list of channels comprising all the device's Hunt Groups.</p> <p>The default value is 1000.</p>
Web: Source IP Address Input [SourceIPAddressInput]	<p>Determines the IP address that the device uses to determine the source of incoming INVITE messages for IP-to-Tel routing.</p> <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 [UseSourceNumberAsDisplayName]	<p>Determines the use of Tel Source Number and Display Name for Tel-to-IP calls.</p> <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

Parameter	Description
	<p>Name is received from the Tel side, the IP Display Name remains empty (default).</p> <ul style="list-style-type: none"> [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]	<p>Determines the use of Source Number and Display Name for IP-to-Tel calls.</p> <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 received from IP, the IP Source Number is used as the Tel Source Number and Presentation is set to Restricted (1). <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). 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>
Web: Use Routing Table for Host Names and Profiles EMS: Use Routing Table For Host Names [AlwaysUseRouteTable]	<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.
Web/EMS: Tel to IP Routing Mode [RouteModeTel2IP]	<p>For a description of this parameter, see "Configuring Outbound IP Routing Table" on page 165.</p>
Web: Outbound IP Routing Table EMS: SIP Routing > Tel to IP	
[Prefix]	<p>This <i>ini</i> file table parameter configures the 'Outbound IP Routing Table' for routing Tel-to-IP and IP-to-IP calls. The format of this parameter is as follows:</p> <p>[PREFIX] FORMAT PREFIX_Index = PREFIX_DestinationPrefix,</p>

Parameter	Description
	<p>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]</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 165. ▪ For a description on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Inbound IP Routing Table EMS: SIP Routing > IP to Hunt	
[PSTNPrefix]	<p>This <i>ini</i> file table parameter configures the routing of IP calls to Hunt Groups (or inbound IP Groups). The format of this parameter is as follows:</p> <p>[PSTNPrefix] FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, 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 172. ▪ To support the In-Call Alternative Routing feature, you can use two entries that support the same call but assigned with a different Hunt Group. The second entry functions as an alternative route if the first rule fails as a result of one of the release reasons configured in the AltRouteCauseIP2Tel table. ▪ Selection of Hunt Groups (for IP-to-Tel calls) is according to destination number, source number, and source IP address. ▪ The source IP address (SourceAddress) can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 and 10.8.8.99. ▪ The source IP address (SourceAddress) can include the

Parameter	Description
	<p>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.</p> <ul style="list-style-type: none"> ▪ 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 413. ▪ For a description on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web/EMS: IP to Tel Routing Mode [RouteModelIP2Tel]	<p>Determines whether to route IP calls to the Hunt Group before or after manipulation of the destination number (configured in "Configuring Number Manipulation Tables" on page 152).</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. ▪ [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 136).</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</p>

Parameter	Description
	<p>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 a detailed description of this feature, see Dial Plan Prefix Tags for IP-to-Tel Routing on page 418.
[EnableETSIDiversion]	<p>Defines 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> <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 Hunt 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</p>

Parameter	Description
	<p>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 Hunt Group. The Destination Number IP to Tel Manipulation table must be used to remove this prefix before placing the call to the ISDN.</p>

12.12.13.2 Alternative Routing Parameters

The alternative routing parameters are described in the table below.

Table 12-64: Alternative Routing Parameters

Parameter	Description
<p>Web/EMS: Redundant Routing Mode [RedundantRoutingMode]</p>	<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>
<p>Web: Enable Alt Routing Tel to IP EMS: Enable Alternative Routing [AltRoutingTel2IPEnable]</p>	<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 destination IP addresses is provided. <p>For information on the Alternative Routing feature, see "Configuring Alternative Routing (Based on Connectivity and QoS)" on page 442.</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

Parameter	Description
	<p>host name is not resolved (default).</p> <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 442. To receive quality information (displayed in the 'Quality Status' and 'Quality Info.' fields in "Viewing IP Connectivity" on page 356) per destination, this parameter must be set to 2 or 3.
Web: Alt Routing Tel to IP Connectivity Method EMS: Alternative Routing Telephone to IP Connection Method [AltRoutingTel2IPConnMethod]	Determines the method used by the device for periodically querying the connectivity status of a destination IP address. <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.
[EnableAltMapTel2IP]	Enables different Tel-to-IP destination number manipulation rules per routing rule when several (up to three) Tel-to-IP routing rules are defined and if alternative routing using release causes is used. For example, if an INVITE message for a Tel-to-IP call is returned with a SIP 404 Not Found response, the call can be re-sent to a different destination number (as defined using the parameter NumberMapTel2IP). <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable
Web: Alt Routing Tel to IP Keep Alive Time EMS: Alternative Routing Keep Alive Time [AltRoutingTel2IPKeepAliveTime]	Defines the time interval (in seconds) between SIP OPTIONS Keep-Alive messages used for the IP Connectivity application. The valid range is 5 to 2,000,000. The default value is 60.
Web/EMS: Alternative Routing Tone Duration [ms] [AltRoutingToneDuration]	Determines the duration (in milliseconds) for which the device plays a tone to the endpoint on each Alternative Routing attempt. When the device finishes playing the tone, a new SIP INVITE message is sent to the new destination. The tone played is the Call Forward Tone (Tone Type #25 in the CPT file). The valid range is 0 to 20,000. The default is 0 (i.e., no tone is played).
Web: Max Allowed Packet Loss for Alt Routing [%] [IPConnQoSMaxAllowedPL]	Packet loss in percentage at which the IP connection is considered a failure and Alternative Routing mechanism is activated. The default value is 20%.
Web: Max Allowed Delay for Alt Routing [msec] [IPConnQoSMaxAllowedDelay]	Transmission delay (in msec) at which the IP connection is considered a failure and the Alternative Routing mechanism is activated. The range is 100 to 10,000. The default value is 250.

Parameter	Description
Web: Reasons for Alternative Tel-to-IP Routing Table EMS: Alt Route Cause Tel to IP	
[AltRouteCauseTel2IP]	<p>This <i>ini</i> file table parameter configures SIP call failure reason values received from the IP side. If an IP call is released as a result of one of these reasons, the device attempts to locate an alternative IP route (address) for the call in the 'Outbound IP Routing Table' (if a Proxy is not used) or used as a redundant Proxy (you need to set the parameter RedundantRoutingMode to 2). The release reason for Tel-to-IP calls is provided in SIP 4xx, 5xx, and 6xx response codes.</p> <p>The format of this parameter is as follows:</p> <pre>[AltRouteCauseTel2IP] FORMAT AltRouteCauseTel2IP_Index = AltRouteCauseTel2IP_ReleaseCause; [AltRouteCauseTel2IP]</pre> <p>For example:</p> <pre>AltRouteCauseTel2IP 0 = 486; (Busy Here) AltRouteCauseTel2IP 1 = 480; (Temporarily Unavailable) AltRouteCauseTel2IP 2 = 408; (No Response)</pre> <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 an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368
Web: Reasons for Alternative IP-to-Tel Routing Table EMS: Alt Route Cause IP to Tel	
[AltRouteCauseIP2Tel]	<p>This <i>ini</i> file table parameter configures call failure reason values received from the PSTN side (in Q.931 presentation). If a call is released as a result of one of these reasons, the device attempts to locate an alternative Hunt 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)</pre>

Parameter	Description
	<p>AltRouteCauseIP2Tel 1 = 1 (Unallocated Number) AltRouteCauseIP2Tel 2 = 17 (Busy Here)</p> <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 Hunt 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 Hunt 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 an explanation on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web/EMS: Forward On Busy Trunk Destination	
[ForwardOnBusyTrunkDest]	<p>This ini file table parameter configures the Forward On Busy Trunk Destination table. This table allows you to define an alternative IP destination - IP address or SIP Request-URI user name and host part (i.e., user@host) per Hunt Group for IP-to-Tel calls. The IP-to-Tel call is forwarded to this IP destination (using 3xx response) if the following exists:</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> <p>Notes:</p> <ul style="list-style-type: none"> The maximum number of indices (starting from 1) depends on the maximum number of Hunt Groups. For the destination, instead of a dotted-decimal IP address, FQDN can be used. In addition, the following syntax can be used: "host:port;transport=xxx"(i.e., IP address, port and transport type). For a detailed description of this feature, see Configuring

Parameter	Description
	Call Forward upon Busy Trunk on page 176

12.12.13.3 Number Manipulation Parameters

The number manipulation parameters are described in the table below.

Table 12-65: Number Manipulation Parameters

Parameter	Description
Web: Set Redirect number Screening Indicator to TEL EMS: Set IP To Tel Redirect Screening Indicator [SetIp2TelRedirectScreeningInd]	<p>Defines the value of the Redirect Number screening indicator in ISDN Setup messages.</p> <ul style="list-style-type: none"> ▪ [-1] Not Configured (default) ▪ [0] User Provided ▪ [1] User Passed ▪ [2] User Failed ▪ [3] Network Provided <p>Note: This parameter is applicable only to digital PSTN interfaces (ISDN).</p>
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

Parameter	Description
	<p>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.</p> <ul style="list-style-type: none"> 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 Hunt 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 Hunt Group ID as prefix (default). [1] Yes = Add Hunt Group ID as prefix to called number. <p>Notes:</p> <ul style="list-style-type: none"> This option can be used to define various routing rules. To use this feature, you must configure the Hunt Group IDs (see Configuring Hunt Group Table on page 146).
Web: Add Trunk ID as Prefix EMS: Add Port ID As Prefix [AddPortAsPrefix]	<p>Determines whether the slot number and port number/Trunk ID are added as a prefix to the called number for Tel-to-IP calls.</p> <ul style="list-style-type: none"> [0] No = slot number and port number/Trunk ID not added as prefix (default). [1] Yes = slot number and port number/Trunk ID added as prefix <p>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.</p> <p>This option can be used to define various routing rules.</p>
Web/EMS: Add Trunk Group ID as Prefix to Source [AddTrunkGroupAsPrefixToSource]	<p>Determines whether the device adds the Hunt Group ID (from where the call originated) as the prefix to the calling number (i.e. source number).</p> <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]	<p>Determines whether the internal channel number is used as the destination number if the called number is missing.</p> <ul style="list-style-type: none"> [0] No (default) [1] Yes <p>Note: This parameter is applicable only to Tel-to-IP calls and if the called number is missing.</p>

Parameter	Description
[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]	<p>Determines whether the Numbering Plan Indicator (NPI) and Type of Numbering (TON) are added to the Calling Number for Tel-to-IP calls.</p> <ul style="list-style-type: none"> [0] No = Do not change the Calling Number (default). [1] Yes = Add NPI and TON to the Calling Number ISDN Tel-to-IP call. <p>For example: After receiving a Calling Number of 555, NPI of 1, and TON of 3, the modified number becomes 13555. This number can later be used for manipulation and routing.</p>
Web: Add NPI and TON to Called Number EMS: Add NPI And TON As Prefix To Called Number [AddNPIandTON2CalledNumber]	<p>Determines whether NPI and TON are added to the Called Number for Tel-to-IP calls.</p> <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. <p>For example: After receiving a Called Number of 555, NPI of 1 and TON of 3, the modified number becomes 13555. This number can later be used for manipulation and routing.</p>
Web: IP to Tel Remove Routing Table Prefix EMS: Remove Prefix [RemovePrefix]	<p>Determines whether the device removes the prefix from the destination number for IP-to-Tel calls.</p> <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" on page 172) from a telephone number for an IP-to-Tel call before forwarding it to Tel. <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 Hunt 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>If enabled, the device swaps the calling and called numbers received from the Tel side (for Tel-to-IP calls). The SIP INVITE message contains the swapped numbers.</p> <ul style="list-style-type: none"> [0] = Disabled (default)

Parameter	Description
	<ul style="list-style-type: none"> [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.
Web: Redirect Number IP -> Tel EMS: Redirect Number Map IP to Tel	
[RedirectNumberMapIp2Tel]	<p>This ini file table parameter 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).</p> <p>The format of this parameter is as follows:</p> <pre>[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]</pre> <p>For example: RedirectNumberMapIp2Tel 1 = *, 88, *, 1, 1, 2, 0, 255, 9, , 255;</p> <p>Notes:</p> <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,

Parameter	Description
	<p>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.</p> <ul style="list-style-type: none"> ▪ 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.
Web: Redirect Number Tel -> IP EMS: Redirect Number Map Tel to IP	
[RedirectNumberMapTel2IP]	<p>This ini file table parameter manipulates the redirect number for Tel-to-IP calls. The manipulated Redirect Number is sent in the SIP Diversion, History-Info, or Resource-Priority headers. The format of this parameter is as follows:</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 following parameters are applicable only to digital interfaces: NumberType, NumberPlan, and IsPresentationRestricted. ▪ The parameters NumberType and NumberPlan are applicable only to the SIP Resource-Priority header.

Parameter	Description
Web: Destination Phone Number Manipulation Table for Tel to IP Calls EMS: SIP Manipulations > Destination Telecom to IPs	
[NumberMapTel2IP]	<p>This <i>ini</i> file table parameter 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:</p> <pre>NumberMapTel2Ip 0 = 01,\$\$,*,0,0,2,\$\$\$\$,971,\$\$\$\$,,\$\$,\$\$; NumberMapTel2Ip 1 = 10,10,*,255,255,3,0,5,100,\$\$,255,\$\$\$,\$\$;</pre> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table parameter can include up to 120 indices (0-119). ▪ The manipulation rules are done in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and then Suffix2Add. ▪ If the called and calling numbers match the DestinationPrefix and/or SourcePrefix conditions, then the parameters 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 152). ▪ For a description on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Destination Phone Number Manipulation Table for IP to Tel Calls EMS: EMS: SIP Manipulations > Destination IP to Telecom	
[NumberMapIP2Tel]	<p>This <i>ini</i> file table parameter manipulates the destination number of IP-to-Tel calls. The format of this parameter is as follows:</p> <pre>[NumberMapIp2Tel] FORMAT NumberMapIp2Tel_Index = NumberMapIp2Tel_DestinationPrefix, NumberMapIp2Tel_SourcePrefix, NumberMapIp2Tel_SourceAddress,</pre>

Parameter	Description
	<p>NumberMapIp2Tel_NumberType, NumberMapIp2Tel_NumberPlan, NumberMapIp2Tel_RemoveFromLeft, NumberMapIp2Tel_RemoveFromRight, NumberMapIp2Tel_LeaveFromRight, NumberMapIp2Tel_Prefix2Add, NumberMapIp2Tel_Suffix2Add, NumberMapIp2Tel_IsPresentationRestricted; [NumberMapIp2Tel]</p> <p>For example:</p> <p>NumberMapIp2Tel 0 = 01,034,10.13.77.8,\$\$,0,\$\$,2,\$\$,667,\$\$; NumberMapIp2Tel 1 = 10,10,1.1.1.1,255,255,3,0,5,100,\$\$,255;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table parameter can include up to 100 indices. ▪ The manipulation rules are done in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and then Suffix2Add. ▪ If the called and calling numbers match the DestinationPrefix, SourcePrefix, and/or SourceAddress conditions, then the RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, 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 152). ▪ For a description on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
[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

Parameter	Description
Web: Source Phone Number Manipulation Table for Tel to IP Calls EMS: SIP Manipulations > Source Telecom to IP	
[SourceNumberMapTel2IP]	<p>This <i>ini</i> file table parameter manipulates the source phone number for Tel-to-IP calls. The format of this parameter is as follows:</p> <pre>[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]</pre> <p>For example:</p> <pre>SourceNumberMapTel2Ip 0 = 22,03,\$\$,0,0,\$\$,2,\$\$,667,\$\$,0,\$\$, \$\$; SourceNumberMapTel2Ip 0 = 10,10,*,255,255,3,0,5,100,\$\$,255,\$\$, \$\$;</pre> <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 Party ID header by configuring the EnableRPIHeader and AddTON2RPI parameters. ▪ To configure manipulation of source numbers for Tel-to-IP calls using the Web interface, see "Configuring Number Manipulation Tables" on page 152). ▪ For a description on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

Parameter	Description
Web: Source Phone Number Manipulation Table for IP to Tel Calls EMS: EMS: SIP Manipulations > Source IP to Telkom	
[SourceNumberMapIP2Tel]	<p>This <i>ini</i> file table parameter 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:</p> <pre>SourceNumberMapIP2Tel 0 = 22,03,\$\$,,\$\$,,\$\$,2,667,\$\$,,\$\$; SourceNumberMapIP2Tel 1 = 034,01,1.1.1.1,\$\$,0,2,\$\$,,\$\$,972,\$\$,10;</pre> <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. ▪ To configure manipulation of source numbers for IP-to-Tel calls using the Web interface, see "Configuring Number Manipulation Tables" on page 152). ▪ For a description on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
[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

Parameter	Description
<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 	
Phone-Context Parameters	
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.
Web: Phone Context Table EMS: SIP Manipulations > Phone Context	
[PhoneContext]	<p>This <i>ini</i> file table parameter defines the Phone Context table. This parameter maps NPI and TON to the SIP Phone-Context parameter. When a call is received from the 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</p>

Parameter	Description
	<p>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 160. ▪ For a description on using <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.12.13.4 LDAP Parameters

The Lightweight Directory Access Protocol (LDAP) parameters are described in the table below. For a detailed description on routing based on LDAP, refer to "Routing Based on LDAP Active Directory Queries" on page 605.

Table 12-66: LDAP Parameters

Parameter	Description
Web: LDAP Service [LDAPServiceEnable]	<p>Determines whether to enable the LDAP service.</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]	Defines the LDAP server's IP address in dotted-decimal notation (e.g., 192.10.1.255). The default is 0.0.0.0.
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]	<p>Defines the LDAP server's bind DN. This is used as the username during connection and binding to the server.</p> <p>For example: LDAPBindDN = "CN=Search user,OU=Labs,DC=OCSR2,DC=local"</p>
Web: LDAP Search Dn [LDAPSearchDN]	<p>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.</p> <p>For example: LDAPSearchHDN = "CN=Search user,OU=Labs,DC=OCSR2,DC=local"</p>

Parameter	Description
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]	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 "msRTCSIP-PrimaryUserAddress".
Web: MS LDAP PBX Number attribute name [MSLDAPPBXNumAttributeName]	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]	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".

12.13 SBC Parameters

The SBC parameters are described in the table below.

Table 12-67: SBC Parameters

Parameter	Description
Web: Enable SBC EMS: Enable ISBC [EnableSBCApplication]	Enables the Session Border Control (SBC) application. <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. In addition to enabling this parameter, the number of maximum SBC/IP-to-IP sessions must be defined in the Software Upgrade Key.
WAN Interface Name [WanInterfaceName]	Defines the WAN interface for the VoIP interface. The available interface options depends on the hardware configuration (e.g., Ethernet, T1, or SHDSL) and/or whether VLANs are defined for the WAN interface (see Virtual LAN Interface (VLAN) on page 301). The value must be enclosed in single quotation marks ('...'), for example, WanInterfaceName = 'GigabitEthernet 0/0'. This WAN interface can be assigned to SIP signaling and/or media interfaces, in the SIP Interface table, where it is represented as "WAN" (see Configuring SIP Interface Table on page 117). If VLANs are configured, for example, for the Ethernet WAN interface (see Data Settings on page 222),

Parameter	Description
	<p>then you can select the WAN VLAN on which you want to run these SIP signaling and/or media interfaces. Therefore, for each outgoing SIP packet, the device sends it on the defined outgoing WAN interface; for each incoming SIP packet, the device identifies the packet according to the WAN interface from where it is received.</p> <p>Notes:</p> <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. This parameter is applicable only if the data-routing functionality is supported (i.e., relevant Software Upgrade Feature Key is installed on the device).
Web/EMS: WAN HTTP Port [WanMgmtHttpPort]	<p>WAN HTTP port number. This parameter allows remote device Web management from the WAN. To enable Web management from the WAN, configure the desired port (e.g., port 80, which is the default HTTP port).</p> <p>The default is 0 (i.e., no remote Web management).</p> <p>Note: If the parameter HTTPOnly is set to 1, HTTP access is not allowed.</p>
Web/EMS: WAN HTTPS Port [WanMgmtHttpsPort]	<p>WAN HTTPS port number. This parameter allows secure remote device Web management from the WAN. To enable secure Web management, configure the desired port (e.g., port 443). The default is 0 (i.e., remote Web management is not secured).</p>
Web: Allow Unclassified Calls [AllowUnclassifiedCalls]	<p>Determines whether calls (incoming packets) that cannot be classified (i.e. classification process fails) into a Source IP Group (in the Classification table) are either rejected or processed.</p> <ul style="list-style-type: none"> [0] Reject = the call is rejected if classification fails. [1] Allow = if classification fails, the incoming packet is assigned to the default IP Group of the default SRD (and the call is subsequently processed). (Default.)
Web: SBC No Answer Timeout [SBCAlertTimeout]	<p>Defines the timeout (in seconds) for SBC outgoing (outbound IP routing) SIP INVITE messages. If the called IP party does not answer the call within this user-defined interval, the device disconnects the session. The device starts the timeout count upon receipt of a SIP 180 Ringing response from the called party. If no other SIP response (for example, 200 OK) is received thereafter within this timeout, the call is released.</p> <p>The valid range is 0 to 3600 seconds. the default is 600.</p>
Web: SBC Max Forwards Limit [SBCMaxForwardsLimit]	<p>Defines the value of the Max-Forwards SIP header. The Max-Forwards header is used to limit the number of servers (such as proxies) that can forward the SIP request. The Max-Forwards value indicates the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request.</p> <p>This parameter affects the Max-Forwards header in the received message as follows:</p> <ul style="list-style-type: none"> If the received header's original value is 0, the message is

Parameter	Description
	<p>not passed on and is rejected.</p> <ul style="list-style-type: none"> If the received header's original value is less than this parameter's value, the header's value is decremented before being sent on. If the received header's original value is greater than the parameter's value, the header's value is replaced by the user-defined parameter's value. <p>The valid value range is 1-70. The default is 10.</p>
Web: Minimum Session-Expires [SBCMinSE]	<p>Defines the minimum amount of time (in seconds) between session refresh requests in a dialog before the session is considered timed out. This value is conveyed in the SIP Min-SE header.</p> <p>The valid range is 0 (default) to 1,000,000 (where 0 means that the device does not limit Session-Expires).</p>
Web/EMS: Handle P-Asserted-Identity [SBCAssertIdentity]	<p>Determines the device's privacy handling of the P-Asserted-Identity header. This indicates how the outgoing SIP message asserts identity.</p> <ul style="list-style-type: none"> [0] Don't Care (default) = P-Asserted Identity header is not affected. [1] Add P-Asserted-Identity Header = Adds a P-Asserted-Identity header. The header's values are taken from the source URL. [2] Remove P-Asserted-Identity Header = Removes the P-Asserted-Identity header. <p>Notes:</p> <ul style="list-style-type: none"> This parameter affects only the initial INVITE request. The configuration of privacy handling in the IP Group table takes precedence over the settings of this global parameter. <ul style="list-style-type: none"> ✓ If in the IP Group this parameter is set to 'Don't care', then the settings of this global parameter is used. ✓ If this global parameter and the IP Group are set to 'Don't care', the device uses the same P-Asserted-Identity header (if present) in the incoming message for the outgoing message. This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).
Web: Keep original user in Register [SBCKeepContactUserinRegister]	<p>Determines whether the device replaces the Contact user with a unique Contact user in the outgoing message in response to a REGISTER request.</p> <ul style="list-style-type: none"> [0] Disable = (default) The device replaces the original Contact user with a unique Contact user, for example: <ul style="list-style-type: none"> ✓ Received Contact: <sip:123@domain.com> ✓ Outgoing (unique) Contact: <sip:FEU1_7_1@SBC> [1] Enable = The original Contact user is retained and used in the outgoing REGISTER request. <p>Note: This parameter is applicable only to REGISTER messages received from USER IP Groups and that are sent to SERVER IP Groups.</p>

Parameter	Description
[SBCReferBehavior]	<p>Defines how the device handles REFER requests.</p> <ul style="list-style-type: none"> ▪ [0] = Refer-To header is unchanged (default). ▪ [1] = Uses the database for Refer-To as described below. <p>When enabled, the device handles REFERs as follows:</p> <ol style="list-style-type: none"> 1 Before passing on the REFER request, the device changes the host part to the device's IP address and adds a special prefix ("T~&R_") to the Contact user part. 2 The incoming INVITE is identified as a REFER-resultant INVITE according to the special prefix. 3 The device replaces the host part (in the Request-URI) with the host from the REFER contact. The prefix ("T~&R_") remains in the user part for regular classification, manipulation, and routing. The special prefix can be used for specific routing rules for REFER-resultant INVITES. 4 The prefix is removed before the resultant INVITE is sent to the destination.
[SBCXferPrefix]	<p>When the SBCReferBehavior is set to 1, the device, while interworking the SIP REFER message, adds the prefix "T~&R-" to the user part of the URI in the Refer-To header. After this, the device can receive an INVITE with such a prefix (the INVITE is sent by the UA that receives the REFER message or 302 response). If the device receives an INVITE with such a prefix, it replaces the prefix with the value defined for the SBCXferPrefix parameter.</p> <p>The default value is empty ("").</p> <p>Note: This feature is also applicable to 3xx redirect responses. The device adds the prefix "T~&R-" to the URI user part in the Contact header if the SBC3xxBehavior parameter is set to 1.</p>
[SBC3xxBehavior]	<p>Determines the device's handling of SIP 3xx responses. When enabled, the device handles SIP redirections between different subnets (e.g., between LAN and WAN sides). This is required where the new address provided by the redirector (Redirect sever) may not be reachable by the far-end user (FEU) located in another subnet. For example, a far-end user (FEU) in the WAN sends a SIP request via the device to a Redirect server in the LAN, and the Redirect server replies with a SIP 3xx response to a PBX in the LAN in the Contact header. If the device sends this response as is (i.e., with the original Contact header), the FEU is unable to reach the new destination.</p> <ul style="list-style-type: none"> ▪ [0] (default) = The device sends the received SIP 3xx response without changing the Contact header (transparent handling). ▪ [1] = The device changes the URI in the Contact header of the received SIP 3xx response to its own URI and adds a special user prefix ("T~&R_"), which is then sent to the FEU. The FEU then sends a new INVITE to the device,

Parameter	Description
	<p>which the device then sends to the correct destination.</p> <p>Notes:</p> <ul style="list-style-type: none"> When this parameter is changed from 1 to 0, new 3xx Contact headers remain unchanged. However, requests with the special prefix continue using the device's database to locate the new destination. Only one database entry is supported for the same host, port, and transport combination. For example, the following URLs cannot be distinguished by the device: <ul style="list-style-type: none"> ✓ sip:10.10.10.10:5060;transport=tcp;param=a ✓ sip:10.10.10.10:5060;transport=tcp;param=b The database entry expires two hours after the last use. The maximum number of destinations (i.e., database entries) is 50. For a detailed description of SIP 3xx Redirect response handling, see "Handling SIP 3xx Redirect Responses" on page 503.
Web: SBC User Registration Time [SBCUserRegistrationTime]	<p>Defines the duration of the periodic registrations between the user and the device (the device responds with this value to the user). When set to 0, the device does not change the Expires header's value received in the user's REGISTER request. If no Expires header is received in the REGISTER message and the SBCUserRegistrationTime parameter is set to 0, then by default, the Expires header's value is set to 180 seconds.</p> <p>The valid range is 0 to 2,000,000 seconds. The default is 0.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: SBC Proxy Registration Time [SBCProxyRegistrationTime]	<p>Defines the duration for which the user is registered in the proxy database (after the device forwards the REGISTER message). When set to 0, the device sends the Expires header's value as received from the user to the proxy.</p> <p>The valid range is 0 to 2,000,000 seconds. The default is 0.</p>
Web: SBC Survivability Registration Time [SBCSurvivabilityRegistrationTime]	<p>Defines the duration of the periodic registrations between the user and the device, when the device is in survivability state (i.e., when REGISTER requests cannot be forwarded to the proxy and are terminated by the device). When set to 0, the device uses the value set by the SBCUserRegistrationTime parameter for the device's response.</p> <p>The valid range is 0 to 2,000,000 seconds. The default is 0.</p>
Web: SBC GRUU Mode [SBCGruuMode]	<p>Determines the Globally Routable User Agent (UA) URI (GRUU) support, according to RFC 5627.</p> <ul style="list-style-type: none"> [0] None = No GRUU is supplied to users. [1] As Proxy = The device provides same GRUU types as the proxy provided the device's GRUU clients. (default) [2] Temporary only = Supply only temporary GRUU to users. (Currently not supported.) [3] Public only = The device provides only public GRUU to users.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [4] Both = The device provides temporary and public GRUU to users. (Currently not supported.) <p>This parameter allows the device to act as a GRUU server for its SIP UA clients, providing them with public GRUU's, according to RFC 5627. The public GRUU provided to the client is depicted in the SIP Contact header parameters, "pub-gruu". Public GRUU remains the same over registration expirations. On the other SBC leg communicating with the Proxy/Registrar, the device acts as a GRUU client.</p> <p>The device creates a GRUU value for each of its registered clients, which is mapped to the GRUU value received from the Proxy server. In other words, the created GRUU value is only used between the device and its clients (endpoints).</p> <p>Public-GRUU: sip:userA@domain.com;gr=unique-id</p>
Web: SBC Direct Media [SBCDirectMedia]	<p>Enables the No Media Anchoring feature (i.e., direct media), which uses SBC SIP signaling capabilities without handling the RTP/SRTP (media) flow between remote SIP user agents. The RTP packet flow does not traverse the device, instead, the two SIP user agents establish a direct RTP/SRTP flow between one another. Signaling continues to traverse the device with minimal intermediation and involvement to enable certain SBC abilities such as routing</p> <ul style="list-style-type: none"> ▪ [0] Disable = All cross SRD's calls via SBC are not direct media - internal SRD calls are according to SRD configuration (default). ▪ [1] Enable = All SBC calls use direct media. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For a detailed description on No Media Anchoring, see "No Media Anchoring" on page 497. ▪ When no media anchoring is enabled: <ul style="list-style-type: none"> ✓ Manipulation is not performed on SDP data (offer/answer transaction) such as ports and IP address. ✓ Coder extensions (transcoding) is not possible. ✓ Coder limitations and preference (Allowed Coders list) can be applied. ✓ Opening voice channels and allocation of IP media ports are not required. ▪ No Media Anchoring is typically implemented in the following scenarios: <ul style="list-style-type: none"> ✓ SBC device is located within the LAN. ✓ Call between two SIP user agents in the same network (LAN) and signals are sent to a SIP proxy server that is located in the WAN. ▪ The benefits of implementing the No Media Anchoring feature includes the following: saves network bandwidth, reduces CPU usage (no RTP/SRTP handling), and avoids interference in SDP negotiation and header manipulation on RTP/SRTP. ▪ The process for handling the No Media Anchoring feature

Parameter	Description
	<p>is as follows:</p> <ul style="list-style-type: none"> ✓ Identifying a No Media Anchoring call, according to configuration and the call's properties (such as source, destination, IP Group, and SRD). ✓ Handling the identified No Media Anchoring call. <ul style="list-style-type: none"> ▪ You can enable No Media Anchoring per SRD, where calls between two user agents that pertain to the same SRD (source and destination) are handled as a No Media Anchoring (direct media) call. ▪ No Media Anchoring calls cannot operate simultaneously with the following SBC features: Force transcoding, Extension Coders. Once No Media Anchoring is identified, these features are disabled. ▪ The Coder Restriction feature operates simultaneously with No Media Anchoring calls. Restricted coders are removed from the SDP offer message. ▪ Chosen configuration can't handle call from any user agent to a foreign user agent (vice versa) but both user agents belong to the same SRD and parameter IntraSRDMediaAnchoring for that specific SRD is > 0. ▪ When this parameter is disabled, No Media Anchoring calls between two user agents that belong to separate SRD's cannot be configured. No Media Anchoring calls between two user agents that belong to the same SRD is configurable only (in this case).
[SBCMediaSecurityBehaviour]	<p>The device supports transcoding between SRTP and RTP. The device can also enforce SBC legs to use SRTP\RTP, using the IP Profile parameter SBCMediaSecurityBehaviour:</p> <ul style="list-style-type: none"> ▪ [0] As is (default): no special handling for RTP\SRTP is done. ▪ [1] SRTP: SBC legs negotiate only SRTP media lines, and RTP media lines are removed from the incoming SDP offer\answer. ▪ [2] RTP: SBC legs negotiate only RTP media lines, and SRTP media lines are removed from the incoming offer\answer. ▪ [3] Both: each offer\answer is extended (if not already) to two media lines - one RTP and the other SRTP. <p>If two SBC legs (after offer\answer negotiation) use different security types (i.e., one RTP and the other SRTP), then the device performs RTP-SRTP transcoding. To transcode between RTP and SRTP, the following prerequisites must be met:</p> <ul style="list-style-type: none"> ▪ At least one supported SDP "crypto" attribute and parameters ▪ EnableMediaSecurity must be set to 1 <p>If one of the above transcoding prerequisites is not met, then:</p> <ul style="list-style-type: none"> ▪ any value other than "As is" is discarded. ▪ if the incoming offer is SRTP, force transcoding, coder transcoding, and DTMF extensions are not applied. <p>Transcoding between RTP and SRTP does not require any</p>

Parameter	Description
	<p>DSP allocation. SRTP to SRTP does not require DSP allocation.</p> <p>Note: This parameter can only be configured as an IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).</p>
[SBCRFC2833Behavior]	<p>Determines RFC 2833 SDP offer\answer negotiation.</p> <ul style="list-style-type: none"> ▪ [0] As is = The device does not intervene in the RFC 2833 negotiation. (default) ▪ [1] Extend = Each outgoing offer\answer includes RFC 2833 in the offered SDP (the device adds RFC 2833 only if the incoming offer does not include RFC 2833). ▪ [2] Disallow = The device removes RFC 2833 from the incoming offer. <p>Note: This parameter can only be configured as an IP Profile, using the IPProfile parameter (see Configuring IP Profiles on page 143).</p>
[SBCAlternativeDTMFMethod]	<p>The device's first priority for DTMF method at each leg is RFC 2833. Therefore, if a specific leg negotiates RFC 2833 successfully, then the chosen DTMF method for this leg is RFC 2833. For legs where RFC 2833 is not negotiated successfully, the device uses this parameter to determine the chosen DTMF method for the leg.</p> <ul style="list-style-type: none"> ▪ [0] = Don't care - the device does not attempt to interwork any special DTMF method. (default) ▪ [1] = In Band ▪ [2] = INFO, Cisco ▪ [3] = INFO, Nortel ▪ [4] = INFO, Korea <p>Note: This parameter can only be configured as an IP Profile, using the IPProfile parameter (see Configuring IP Profiles on page 143).</p>
Web: Diversion Mode [SBCDiversionMode]	<p>Defines the device's handling of the SIP Diversion header. For a detailed description of the device's interworking of the History-Info and Diversion headers, see "Interworking SIP Diversion and History-Info Headers" on page 505.</p> <ul style="list-style-type: none"> ▪ [0] Don't Care = Diversion header is not handled. (default) ▪ [1] Add = History-Info header converted to a Diversion header. ▪ [2] Remove = Removes the Diversion header and the conversion to the History-Info header depends on the settings of the SBCHistoryInfoMode parameter. <p>Note: This parameter can only be configured as an IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).</p>
Web: History Info Mode [SBCHistoryInfoMode]	<p>Defines the device's handling of the History-Info header. For a detailed description of the device's interworking of the History-Info and Diversion headers, see "Interworking SIP Diversion and History-Info Headers" on page 505.</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ [0] Don't Care = History-Info header is not handled. (default) ▪ [1] Add = Diversion header converted to a History-Info header. ▪ [2] Remove = History-Info header removed from the SIP dialog and the conversion to the Diversion header depends on the settings of the SBCEX diversionMode parameter. <p>Note: This parameter can only be configured as an IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143).</p>
Web: Extension Coders Group ID [SBCEX extensionCodersGroupID]	<p>Defines the Coders Group ID for extended (additional) coders, per IP Profile. This is used when transcoding is required between two user agents (i.e., the SDP answer from one user agent doesn't include any coder included in the offer previously sent by the other user agent). Therefore, to allow user agents of different IP Groups to communicate with each other (regardless of their capabilities), an extended coders table with at least one coder that is supported by each IP Groups' user agents needs to be assigned to each IP Group. Therefore, each offer destined to specific IP Groups includes this coder.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter can only be configured as an IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143). ▪ To configure Coders Groups, see "Configuring Coders Groups" on page 140.
Web: Allowed Coders Mode [SBCAllowedCodersMode]	<p>Determines the mode of the Allowed Coders feature.</p> <ul style="list-style-type: none"> ▪ [0] Restriction = In the incoming SDP offer, the device uses only coders that are also listed in the Allowed Coders Group; the rest are removed from the SDP offer (i.e., only coders common between SDP offered coders and Allowed Coders Group are used). If an Extension Coders Group is also selected (using the IP Profile's SBCEX extensionCodersGroupID parameter), then these coders are added to the SDP offer. ▪ [1] Preference = The device rearranges the priority (order) of the coders in the incoming SDP offer according to their order of appearance in the Allowed Coders Group list. ▪ [2] Restriction and Preference = Performs both Restriction and Preference. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter can only be configured as an IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 143). ▪ To define Allowed Coders Groups, use the AllowedCodersGroup parameter. ▪ To configure Extension Coders Groups, use the CodersGroups parameter.

Parameter	Description
	<ul style="list-style-type: none"> For a detailed description of the Allowed Coders feature, see "Coder Restrictions Control" on page 499.
Web: Allowed Audio Coders Table	
[AllowedCodersGroup0] [AllowedCodersGroup1] [AllowedCodersGroup2] [AllowedCodersGroup3] [AllowedCodersGroup4]	<p>This <i>ini</i> file table parameter allows you to define up to 5 Allowed Coders Groups, each with up to 10 coders. The Allowed Coders Group determines the coders that can be used for a specific SBC leg. Coders excluded from the Allowed Coders Group are removed from the SDP offer (only coders common between SDP offered coders and Allowed Coders are used). In addition, coders defined in top entries in the Allowed Coders Group are assigned higher priority than those entered in lower entries.</p> <p>[AllowedCodersGroupx] FORMAT AllowedCodersGroup_Index = AllowedCodersGroup_Name; [AllowedCodersGroup]</p> <p>Where,</p> <ul style="list-style-type: none"> AllowedCodersGroupx = Allowed Coders Group index (0-4). Index = Coder index number per group (0-9). Name = Coder name. For supported coders, see the CodersGroup parameter. <p>For example, below represents two configured Allowed Coders Groups, 0 and 1. Group 0 has two coders; Group 1 has one coder. The highest priority coder is G.723.1.</p> <p>[AllowedCodersGroup0] FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name; AllowedCodersGroup0 0 = g7231; AllowedCodersGroup0 1 = g711Alaw64k; [\AllowedCodersGroup0]</p> <p>[AllowedCodersGroup1] FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup0_Name; AllowedCodersGroup1 0 = g711Ulaw64k; [\AllowedCodersGroup1]</p> <p>Notes:</p> <ul style="list-style-type: none"> The Allowed Coders table is performed on audio media only. Allowed Coder Groups can be assigned to IP Profiles (see "Configuring IP Profiles" on page 143). For configuring the table using the Web interface, see "Configuring Allowed Coder Groups" on page 197. For a description on configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

Parameter	Description
Web: Message Manipulations Table EMS: Message Manipulations	
[MessageManipulations]	<p>This ini file table parameter defines manipulation rules for SIP header messages.</p> <p>The format of this parameter is as follows:</p> <pre>[MessageManipulations] FORMAT MessageManipulations_Index = MessageManipulations_ManSetID, MessageManipulations_MessageType, MessageManipulations_Condition, MessageManipulations_ActionSubject, MessageManipulations_ActionType, MessageManipulations_ActionValue, MessageManipulations_RowRole; [MessageManipulations]</pre> <p>For example, the below configuration changes the user part of the SIP From header to 200:</p> <pre>MessageManipulations 1 = 0, Invite.Request, , Header.From.Url.User, 2, 200, 0;</pre> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table can include up to 200 indices (where 1 is the first index). ▪ 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 detailed description of the table's individual parameters and for configuring the table using the Web interface, see "Configuring Message Manipulations" on page 206. ▪ For a description on configuring ini file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Admission Control EMS: Call Admission Control	
[SBCAdmissionControl]	<p>This <i>ini</i> file table parameter defines limitations on the number of allowed concurrent calls (SIP dialogs). This is useful for controlling bandwidth utilization between Voice and Data traffic.</p> <p>The format of this parameter is as follows:</p> <pre>[SBCAdmissionControl] FORMAT SBCAdmissionControl_Index = SBCAdmissionControl_LimitType, SBCAdmissionControl_IPGroupID, SBCAdmissionControl_SRDID, SBCAdmissionControl_RequestType, SBCAdmissionControl_RequestDirection, SBCAdmissionControl_Limit, SBCAdmissionControl_LimitPerUser, SBCAdmissionControl_Rate, SBCAdmissionControl_MaxBurst; [SBCAdmissionControl]</pre>

Parameter	Description
	<p>For example, the below configuration allows a maximum of 10 concurrent SIP INVITEs for IP Group 1: SBCAdmissionControl 1 = 0, 1, -1, 1, 0, 10, -1, 0, 0;</p> <p>Notes:</p> <ul style="list-style-type: none"> For a detailed description of the table's individual parameters and for configuring the table using the Web interface, see "Configuring Admission Control" on page 195. For a description on configuring ini file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: Classification Table EMS: SBC Classification	
[Classification]	<p>This <i>ini</i> file table parameter configures the Classification table. This table classifies the incoming SIP INVITE to a Source IP Group. The format of this parameter is as follows:</p> <pre>[Classification] FORMAT Classification_Index = Classification_SrcIPGroupID, Classification_SrcSRDID, Classification_SrcAddress, Classification_SrcUsernamePrefix, Classification_SrcHost, Classification_DestUsernamePrefix, Classification_DestHost; [Classification]</pre> <p>For example: Classification 1 = -1, -1, , * , * , * , * ;</p> <p>Notes:</p> <ul style="list-style-type: none"> This table can include up to 20 indices (where 0 is the first index). If this classification process fails to determine the Source IP Group to which the incoming packet belongs, the call can either be rejected or assigned to the default IP Group of the default SRD (and processed), according to the parameter AllowUnclassifiedCalls. For a detailed description of the table's individual parameters and for configuring the table using the Web interface, see "Configuring Classification Table" on page 198. For a description on configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: SBC IP-to-IP Routing Table EMS: IP to IP Routing	
[IP2IPRouting]	<p>This <i>ini</i> file table parameter configures the SBC IP-to-IP Routing table for routing received SIP messages such as INVITE messages to an IP destination. The format of this parameter is as follows:</p> <pre>[IP2IPRouting] FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,</pre>

Parameter	Description
	<p>IP2IPRouting_RequestType, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID, IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort, IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions; [IP2IPRouting]</p> <p>For example: IP2IPRouting 1 = 1, *, *, *, *, 3, 0, -1, -1, , 0, -1, 0;</p> <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 specific routing rule to be effective, the matching characteristics must match. If no matching rule is located, the call is rejected. ▪ For a detailed description of the table's individual parameters and for configuring the table using the Web interface, see "Configuring SBC IP2IP Routing" on page 201. ▪ For a description on configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.
Web: SBC Alternative Routing Reasons Table EMS: Alternative Routing Reasons	
[SBCAlternativeRoutingReasons]	<p>This <i>ini</i> file table parameter configures the SBC Alternative Routing Reasons table. This table is used for alternative IP-to-IP routing (defined in the 'IP2IP Routing' table). If 4xx, 5xx, or 6xx SIP responses are received as a result of outgoing SIP dialog-initiating methods (e.g., INVITE, OPTIONS, and SUBSCRIBE messages), the device re-sends the messages (to an alternative route) if the response is defined in this table and if there are alternative routes configured in the 'IP2IP Routing' table.</p> <p>The format of this parameter is as follows:</p> <pre>[SBCAlternativeRoutingReasons] FORMAT SBCAlternativeRoutingReasons_Index = SBCAlternativeRoutingReasons_ReleaseCause; [\SBCAlternativeRoutingReasons]</pre> <p>For example: SBCAlternativeRoutingReasons 0 = 403; SBCAlternativeRoutingReasons 1 = 404;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table can include up to five indices (where 0 is the first index). ▪ For a description on configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

Parameter	Description
Web: IP to IP Inbound Manipulation Table EMS: IP to IP Inbound Manipulation	
[IPInboundManipulation]	<p>This <i>ini</i> file table parameter configures the IP to IP Inbound Manipulation table. This table allows you to manipulate the SIP URI user part (source and/or destination) of the inbound SIP dialog message. The format of this parameter is as follows:</p> <pre>[IPInboundManipulation] FORMAT IPInboundManipulation_Index = IPInboundManipulation_IsAdditionalManipulation, IPInboundManipulation_ManipulatedURI, IPInboundManipulation_ManipulationPurpose, IPInboundManipulation_SrcIPGroupID, IPInboundManipulation_SrcUsernamePrefix, IPInboundManipulation_SrcHost, IPInboundManipulation_DestUsernamePrefix, IPInboundManipulation_DestHost, IPInboundManipulation_RequestType, IPInboundManipulation_RemoveFromLeft, IPInboundManipulation_RemoveFromRight, IPInboundManipulation_LeaveFromRight, IPInboundManipulation_Prefix2Add, IPInboundManipulation_Suffix2Add; [IPInboundManipulation]</pre> <p>For example: IPInboundManipulation 1 = 0, 0, 0, -1, *, abc, *, *, 0, 0, 0, 255, , ;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table can include up to 100 indices. ▪ For SIP URI host name (source and destination) manipulations, you can also use the 'IP Group' table. These host names are simply replaced with the names configured for the Source and Destination IP Groups respectively. ▪ For a detailed description of the table's individual parameters and for configuring the table using the Web interface, see "Configuring IP-to-IP Inbound Manipulations" on page 210. ▪ For a description on configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

Parameter	Description
Web: IP to IP Outbound Manipulation Table EMS: IP to IP Outbound Manipulation	
[IPOutboundManipulation]	<p>This <i>ini</i> file table parameter configures the IP to IP Outbound Manipulation table. This table allows you to manipulate the SIP URI user part (source and/or destination) of the outbound SIP dialog message. The format of this parameter is as follows:</p> <pre>[IPOutboundManipulation] FORMAT IPOutboundManipulation_Index = IPOutboundManipulation_IsAdditionalManipulation, IPOutboundManipulation_ManipulatedURI, IPOutboundManipulation_SrcIPGroupID, IPOutboundManipulation_DestIPGroupID, IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost, IPOutboundManipulation_DestUsernamePrefix, IPOutboundManipulation_DestHost, IPOutboundManipulation_RequestType, IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight, IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add, IPOutboundManipulation_Suffix2Add, IPOutboundManipulation_PrivacyRestrictionMode; [IPOutboundManipulation]</pre> <p>For example: IPOutboundManipulation 1 = 0, 0, 2, -1, *, *, *, *, 1, 3, 0, 255, , , 0;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table can include up to 100 indices (where 0 is the first index). ▪ Manipulated destination SIP URI user names are done on the following SIP headers: Request URI, To, and Remote-Party-ID (if exists). Manipulated source SIP URI user names are done on the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists). ▪ For SIP URI host name (source and destination) manipulations, you can also use the 'IP Group' table. These host names are simply replaced with the names configured for the Source and Destination IP Groups respectively. ▪ For a detailed description of the table's individual parameters and for configuring the table using the Web interface, see "Configuring IP-to-IP Outbound Manipulations" on page 212. ▪ For a description on configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.14 Standalone Survivability Parameters

The Stand-alone Survivability (SAS) parameters are described in the table below.

Table 12-68: SAS Parameters

Parameter	Description
Web: Enable SAS EMS: Enable [EnableSAS]	<p>Enables the Stand-Alone Survivability (SAS) feature.</p> <ul style="list-style-type: none"> [0] Disable Disabled (default) [1] Enable = SAS is enabled <p>When enabled, the device receives the registration requests from different SIP entities in the local network and then forwards them to the defined proxy. If the connection to the proxy fails ('Emergency Mode'), the device serves as a proxy by allowing calls internal to the local network or outgoing to PSTN.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: SAS Local SIP UDP Port EMS: Local SIP UDP [SASLocalSIPUDPPort]	<p>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.</p>
Web: SAS Default Gateway IP EMS: Default Gateway IP [SASDefaultGatewayIP]	<p>The default gateway used in SAS 'Emergency Mode'. When an incoming SIP INVITE is received and the destination Address-Of-Record is not included in the SAS database, the request is immediately sent to this default gateway.</p> <p>The address can be configured as an IP address (dotted-decimal notation) or as a domain name (up to 49 characters). The default is a null string, which is interpreted as the local IP address of the gateway.</p>
Web: SAS Registration Time EMS: Registration Time [SASRegistrationTime]	<p>Determines the value of the SIP Expires header that is sent in a 200 OK response to an incoming REGISTER message when in SAS 'Emergency Mode'.</p> <p>The valid range is 0 (Analog) or 10 (Digital) to 2,000,000. The default value is 20.</p>
Web: SAS Local SIP TCP Port EMS: Local SIP TCP Port [SASLocalSIPTCPPort]	<p>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.</p>
Web: SAS Local SIP TLS Port EMS: Local SIP TLS Port [SASLocalSIPTLSPort]	<p>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.</p>
Web/EMS: Enable Record-Route [SASEnableRecordRoute]	<p>Determines whether the device's SAS application adds the SIP Record-Route header to SIP requests. This ensures that SIP messages traverse the device's SAS agent by including the SAS IP address in the Record-Route header.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable

Parameter	Description
	<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. The presence of this parameter indicates loose routing; the lack of 'lr' indicates strict routing. For example:</p> <ul style="list-style-type: none"> Loose routing: Record-Route: <sip:server10.biloxi.com;lr> Strict routing: Record-Route: <sip:bigbox3.site3.atlanta.com>
Web: SAS Proxy Set EMS: Proxy Set [SASProxySet]	<p>Determines the Proxy Set (index number) used in SAS Normal mode to forward REGISTER and INVITE requests from users that are served by the SAS application.</p> <p>The valid range is 0 to 5. The default value is 0 (i.e., default Proxy Set).</p>
Web: Redundant SAS Proxy Set EMS: Redundant Proxy Set [RedundantSASProxySet]	<p>Determines the Proxy Set (index number) used in SAS Emergency mode for fallback when the user is not found in the Registered Users database. Each time a new SIP request arrives, the SAS application checks whether the user is listed in the registration database. If the user is located in the database, the request is sent to the user. If the user is not found, the request is forwarded to the next redundant SAS defined in the Redundant SAS Proxy Set. If that SAS Proxy IP appears in the Via header of the request, it is not forwarded (thereby, preventing loops in the request's course). If no such redundant SAS exists, the SAS sends the request to its default gateway (configured by the parameter SASDefaultGatewayIP).</p> <p>The valid range is -1 to 5. The default value is -1 (i.e., no redundant Proxy Set).</p>
Web/EMS: SAS Block Unregistered Users [SASBlockUnRegUsers]	<p>Determines whether the device rejects SIP INVITE requests received from unregistered SAS users. This applies to SAS Normal and Emergency modes.</p> <ul style="list-style-type: none"> [0] Un-Block = Allow INVITE from unregistered SAS users (default). [1] Block = Reject dialog-establishment requests from unregistered SAS users.
[SASEnableContactReplace]	<p>Enables the device to change the SIP Contact header so that it points to the SAS host and therefore, the top-most SIP Via header and the Contact header point to the same host.</p> <ul style="list-style-type: none"> [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>

Parameter	Description
Web: SAS Survivability Mode EMS: Survivability Mode [SASSurvivabilityMode]	<p>Determines the Survivability mode used by the SAS application.</p> <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. ▪ [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>

Parameter	Description
[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 Registration Manipulation Table EMS: Stand-Alone Survivability	
[SASRegistrationManipulation]	<p>This <i>ini</i> file table parameter configures the SAS Registration Manipulation table. This table is used by the SAS application to manipulate the SIP Request-URI user part of incoming INVITE messages and of incoming REGISTER request AoR (To header), before saving it to the registered users database. The format of this table parameter is as follows:</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.</p> <p>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 "Configuring Stand-Alone Survivability" on page 216.

Parameter	Description
Web: SAS IP-to-IP Routing Table	
[IP2IPRouting]	<p>This <i>ini</i> file table parameter 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: IP2IPRouting 1 = -1, *, *, *, *, 0, -1, -1, , 0, -1, 0;</p> <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, see "Configuring IP2IP Routing Table (SAS)" on page 218. ▪ For a description on configuring <i>ini</i> file table parameters, see "Configuring ini File Table Parameters" on page 368.

12.15 IP Media Parameters

The IP media parameters are described in the table below.

Table 12-69: IP Media Parameters

Parameter	Description
Automatic Gain Control (AGC) Parameters	
Web: Enable AGC EMS: AGC Enable [EnableAGC]	<p>Activates 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 TelProfile parameter. ▪ For a description of AGC, see Automatic Gain Control (AGC) on page 646.
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 ▪ [22] 22 = 13.00 dB/sec ▪ [23] 23 = 14.00 dB/sec ▪ [24] 24 = 15.00 dB/sec

Parameter	Description
	<ul style="list-style-type: none"> ▪ [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]	<p>Determines the AGC direction.</p> <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]	<p>Determines 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.</p>
EMS: Minimal Gain [AGCMinGain]	<p>Defines the minimum gain (in dB) by the AGC when activated. The range is 0 to -31. The default is -20.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: Maximal Gain [AGCMaxGain]	<p>Defines the maximum gain (in dB) by the AGC when activated. The range is 0 to 18. The default is 15.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: Disable Fast Adaptation [AGCDisableFastAdaptation]	<p>Disables the AGC Fast Adaptation mode.</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>
Energy Detector Parameters	
Note: Currently, this feature is not supported.	
Enable Energy Detector [EnableEnergyDetector]	<p>Activates 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).</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Energy Detector Quality Factor [EnergyDetectorQualityFactor]	<p>Determines 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.</p>
Energy Detector Threshold [EnergyDetectorThreshold]	<p>Defines the Energy Detector's threshold. A signal below or above this threshold invokes an 'Above' or 'Below' event.</p> <p>The threshold is calculated as follows: $\text{Actual Threshold} = -44 \text{ dBm} + (\text{EnergyDetectorThreshold} * 6)$ The valid value range is 0 to 7. The default is 3 (i.e., -26 dBm).</p>

Parameter	Description
Pattern Detection Parameters Note: For an overview on the pattern detector feature for TDM tunneling, see DSP Pattern Detector on page 650.	
Web: Enable Pattern Detector [EnablePatternDetector]	Enables or disables the activation of the Pattern Detector (PD). Valid options include: <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default) ▪ [1] Enable = 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.

12.16 Auxiliary and Configuration Files Parameters

This subsection describes the device's auxiliary and configuration files parameters.

12.16.1 Auxiliary/Configuration File Name Parameters

The configuration files (i.e., auxiliary files) can be loaded to the device using the Web interface (see "Loading Auxiliary Files" on page 337). For loading these files using the *ini* file, you need to configure these files in the *ini* file and configured whether they must be stored in the non-volatile memory. The table below lists the *ini* file parameters associated with these auxiliary files. For a detailed description of the auxiliary files, see "Auxiliary Configuration Files" on page 393.

Table 12-70: 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>The name of the file containing the Call Progress Tones definitions. Refer to the <i>Product Reference Manual</i> for additional information on how to create and load this file.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web/EMS: Prerecorded Tones File [PrerecordedTonesFileName]	<p>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>
Web: CAS File EMS: Trunk Cas Table Index [CASFileName_x]	<p>CAS file name (e.g., 'E_M_WinkTable.dat') that defines the CAS protocol (where x denotes the CAS file ID 0 to 7). It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the device's trunks, using the parameter CASTableIndex or it can be associated per B-channel using the parameter CASChannelIndex.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>

Parameter	Description
Web: Dial Plan EMS: Dial Plan Name [CasTrunkDialPlanName_x]	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]	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]	The name (and path) of the file containing the User Information data.

12.16.2 Automatic Update Parameters

The automatic update of software and configuration files parameters are described in the table below.

Table 12-71: Automatic Update of Software and Configuration Files Parameters

Parameter	Description
General Automatic Update Parameters	
[AutoUpdateCmpFile]	<p>Enables or disables 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>Determines the number of minutes the device waits between automatic updates. The default value is 0 (i.e., the update at fixed intervals mechanism is disabled).</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[AutoUpdatePredefinedTime]	<p>Schedules an automatic update to a user-defined time of the day. 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

Parameter	Description
[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 IniFileUrl.</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.
Software/Configuration File URL Path for Automatic Update Parameters	
[CmpFileURL]	<p>Specifies the name of the <i>cmp</i> file and the path to the server (IP address or FQDN) from where the device loads a new <i>cmp</i> file and updates itself. The <i>cmp</i> file can be loaded using HTTP/HTTPS. 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>Specifies the name of the <i>ini</i> file and the path to the server (IP address or FQDN) on which it is located. The <i>ini</i> file can be loaded using HTTP/HTTPS. For example: <code>http://192.168.0.1/filename</code> <code>http://192.8.77.13/config<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 '<MAC>' 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.

Parameter	Description
[PrtFileURL]	<p>Specifies the name of the Prerecorded Tones file and the path to the server (IP address or FQDN) on which it is located. For example: http://server_name/file, https://server_name/file.</p> <p>Note: The maximum length of the URL address is 99 characters.</p>
[CptFileURL]	<p>Specifies the name of the CPT file and the path to the server (IP address or FQDN) on which it is located. For example: http://server_name/file, https://server_name/file.</p> <p>Note: The maximum length of the URL address is 99 characters.</p>
[CasFileURL]	<p>Specifies the name of the CAS 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.</p> <p>Note: The maximum length of the URL address is 99 characters.</p>
[TLSTrustFileUrl]	<p>Specifies the name of the TLS trusted root certificate file and the URL from where it's downloaded.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[TLSCertFileUrl]	<p>Specifies the name of the TLS certificate file and the URL from where it's downloaded.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[UserInfoFileURL]	<p>Specifies the name of the User Information file and the path to the server (IP address or FQDN) on which it is located. For example: http://server_name/file, https://server_name/file</p> <p>Note: The maximum length of the URL address is 99 characters.</p>

13 SIP Software Package

The table below lists the device's standard SIP software package.

Table 13-1: Software Package

File Name	Description
Firmware (RAM CMP) File	
MP500_MSBG_SIP_<sw ver.>.cmp	Image file containing the device's software
ini Configuration Files	
MP500_4fxs_4fxo.ini	Sample ini file for Mediant 800/4xFXS/4xFXO
MP500_12fxo.ini	Sample ini file for Mediant 800/12xFXO
usa_tones_xx.dat	Default loadable Call Progress Tones *.dat file
usa_tones_xx.ini	Call Progress Tones ini file (used to create *.dat file)
Miscellaneous Files	
SNMP MIBs	MIB library for SNMP browser
CAS Protocol Files	Used for various signaling types, such as E_M_WinkTable.dat
Utilities	
DConvert	TrunkPack Downloadable Conversion Utility - to create Call Progress Tones, Voice Prompts, and CAS files
ACSyslog	Syslog server
CPTWizard	Call Progress Tones Wizard
ISDN Trace Utility	Utility that is used to convert ISDN traces to textual form



Notes:

- The ini and Utility files are shipped with the device in CD format.
- The device is supplied with a cmp file pre-installed on its flash memory. Therefore, this file is not included on the supplied CD. However, if you are an AudioCodes registered customer, you can obtain the latest cmp version files (as well as documentation and other software such as the *ini* and MIB files, and Utilities) from AudioCodes Web site at www.audiocodes.com/downloads (customer registration is performed online at this Web site). If you are not a direct customer of AudioCodes, please contact the AudioCodes' Distributor and Reseller from whom this product was purchased.

Reader's Notes

14 Technical Specifications

The device's technical specifications are listed in the table below.

Table 14-1: Technical Specifications

Function	Specification
Interfaces	
PSTN	Capacity Voice interfaces: 8 analog PSTN interfaces, 4 FXS and 4 FXO The configuration is fixed and is not field upgradable or changeable Future support for up to 12 analog PSTN interfaces, 4 BRI ports and single E1/T1/J1 span module
Digital Interfaces* (Optional)	Single span E1/T1/ using RJ-48c connectors
Analog Interfaces (Optional)	4 ports FXO and 4 FXS ports using RJ-11 connectors Option of 1 FXS Lifeline ports in case of power failure FXS Loop Impedance: Up to 1,600 Ohms
BRI Interfaces* (Optional)	4 BRI ports (8 calls), network S/T interfaces. NT or TE termination
Networking Interfaces	
WAN (Optional)	WAN interface 10/100/1000 Base-T Copper Support for T1, SHDSL, ADSL2+* and Optical Gigabit Ethernet*
LAN	4 ports 10/100/1000Base-T and additional 8 10/100Base-TX ports, PoE- Power-Over Ethernet on all ports is optional (Compliant to 802.3af-2003 with auto-detection Up to 15.4W per port), PoE management
WiFi* (Optional)	WiFi Access Point support for 802.11 a/b/g/n
OSN Server Platform (Optional)	
Single Chassis Integration	Embedded, open Network Solution Platform for third-party services
CPU	Intel Atom 1.6 GHz
Memory	1G RAM
Storage	SATA storage
Media Processing	
Voice Coders	G.711, G.723.1, G.726, G.729A, and AMR-WB (G.722.2), G.722 Independent dynamic vocoder selection per channel
Echo Cancellation	G.165 and G.168-2002, with 32, 64 or 128 msec tail length
Quality Enhancement	Dynamic programmable jitter buffer, VAD, CNG
DTMF/MF Tones	Packet-side or PSTN-side detection and generation, RFC 2833 compliant DTMF relay and Call Progress tones Detection and Generation
IP Transport	VoIP (RTP/RTCP) per IETF RFC 3550 and 3551, IPv6 Supported
Fax Transport	T.38 compliant (real time fax), Automatic bypass to PCM

Function	Specification
Signaling	
Digital – PSTN Protocols	<ul style="list-style-type: none"> E1/T1: <ul style="list-style-type: none"> ✓ PRI: ETSI/Euro ISDN, ANSI NI2, 4/5ESS, DMS 100, QSIG (basic and supplementary), Japan INS1500, VN3, VN4, VN6, Australian Telecom, New Zealand Telecom, Hong Kong Variant, Korean Variant ✓ CAS: <ul style="list-style-type: none"> - T1 CAS (protocol type 2) (MF-R1\DTMF) – supports various variants supplied as state machine such as E&M family, E911CAMA, Loop\Ground Start - E1 MFCR2 (protocol type 7) – supports various countries supplied as state machine - E1 CAS (protocol type 8) (MF-R2\MF-R1\DTMF) – supports R2D variant supplied as state machine - E1\T1 RAW CAS (protocol type 3 and 9 accordingly) - Customized state machine BRI: 4 BRI ports (8 calls) with S/T interfaces. Supports Euro ISDN, QSIG, VN6 and NTT
Analog signaling	Loop Start FXS/FXO, Caller ID, polarity reversal, distinctive ringing, visual Message Waiting Indication
Data Routing (Optional)	
	<ul style="list-style-type: none"> DHCP/PPPoE/L2TP/PPTP client towards WAN; DHCP server towards LAN VLAN Layer 3 routing Internal layer 2 switching Static and dynamic routing (RIP1, RIP2, OSPF, BGP)
Control and Management	
Control Protocols	SIP-TCP, SIP-UDP, SIP-TLS and SIP-MSCML*, IPv6 Supported Standalone Survivability for service continuity
Operations & Management	<ul style="list-style-type: none"> AudioCodes' Element Management System Embedded HTTP Web Server, SNMP V2/V3 Remote configuration and software download via HTTP or HTTPS, RADIUS, Syslog (for events and alarms)
IP/VoIP Quality of Service	
	<ul style="list-style-type: none"> IEEE 802.1P, TOS, DiffServ labeling IEEE 802.1Q VLAN tagging RTCP-XR* (Extended Reports per RFC 3611) Shaping Policing, Queuing, Bandwidth Reservation (Optional)
Security	
Session Border Controller (SBC)	<ul style="list-style-type: none"> SIP Header conversion SIP Normalization Survivability IP-to-IP routing translations of various SIP transport types; UDP, TCP, TLS

Function	Specification
	<ul style="list-style-type: none"> ▪ Translation of RTP, SRTP* ▪ Support SIP trunk with multi-ITSP (Registrations to ITSPs is invoked independently) ▪ Topology hiding ▪ Call Admission Control ▪ Call Black/White list
Data Security (Optional)	<ul style="list-style-type: none"> ▪ IPsec ▪ ESP – Tunnel mode ▪ Encryption ▪ Authentication ▪ IKE mode – IPsec VPN ▪ IDS/IPS: <ul style="list-style-type: none"> ✓ Fragmented traffic ✓ Malformed Request ✓ Ping of Death ✓ Properly formed request from unauthenticated source ✓ DDoS attack ✓ SYN flood ▪ Stateful packet inspection firewall ▪ DMZ Host ▪ Port Triggering ▪ Packet Filtering ▪ Application Layer Gateway
Hardware Specifications	
Power Supply	Single universal power supply 100-240V 1.5A 50-60 Hz
Physical Dimensions	320mm x 345mm x 1U
Regulatory Compliance	
Safety and EMC Standards	UL60950-1, EN60950-1, CB certification including National deviations EN55024, EN55022 Class A, EN61000-3-2, EN61000-3-3, EN300 386, FCC 47 Part 15 Class A
Telecommunication Standards	TIA/EIA-IS-968, ETSI ES 203 021 (FXO interface)

*Future support.



User's Manual Ver. 6.2