

MGCP MP-1xx Series & MP-11x Series



User's Manual 4.6

Table of Contents

Introductory Information	12
1 Overview	13
1.1 Introduction	13
1.2 Gateway Description	13
1.3 MediaPack Features	15
1.3.1 General Features.....	15
1.3.2 MP-1xx Hardware Features.....	15
1.3.3 MP-11x Hardware Features	16
2 MediaPack Physical Description	17
2.1 MP-1xx Physical Description.....	17
2.1.1 MP-1xx Front Panel.....	17
2.1.2 MP-1xx Rear Panel.....	19
2.2 MP-11x Physical Description	22
2.2.1 MP-11x Front Panel.....	22
2.2.2 MP-11x Rear Panel	23
3 Installing the MediaPack	25
3.1 Installing the MP-1xx.....	25
3.1.1 Unpacking.....	25
3.1.2 Mounting the MP-1xx.....	26
3.1.3 Cabling the MP-1xx	30
3.2 Installing the MP-11x.....	35
3.2.1 Unpacking.....	35
3.2.2 Package Contents	35
3.2.3 19-inch Rack Installation Package	35
3.2.4 Mounting the MP-11x.....	36
3.2.5 Cabling the MP-11x	38
4 Getting Started	41
4.1 Assigning the MediaPack IP Address	41
4.1.1 Assigning an IP Address Using HTTP.....	41
4.1.2 Assigning an IP Address Using BootP	43
4.2 Restoring Networking Parameters to their Initial State	44
5 MediaPack Initialization & Configuration Files	45
5.1 Boot Firmware & Operational Firmware.....	45
5.2 MediaPack Startup.....	45
5.3 Using BootP/DHCP	46
5.3.1 BootP/DHCP Server Parameters	46
5.3.2 Host Name Support	48
5.3.3 Selective BootP	48
5.3.4 Vendor Specific Information	49
5.3.5 Microsoft™ DHCP/BootP Server.....	50
5.4 Configuration Parameters and Files.....	50
5.4.1 Initialization (ini) Files	51

5.4.2	Auxiliary Files.....	58
5.5	Backup Copies of ini and Auxiliary Files	75
5.6	Upgrading MediaPack Software.....	76
6	Standard Control Protocols	77
6.1	General	77
6.2	MGCP Control Protocol.....	77
6.2.1	MGCP Overview	77
6.2.2	MGCP Operation	77
6.2.3	Using DNS with MGCP.....	78
6.2.4	MGCP KeepAlive Mechanism	78
6.2.5	MediaPack Distinctive Ringing Mechanism.....	79
6.2.6	SDP Support in MGCP	79
6.2.7	MGCP FAX.....	80
6.2.8	Fax Transport Type Setting with Local Connection Options	85
6.2.9	MGCP Profiling	85
6.2.10	TGCP Compatibility	85
6.2.11	MGCP Coder Negotiation	86
6.2.12	Supported MGCP Packages	90
7	MediaPack Management.....	99
7.1	Using SNMP.....	99
7.1.1	About SNMP	99
7.1.2	Carrier-Grade Alarm System	101
7.1.3	Cold Start Trap	102
7.1.4	Performance Measurements for a Third-Party System	102
7.1.5	SNMP Interface Details	106
7.1.6	SNMP NAT Traversal	113
7.2	Administrative State Control.....	113
7.2.1	Node Maintenance.....	113
7.2.2	Graceful Shutdown	114
7.3	Embedded Web Server.....	114
7.3.1	Embedded Web Server Protection & Security Mechanisms	115
7.3.2	Limiting the Embedded Web Server to Read-Only Mode	116
7.3.3	Correlating PC / MediaPack IP Address & Subnet Mask.....	117
7.3.4	Accessing the Embedded Web Server.....	117
7.3.5	Accessing the Embedded Web Server.....	118
7.3.6	Using Internet Explorer to Access the Embedded Web Server.....	118
7.4	Getting Acquainted with the Web Interface.....	119
7.4.1	About the Web Interface Screen	119
7.4.2	Saving Changes	120
7.4.3	Protocol Management.....	122
7.4.4	Advanced Configuration Screen.....	127
7.4.5	Status and Diagnostic Menu.....	148
7.4.6	Software Update	155
7.4.7	Save Configuration	163
7.4.8	Reset Button.....	164
7.5	Restoring and Backing Up the Device Configuration	165
8	Diagnostics & Troubleshooting	167
8.1	Diagnostics Overview.....	167
8.2	Troubleshooting MediaPack Devices via the RS-232 Port	168
8.2.1	Viewing the Gateway's Information	168

8.2.2	Changing the Networking Parameters.....	168
8.2.3	Determining MediaPack Initialization Problems	169
8.2.4	Reinitializing the MediaPack.....	169
8.3	LED Indicators.....	172
8.3.1	MediaPack Front Panel LED Indicators.....	172
8.4	MediaPack Self-Testing	172
8.5	Syslog	173
8.5.1	Operating the Syslog Server	174
8.6	The Embedded Web Server's 'Message Log' (Integral Syslog).....	175
8.7	CommandShell - The Embedded CLI	175
8.8	Control Protocol Reports.....	176
8.8.1	MGCP Error Conditions.....	176
8.8.2	SNMP Traps	176
8.9	Solutions to Possible Problems.....	177
8.9.1	Solutions to Possible Voice Problems	177
8.9.2	Solutions to Possible General Problems	177
9	Selected Technical Specifications.....	179
9.1	MP-11x Specifications.....	179
9.2	MP-1xx Specifications.....	181
10	Appendix A - BootP/TFTP Server.....	185
10.1	Introduction	185
10.1.1	Key Features	185
10.1.2	Specifications.....	185
10.1.3	BootP/TFTP Server Installation	186
10.1.4	Logging Screen.....	186
10.1.5	Preferences Screen	187
10.1.6	Client Configuration Screen.....	187
10.1.7	Template Screen	188
10.2	Screen Details.....	188
10.2.1	Main Screen.....	188
10.2.2	Preferences Screen	190
10.2.3	Client Configuration Screen.....	191
10.2.4	Templates Screen.....	192
11	Appendix B - Individual <i>ini</i> File Parameters.....	195
11.1	Individual ini File Parameters	195
11.1.1	System Parameters	195
11.1.2	Infrastructure Parameters.....	199
11.1.3	Media Processing Parameters	205
11.1.4	Analog Parameters	214
11.1.5	Parameters Common to All Control Protocols.....	218
11.1.6	MGCP-Specific Parameters	223
11.1.7	SNMP Parameters.....	226

12 Appendix C - RTP/RTCP Payload Types	229
12.1 Payload Types Defined in RFC 3551	229
12.2 Payload Types Not Defined in RFC 3551	230
12.3 Default Dynamic Payload Types Which are Not Voice Coders.....	230
12.4 Default RTP/RTCP/T.38 Port Allocation	230
13 Appendix D - DTMF, Fax and Modem Transport Modes	233
13.1 DTMF/MF Relay Settings.....	233
13.2 Fax/Modem Settings	233
13.3 Configuring Fax Relay Mode.....	233
13.4 Configuring Fax/Modem ByPass Mode.....	234
13.5 Configuring Fax/Modem Bypass NSE mode.....	234
13.6 Supporting V.34 Faxes.....	235
13.6.1 Using Bypass Mechanism for V.34 Fax Transmission:.....	235
13.6.2 Using Events Only Mechanism for V.34 Fax Transmission	235
13.6.3 Using Relay Mode for Various Fax Machines (T.30 and V.34).....	236
14 Appendix E - Security	237
14.1 SSL/TLS.....	237
14.1.1 Web Server Configuration	237
14.1.2 Using the Secure Web Server	237
14.1.3 Secure Telnet	238
14.1.4 Server Certificate Replacement.....	238
14.1.5 Client Certificates.....	239
14.2 RADIUS Support.....	240
14.2.1 Setting Up a RADIUS Server.....	240
14.2.2 Configuring RADIUS Support.....	241
14.3 Network Port Usage	242
14.4 Recommended Practices	243
14.5 Legal Notice	244
15 Appendix F - Utilities.....	245
15.1 TrunkPack Downloadable Conversion Utility	245
15.1.1 Converting a CPT ini File to a Binary dat File.....	246
15.1.2 Generating Voice Prompts Files.....	247
15.1.3 Generating CAS Protocol Configuration Files	250
15.1.4 Generating Prerecorded Tones Files	252
15.2 MGCP Tester Utility	255
16 Appendix G - MGCP Compliance	257
16.1 MGCP Compliance Matrix.....	257
17 Appendix H - SNMP Traps	273
17.1 Alarm Traps.....	273
17.1.1 Component: Board#<n>	273
17.1.2 Component: AlarmManager#0	274
17.1.3 Component: EthernetLink#0.....	275

17.2	Log Traps (Notifications).....	276
17.3	Other Traps.....	277
17.4	Trap Varbinds.....	278
18	Appendix I - Customizing the Web Interface	279
18.1	Company & Product Bar Components.....	279
18.2	Replacing the Main Corporate Logo	280
18.2.1	Replacing the Main Corporate Logo with an Image File	280
18.2.2	Replacing the Main Corporate Logo with a Text String.....	282
18.3	Replacing the Background Image File	282
18.4	Customizing the Product Name	283
18.4.1	Customizing the Web Browser Title Bar.....	284
18.5	Modifying ini File Parameters via the Web Interface's AdminPage.....	284
19	Appendix J - Call Progress Tones Wizard	287
19.1	About this Software.....	287
19.2	Installation.....	287
19.3	Initial Settings.....	287
19.4	Recording Dialog – Automatic Mode.....	289
19.5	Recording Dialog – Manual Mode.....	291
19.6	The Call Progress Tone ini File.....	292
20	Appendix K - Regulatory Information.....	295
20.1	Appendix - Regulatory Information - MP-11x/FXS	295
20.2	Appendix - Regulatory Information - MP-1xx/FXO	298
20.3	Appendix - Regulatory Information - MP-1xx/FXS	301
20.4	Appendix - Regulatory Information - MP-124/FXS.....	303
21	List of Abbreviations.....	305
22	Index.....	309

List of Figures

Figure 1-1: Typical MediaPack VoIP Application	14
Figure 2-1: MP-108 Front Panel.....	17
Figure 2-2: MP-124 Front Panel.....	17
Figure 2-3: MP-104/FXS Rear Panel Connectors.....	19
Figure 2-4: MP-124 (FXS) Rear Panel Connectors	20
Figure 2-5: MP-118 Front Panel Connectors	22
Figure 2-6: MP-118 Rear Panel Connectors.....	23
Figure 3-1: Desktop or Shelf Mounting.....	27
Figure 3-2: MP-108 with Brackets for Rack Installation	28
Figure 3-3: MP-124 with Brackets for Rack Installation	29
Figure 3-4: MP-102 Wall Mount	30
Figure 3-5: RJ-45 Ethernet Connector Pinout.....	31
Figure 3-6: RJ-11 Phone Connector Pinout.....	31
Figure 3-7: 50-pin Telco Connector (MP-124/FXS only).....	31
Figure 3-8: MP-124 in a 19-inch Rack with MDF Adaptor.....	32
Figure 3-9: RS-232 Cable Wiring	33
Figure 3-10: Lifeline Splitter Pinout & RJ-11 Connector for MP-10x/FXS.....	33
Figure 3-11: MP-104/FXS Lifeline Setup.....	34
Figure 3-12: 19-inch Rack Shelf.....	36
Figure 3-13: View of the MP-11x Base.....	36
Figure 3-14: MP-11x Rack Mount	37
Figure 3-15: RJ-45 Ethernet Connector Pinout.....	38
Figure 3-16: RJ-11 Phone Connector Pinout	38
Figure 3-17: PS/2 Pinout.....	39
Figure 3-18: PS/2 to DB-9 Pinout.....	39
Figure 3-19: Lifeline Splitter Pinout & RJ-11 Connector	40
Figure 7-1: Enter Network Password Screen.....	118
Figure 7-2: Web Interface Screen - Example.....	119
Figure 7-3: Quick Setup Screen	121
Figure 7-4: Protocol Management Screen	122
Figure 7-5: Basic Configuration Screen (MGCP).....	124
Figure 7-6: General Parameters Screen (MGCP).....	125
Figure 7-7: Channel Configuration Screen (MGCP).....	126
Figure 7-8: Advanced Configuration Screen (MGCP).....	127
Figure 7-9: Network Settings Drop-Down Menu.....	128
Figure 7-10: Channel Settings Drop-Down Menu	128
Figure 7-11: Advanced Configuration Parameters Screen	129
Figure 7-12: IP Settings Screen	129
Figure 7-13: Application Settings Screen.....	130
Figure 7-14: SNMP Manager's Table Screen	131
Figure 7-15: Web & Telnet Access List Screen.....	132
Figure 7-16: Security Settings Screen.....	133
Figure 7-17: IPsec Table Screen (Existing Table Row).....	134
Figure 7-18: IPsec Table Screen (Non -Existing Table Row).....	135
Figure 7-19: IKE Table Screen (Existing Table Row)	136
Figure 7-20: IKE Table Screen (Non -Existing Table Row).....	137
Figure 7-21: RTP Settings Screen (Network Settings).....	138
Figure 7-22: Routing Table Screen	138
Figure 7-23: Ethernet Port Information Screen	139
Figure 7-24: VLAN Settings Screen	140
Figure 7-25: Voice Settings Screen.....	141
Figure 7-26: Fax/Modem/CID Settings Screen	142
Figure 7-27: RTP Settings Screen (Channel Settings).....	143
Figure 7-28: Hook-Flash Settings Screen	143
Figure 7-29: Configuration File Screen	144
Figure 7-30: Regional Settings Screen	145

Figure 7-31: Change Password Screen - For Users with Administrator Privileges.....	147
Figure 7-32: Change Password Screen - For Users with Monitoring Privileges	147
Figure 7-33: Status and Diagnostic Menu Screen	148
Figure 7-34: Channel Status Screen - FXO	149
Figure 7-35: Channel Status Screen - FXS.....	149
Figure 7-36: Channel Status Screen.....	151
Figure 7-37: RTP/RTCP Settings Screen.....	151
Figure 7-38: Fax & Modem Settings Screen	151
Figure 7-39: Transport Settings Screen	152
Figure 7-40: Voice Settings Screen.....	152
Figure 7-41: IBS Detector Settings Screen	152
Figure 7-42: Jitter Buffer Settings Screen	152
Figure 7-43: IPmedia Settings Screen	153
Figure 7-44: Message Log Screen	154
Figure 7-45: Versions Screen.....	155
Figure 7-46: Start Software Upgrade Screen	156
Figure 7-47: Start Software Upgrade Screen	157
Figure 7-48: Load CMP File Dialog Screen.....	158
Figure 7-49: File Loading Dialog Screen.....	159
Figure 7-50: File Loading Dialog Screen - CPT Type Displayed	160
Figure 7-51: End of Process Dialog Screen	161
Figure 7-52: Auxiliary Files Download Screen	162
Figure 7-53: Auxiliary Files Download Screen	163
Figure 7-54: Save Configuration Dialog Screen.....	164
Figure 7-55: Reset Screen	165
Figure 8-1: BootP/TFTP Server Main Screen	170
Figure 8-2: Client Configuration	170
Figure 8-3: Preferences Screen	171
Figure 8-4: BootP/TFTP Server - Client Found	172
Figure 8-5: AC Syslog	173
Figure 8-6: Setting the Syslog Server IP Address.....	174
Figure 10-1: Main Screen.....	188
Figure 10-2: Preferences Screen	190
Figure 10-3: Client Configuration Screen.....	191
Figure 10-4: Templates Screen.....	192
Figure 15-1: Downloadable Conversion Utility Opening Screen.....	245
Figure 15-2: Call Progress Tones Screen	246
Figure 15-3: Voice Prompts Screen	247
Figure 15-4: Select Files Window.....	248
Figure 15-5: File Data Window.....	249
Figure 15-6: Call Associated Signaling (CAS) Screen.....	251
Figure 15-7: Prerecorded Tones File(s) Screen.....	252
Figure 15-8: Prerecorded Tones File(s) Screen with wav Files	253
Figure 15-9: File Data Dialog Box	253
Figure 15-10: Encoded ini File(s) Screen.....	254
Figure 18-1: Customized Web Interface Title Bar	279
Figure 18-2: Logo Image Download Screen.....	280
Figure 18-3: Default Web Browser Title Bar.....	284
Figure 18-4: ini Parameters Screen	285
Figure 19-1: Initial Settings Dialog	288
Figure 19-2: Recording Dialog	289
Figure 19-3: Recording Dialog after Automatic Detection.....	290
Figure 19-4: Recording Dialog in Manual Mode.....	291
Figure 19-5: Call Progress Tone Properties.....	292
Figure 19-6: Call Progress Tone Database Matches	293
Figure 19-7: Full PBX/Country Database Match	293

List of Tables

Table 2-1: Front Panel Buttons on the MP-1xx	18
Table 2-2: Indicator LEDs on the MP-1xx Front Panel.....	18
Table 2-3: MP-10x Rear Panel Component Descriptions	19
Table 2-4: Indicator LEDs on the MP-10x Rear Panel	19
Table 2-5: MP-124 Rear Panel Component Descriptions	20
Table 2-6: Indicator LEDs on the MP-124 Rear Panel.....	20
Table 2-7: Definition of MP-11x Front Panel LED Indicators	22
Table 2-8: MP-11x Rear Panel Component Descriptions	23
Table 3-1: Cables and Cabling Procedure	30
Table 3-2: Pin Allocation in the 50-pin Telco Connector	32
Table 3-3: MP-104/FXS Lifeline Setup Component Descriptions	34
Table 3-4: View of the MP-11x Base.....	36
Table 3-5: MP-11x Rack Mount.....	37
Table 3-6: Cables and Cabling Procedure	38
Table 4-1: MediaPack Default Networking Parameters	41
Table 5-1: Command Line Switch Descriptions	47
Table 5-2: Vendor Specific Information Field	49
Table 5-3: Vendor Specific Information Fields	50
Table 5-4: Table of Parameter Values Example - Remote Management Connections	54
Table 5-5: Table of Parameter Values Example - Port-to-Port Connections	54
Table 5-6: Call Progress Tones.....	64
Table 5-7: Number Of Distinctive Ringing Patterns	67
Table 6-1: MGCP fax package Loose Mode MP-118	80
Table 6-2: Fax Transport Type.....	85
Table 6-3: MGCP Mapping of Payload Numbers to Coders	87
Table 6-4: Generic Media Package - G.....	90
Table 6-5: DTMF Package - D	90
Table 6-6: Line Package - L	91
Table 6-7: Handset Emulation Package - H.....	92
Table 6-8: PacketCable (NCS) Line Package - L.....	93
Table 6-9: Generic Media Package - G	94
Table 6-10: RTP Package - R	95
Table 6-11: Fax Package Definition - FXR.....	97
Table 6-12: Extended Line Package - XL.....	97
Table 7-1: Default IP Address and Subnet Mask	117
Table 7-2: Channel Status Color Indicator Key	150
Table 8-1: Possible Initialization Problems.....	169
Table 8-2: Solutions to Possible Voice Problems	177
Table 8-3: Solutions to Possible General Problems.....	177
Table 9-1: MP-11x Functional Specifications (continues on pages 179 to 180).....	179
Table 9-2: MP-1xx Selected Technical Specifications (continues on pages 181 to 183)	181
Table 11-1: System Parameters.....	196
Table 11-2: Infrastructure Parameters	199
Table 11-3: Media Processing Parameters	205
Table 11-4: Analog Parameters	214
Table 11-5: Common Control Parameters	218
Table 11-6: MGCP Specific Parameters	223
Table 11-7: SNMP Parameters	226
Table 12-1: Payload Types Defined in RFC 3551.....	229
Table 12-2: Payload Types Not Defined in RFC 3551	230
Table 12-3: Payload Types Not Defined in RFC 3551	230
Table 12-4: Default RTP/RTCP/T.38 Port Allocation	231
Table 13-1: V.34 Fax to V.34 Fax - Bypass Mode	235
Table 13-2: V.34 Fax to V.34 Fax - Events Only Mode.....	236
Table 13-3: V.34 Fax to V.34 Fax - Relay Mode.....	236

Table 14-1: Default TCP/UDP Network Port Numbers	242
Table 16-1: MGCP Compliance Matrix.....	257
Table 17-1: acBoardFatalError Alarm Trap	273
Table 17-2: acBoardEvResettingBoard Alarm Trap	274
Table 17-3: acActiveAlarmTableOverflow Alarm Trap	274
Table 17-4: acBoardEthernetLinkAlarm Alarm Trap	275
Table 17-5: acKeepAlive Log Trap	276
Table 17-6: acPerformanceMonitoringThresholdCrossing Log Trap	277
Table 17-7: coldStart Trap.....	277
Table 17-8: authenticationFailure Trap	277
Table 17-9: acBoardEvBoardStarted Trap.....	278
Table 18-1: Customizable Logo ini File Parameters for the Image File	281
Table 18-2: Customizable Logo ini File Parameters for the String Text	282
Table 18-3: Customizable Background ini File Parameters	283
Table 18-4: Customizable Product Name ini File Parameters	284
Table 21-1: List of Abbreviations.....	305

Introductory Information

Notice

This User's Manual describes the installation and use of the MediaPack MP-11x and MP-1xx AudioCodes analog Media Gateways having similar functionality except for the number of channels. MP-11x refers collectively to MP-118 8-port, MP-114 4-port and MP-112 2-port Media Gateways. MP-1xx refers collectively to MP-124 24-port, MP-108 8-port, MP-104 4-port and MP-102 2-port Media Gateways

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered Technical Support customers at <http://www.audiocodes.com> under Support / Product Documentation.

© 2005 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: July 20, 2005

Date Printed: July 21, 2005

Note: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press the **Alt** and **◀** keys.

Trademarks

AC logo, Ardito, AudioCoded, AudioCodes, AudioCodes logo, IPmedia, Mediant, MediaPack, MP-MLQ, NetCoder, Stretto, TrunkPack, VoicePacketizer and VoIPerfect, are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners.

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 <mailto:support@audiocodes.com>.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used. Only industry-standard terms are used throughout this manual. Hexadecimal notation is indicated by 0x preceding the number.

Related Documentation

Document #	Manual Name
LTRT-840xx	VoPLib API Reference Manual
LTRT-61603	MP Series Release Notes Ver 4.6.doc

1 Overview

1.1 Introduction

This document provides you with the information on installation, configuration and operation of the two MediaPack Series of VoIP analog Media Gateways.

The **MP-1xx** Series refers collectively to MP-124 24-port, MP-108 8-port, MP-104 4-port, MP-102 2-port, MP-118 8-port, MP-114 4-port and MP-112 2-port analog Media Gateways.

The **MP-11x** Series refers collectively to MP-118 8-port, MP-114 4-port and MP-112 2-port analog Media Gateways.

As these units have similar functionality, except for the number of channels and some minor features, they are referred to collectively as the MediaPack.

Prior knowledge of regular telephony and data networking concepts is preferred.

1.2 Gateway Description

The MediaPack series of analog VoIP gateways are cost-effective, cutting edge technology products. These stand-alone analog VoIP gateways provide superior voice technology for connecting legacy telephones, fax machines and PBX systems with IP-based telephony networks, as well as for integration with new IP-based PBX architecture. These products are designed and tested to be fully interoperable with leading softswitches and SIP servers.

The MediaPack gateways incorporate up to 24 analog ports for connection, either directly to an enterprise PBX (FXO), to phones, or to fax (FXS), supporting up to 24 simultaneous VoIP calls.

Additionally, the MediaPack units are equipped with a 10/100 Base-TX Ethernet port for connection to the network.

The MediaPack gateways are best suited for small to medium size enterprises, branch offices or for residential media gateway solutions.

The MediaPack gateways enable users to make free local or international telephone / fax calls between the distributed company offices, using their existing telephones / fax. These calls are routed over the existing network ensuring that voice traffic uses minimum bandwidth.

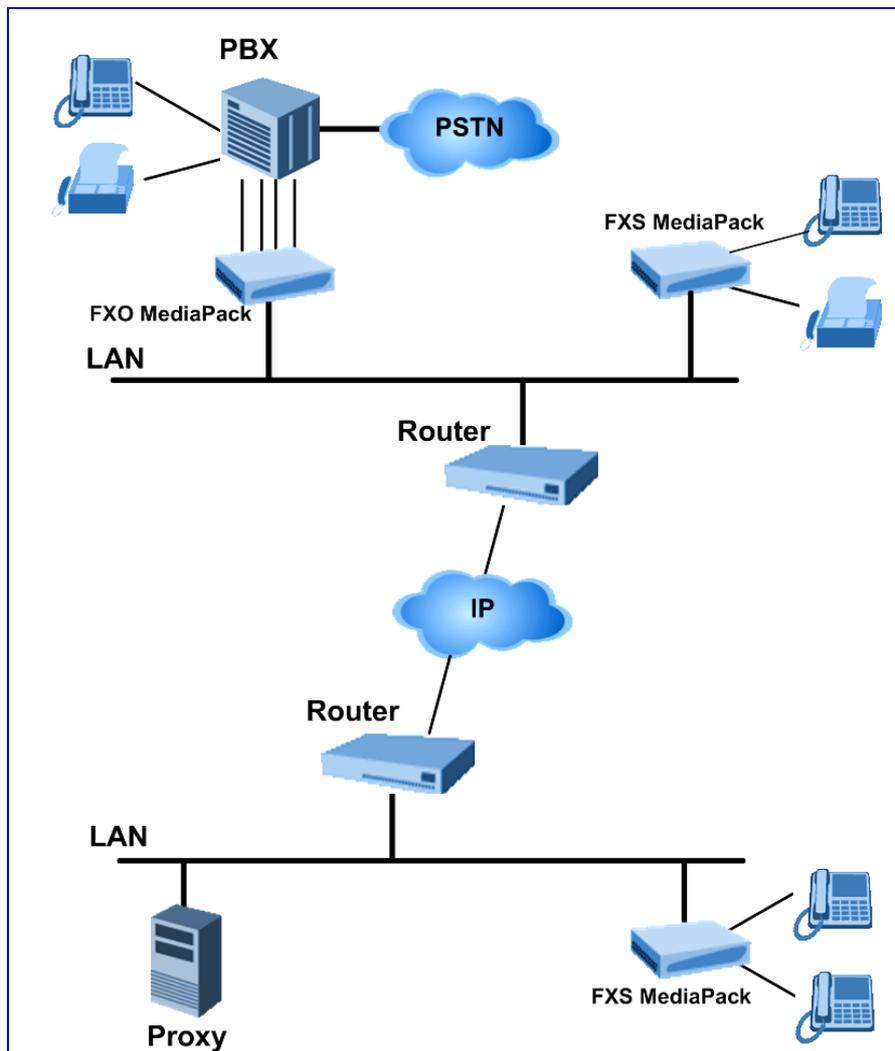
The MediaPack gateways are very compact devices that can be installed as a desk-top unit or on the wall or in a 19-inch rack.

The MediaPack gateways support SIP (Session Initiation Protocol) protocol, enabling the deployment of "voice over IP" solutions in environments where each enterprise or residential location is provided with a simple media gateway.

This provides the enterprise with a telephone connection (e.g., RJ-11), and the capability to transmit the voice and telephony signals over a packet network.

The layout diagram (Figure 1-1), illustrates a typical MediaPack VoIP application.

Figure 1-1: Typical MediaPack VoIP Application



1.3 MediaPack Features

This section provides a high-level overview of some of the many MediaPack supported features.

1.3.1 General Features

- Superior, high quality Voice, Data and fax over IP networks.
- Toll quality voice compression.
- Enhanced capabilities including MWI, long haul, metering, CID and out door protection.
- Proven integration with leading PBXs, IP-PBXs, Softswitches and SIP servers.
- Spans a range of 2 to 24 FXS/FXO analog ports.
- Selectable G.711 or multiple Low Bit Rate (LBR) coders per channel.
- T.38 fax with superior performance (handling a round-trip delay of up to nine seconds).
- Echo Canceled, Jitter Buffer, Voice Activity Detection (VAD) and Comfort Noise Generation (CNG) support.
- Comprehensive support for supplementary services.
- Web Management for easy configuration and installation.
- EMS for comprehensive management operations (FCAPS).
- Simple Network Management Protocol (SNMP) and Syslog support.
- SMDI support for Voice Mail applications.
- Multiplexes RTP streams from several users together to reduce bandwidth overhead.
- T.38 fax fallback to PCM (or NSE).
- Can be integrated into a VLAN-aware environment.
- Capable of automatically updating its firmware version and configuration.
- Secured SIP Signaling (SIPS), Web access (HTTPS) and Telnet access using SSL / TLS.

1.3.2 MP-1xx Hardware Features

- MP-124 19-inch, 1 U rugged enclosure provides up to 24 analog FXS ports, using a single 50 pin Telco connector.
- MP-10x compact, rugged enclosure only one-half of a 19-inch rack unit, 1 U high (1.75" or 44.5 mm).
- Lifeline - provides a wired phone connection to PSTN line when there is no power, or the network fails (applies to MP-10x FXS gateways).
- LEDs on the front and rear panels that provide information on the operating status of the media gateway and the network interface.
- Restart button on the Front panel that restarts the MP-1xx gateway, and is also used

to restore the MP-1xx parameters to their factory default values.

1.3.3 MP-11x Hardware Features

- MP-11x compact, rugged enclosure only one-half of a 19-inch rack unit, 1 U high.
- Lifeline - provides a wired phone connection to PSTN line when there is no power, or the network fails.
- LEDs on the front panel that provide information on the operating status of the media gateway and the network interface.
- Restart button on the back panel that restarts the MP-11x gateway, and is also used to restore the MP-11x parameters to their factory default values.

2 MediaPack Physical Description

This section provides detailed information on the hardware, the location and functionality of the LEDs, buttons and connectors on the front and rear panels of the MP-1xx (refer to Section 2.1 below) and MP-11x (Section 2.2 on page 22) gateways.

For detailed information on installing the MediaPack, refer to Section 3 on page 25.

2.1 MP-1xx Physical Description

2.1.1 MP-1xx Front Panel

Figure 2-1 and Figure 2-2 illustrate the front layout of the MP-108 (almost identical on MP-104 and MP-102) and MP-124 respectively. Refer to Section 2.1.1.1 for meaning of the front panel buttons; refer to Section 2.1.1.2 for functionality of the front panel LEDs.

Figure 2-1: MP-108 Front Panel

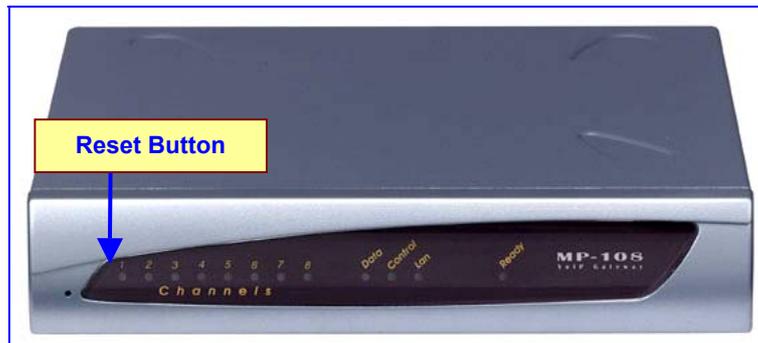


Figure 2-2: MP-124 Front Panel



2.1.1.1 MP-1xx Front Panel Buttons

Table 2-1 lists and describes the front panel buttons on the MP-1xx.

Table 2-1: Front Panel Buttons on the MP-1xx

Type	Function	Comment
Reset button	Reset the MP-1xx	Press the reset button with a paper clip or any other similar pointed object, until the gateway is reset.
	Restore the MP-1xx parameters to their factory default values	Refer to Section 4.2 on page 44.

2.1.1.2 MP-1xx Front Panel LEDs

Table 2-2 lists and describes the front panel LEDs on the MP-1xx.



Note: MP-1xx (FXS/FXO) media gateways feature almost identical front panel LEDs; they only differ in the number of channel LEDs that correspond to the number of channels.

Table 2-2: Indicator LEDs on the MP-1xx Front Panel

Label	Type	Color	State	Function
Ready	Device Status	Green	ON	Device Powered, self-test OK
		Orange	Blinking	Software Loading/Initialization
		Red	ON	Malfunction
LAN	Ethernet Link Status	Green	ON	Valid 10/100 Base-TX Ethernet connection
		Red	ON	Malfunction
Control	Control Link	Green	Blinking	Sending and receiving SIP messages
		Blank		No traffic
Data	Packet Status	Green	Blinking	Transmitting RTP (Real-Time Transport Protocol) Packets
		Red	Blinking	Receiving RTP Packets
		Blank	-	No traffic
Channels	Telephone Interface	Green	ON	Offhook / Ringing for FXS Phone Port FXO Line-Seize/Ringing State for Line Port
		Green	Blinking	There's an incoming call, before answering
		Red	ON	Line Malfunction
		Blank	-	Normal

2.1.2 MP-1xx Rear Panel

2.1.2.1 MP-10x Rear Panel

Figure 2-3 illustrates the rear panel layout of the MP-104. For descriptions of the MP-10x rear panel components, refer to Table 2-3. For the functionality of the MP-10x rear panel LEDs, refer to Table 2-4.



Tip 1: MP-10x (FXS/FXO) media gateways feature almost identical rear panel connectors and LEDs, located slightly differently from one device to the next.

Tip 2: The RJ-45 port (Eth 1) on the MP-10x/FXO rear panel is inverted on the MP-1xx/FXS. The label on the rear panel also distinguishes FXS from FXO devices.

Figure 2-3: MP-104/FXS Rear Panel Connectors

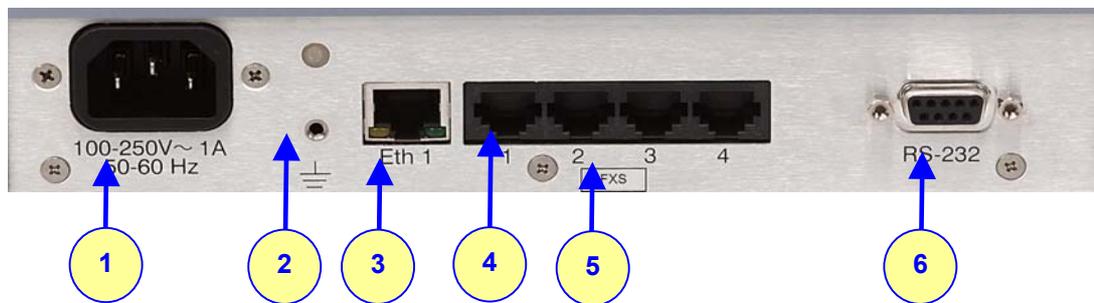


Table 2-3: MP-10x Rear Panel Component Descriptions

Item #	Label	Component Description
1	100-250V ~ 1A 50-60 Hz	AC power supply socket.
2		Protective earthing screw (mandatory for all installations).
3	Eth 1	10/100 Base-TX Ethernet connection.
4	-	2, 4 or 8 FXS/FXO ports.
5	FXS or FXO	To distinguish between FXS & FXO devices.
6	RS-232	9-pin RS-232 status port (for Cable Wiring of the RS-232 refer to Figure 3-9 on page 33).

Table 2-4: Indicator LEDs on the MP-10x Rear Panel

Label	Type	Color	State	Meaning
ETH-1	Ethernet Status	Yellow	ON	Ethernet port receiving data
		Red	ON	Collision

Note that the Ethernet LEDs are located within the RJ-45 socket.

2.1.2.2 MP-124 Rear Panel

Figure 2-4 illustrates the rear panel layout of the MP-124. For descriptions of the MP-124 rear panel components, refer to Table 2-5. For the functionality of the MP-124 rear panel LEDs, refer to Table 2-6.

Figure 2-4: MP-124 (FXS) Rear Panel Connectors

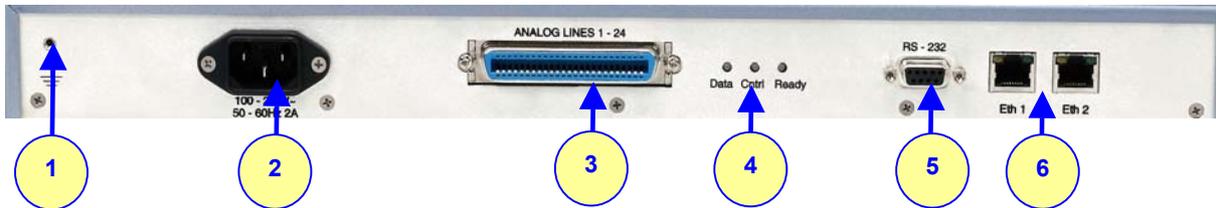


Table 2-5: MP-124 Rear Panel Component Descriptions

Item #	Label	Component Description
1		Protective earthing screw (mandatory for all installations).
2	100-250 V~ 50 - 60 Hz 2A	AC power supply socket.
3	ANALOG LINES 1 –24	50-pin Telco for 1 to 24 analog lines.
4	Data Cntrl Ready	LED indicators (described in Table 2-6).
5	RS-232	9-pin RS-232 status port (for Cable Wiring of the RS-232 refer to Figure 3-9 on page 33).
6	Eth 1 Eth 2	Dual 10/100 Base-TX Ethernet connections.



Note: The Dual In-line Package (DIP) switch, located on the MP-124 rear panel (supplied with some of the units), is not functional and should **not** be used.

The Ethernet LEDs are located within each of the RJ-45 sockets.

Note that on the MP-124 the rear panel also duplicates the Data, Control and Ready LEDs from the front panel.

Table 2-6: Indicator LEDs on the MP-124 Rear Panel

Label	Type	Color	State	Function
Data	Packet Status	Green	ON	Transmitting RTP Packets
		Red	ON	Receiving RTP Packets
		Blank		No traffic
Cntrl	Control Link	Green	Blinking	Sending and receiving H.323 messages
		Blank		No traffic
Ready	Device Status	Green	ON	Device Powered and Self-test OK
		Orange	ON	Software Loading/Initialization
		Red	ON	Malfunction
Eth 1	Ethernet Status	Green	ON	Valid 10/100 Base-TX Ethernet connection
		Red	ON	Malfunction
Eth 2	Ethernet Status	Green	ON	Valid 10/100 Base-TX Ethernet connection

Label	Type	Color	State	Function
		Red	ON	Malfunction

2.2 MP-11x Physical Description

2.2.1 MP-11x Front Panel

Figure 2-5 illustrates the front layout of the MP-118 (similar on MP-114 and MP-112 except for numbers of channels). Table 2-7 lists and describes the front panel LEDs on the MP-11x.



Tip: MP-11x gateways feature almost identical front panel LEDs; they only differ in the number of channel LEDs that correspond to the number of channels.

Figure 2-5: MP-118 Front Panel Connectors

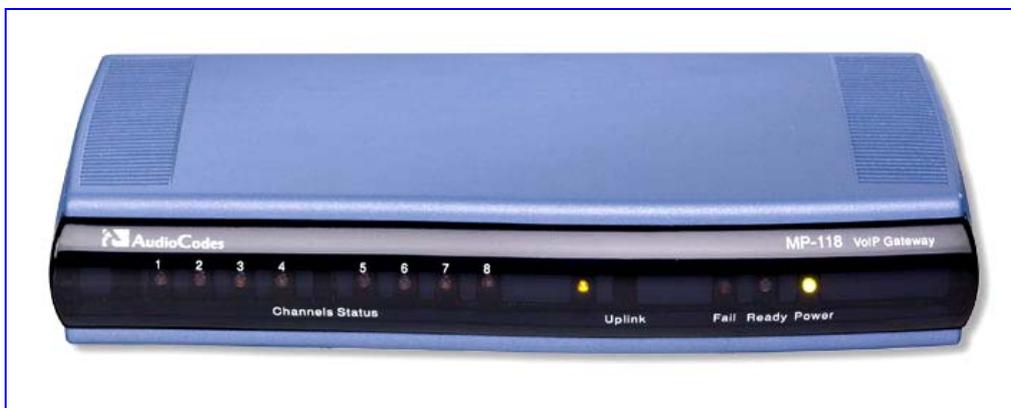


Table 2-7: Definition of MP-11x Front Panel LED Indicators

LED	Type	Color	State	Definition
Channels Status	Telephone Interface	Green	Blinking	The phone is ringing (incoming call, before answering).
			Fast Blinking	Line malfunction
			On	Offhook
			Off	Normal onhook position
Uplink	Ethernet Link Status	Green	On	Valid 10/100 Base-TX Ethernet connection
			Off	No uplink
Fail	Failure Indication	Red	On	Failure (fatal error). Or system initialization.
			Off	Normal working condition
Ready	Device Status	Green	On	Device powered, self-test OK
			Off	Software loading or System failure
Power	Power Supply Status	Green	On	Power is currently being supplied to the device
			Off	Either there's a failure / disruption in the AC power supply or power is currently not being supplied to the device through the AC power supply entry.

2.2.2 MP-11x Rear Panel

Figure 2-6 illustrates the rear layout of the MP-118 (almost identical on MP-114 and MP-112). Table 2-8 lists and describes the rear panel connectors and button on the MP-11x.

Figure 2-6: MP-118 Rear Panel Connectors

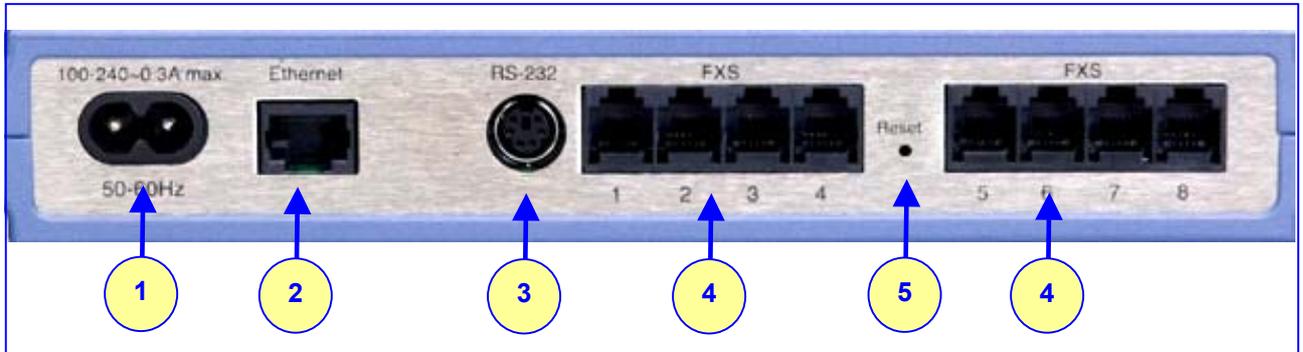


Table 2-8: MP-11x Rear Panel Component Descriptions

Item #	Label	Component Description
1	100-240~0.3A max.	AC power supply socket
2	Ethernet	10/100 Base-TX Uplink port
3	RS-232	RS-232 status port (requires a DB-9 to PS/2 adaptor)
4	FXS	4 RJ-11 FXS ports (total 8)
5	Reset	Reset button

Reader's Notes

3 Installing the MediaPack

This section provides information on the installation procedure for the MP-1xx (refer to Section 3.1 below) and the MP-11x (refer to Section 3.2 on page 35). For information on how to start using the gateway, refer to Section 4 on page 41.



Caution Electrical Shock

The equipment must only be installed or serviced by qualified service personnel.

3.1 Installing the MP-1xx

➤ To install the MP-1xx, take these 4 steps:

1. Unpack the MP-1xx (refer to Section 3.1.1 below).
2. Check the package contents (refer to Section 3.1.1.1 below).
3. Mount the MP-1xx (refer to Section 3.1.2 on page 26).
4. Cable the MP-1xx (refer to Section 3.1.3 on page 30).

After connecting the MP-1xx to the power source, the Ready and LAN LEDs on the front panel turn to green (after a self-testing period of about 1 minute). Any malfunction changes the Ready LED to red.

When you have completed the above relevant sections you are then ready to start configuring the gateway (Section 4 on page 41).

3.1.1 Unpacking

➤ To unpack the MP-1xx, take these 6 steps:

1. Open the carton and remove packing materials.
2. Remove the MP-1xx gateway from the carton.
3. Check that there is no equipment damage.
4. Check, retain and process any documents.
5. Notify AudioCodes or your local supplier of any damage or discrepancies.
6. Retain any diskettes or CDs.

3.1.1.1 Package Contents

Ensure that in addition to the MP-1xx, the package contains:

- AC power cable for the AC power supply option.
- 3 brackets (2 short, 1 long) and bracket-to-device screws for 19-inch rack installation option (MP-10x only).
- 2 short equal-length brackets and bracket-to-device screws for MP-124 19-inch rack

installation.

- Lifeline cable (RJ-11 adaptor cable for 1 to 2). Supplied with MP-10x/FXS only, by special order.
- A CD with software and documentation may be included.
- The MP-1xx Fast Track Installation Guide.

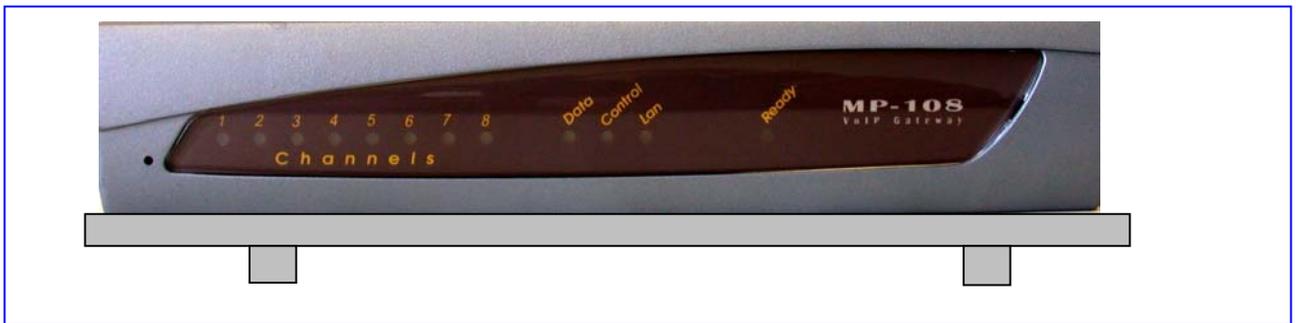
3.1.2 Mounting the MP-1xx

The MP-1xx can be mounted on a desktop or on a wall (only MP-10x), or installed in a standard 19-inch rack. Refer to Section 3.1.3 on page 30 for cabling the MP-1xx.

3.1.2.1 Mounting the MP-1xx on a Desktop

No brackets are required. Simply place the MP-1xx on the desktop in the position you require.

Figure 3-1: Desktop or Shelf Mounting



Rack Mount Safety Instructions (UL)

When installing the chassis in a rack, be sure to implement the following Safety instructions recommended by Underwriters Laboratories:



- **Elevated Operating Ambient** - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T_{ma}) specified by the manufacturer.
- **Reduced Air Flow** - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation on the equipment is not compromised.
- **Mechanical Loading** - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- **Circuit Overloading** - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing** - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g., use of power strips.)

3.1.2.2 Installing the MP-10x in a 19-inch Rack

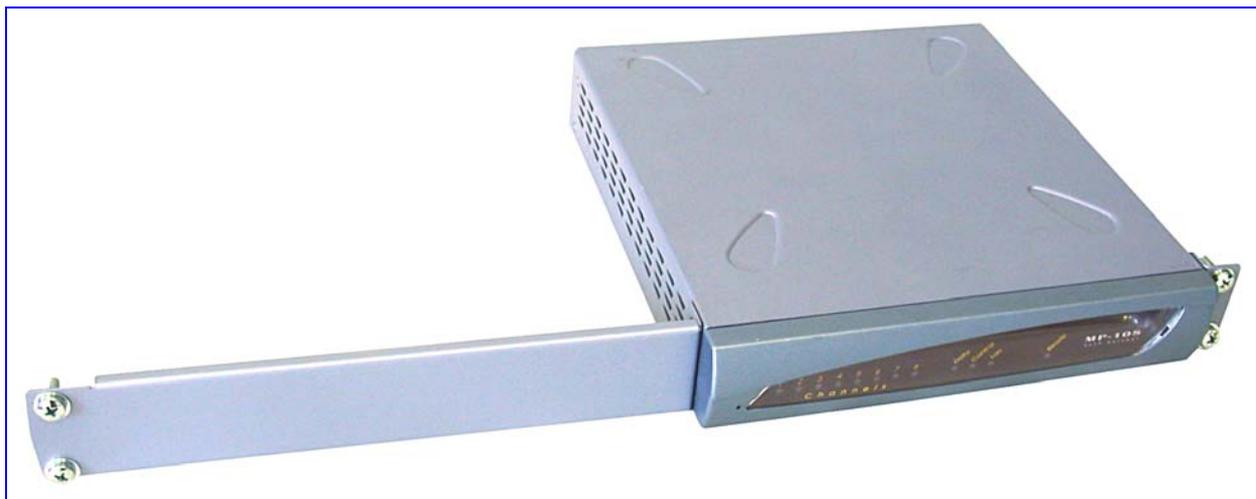
The MP-10x is installed into a standard 19-inch rack by the addition of two supplied brackets (1 short, 1 long). The MP-108 with brackets for rack installation is shown in [Figure 3-2](#).

➤ To install the MP-10x in a 19-inch rack, take these 9 steps:

1. Remove the two screws on one side of the device nearest the front panel.
2. Insert the peg on the short bracket into the third air vent down on the column of air vents nearest the front panel.
3. Swivel the bracket until the holes in the bracket line up with the two empty screw holes on the device.
4. Use the screws found in the devices' package to attach the short bracket to the side of the device.
5. Remove the two screws on the other side of the device nearest the front panel.

6. Position the long bracket so that the holes in the bracket line up with the two empty screw holes on the device.
7. Use the screws found in the device's package to attach the long bracket to the side of the device.
8. Position the device in the rack and line up the bracket holes with the rack frame holes.
9. Use four standard rack screws to attach the device to the rack. These screws are not provided with the device.

Figure 3-2: MP-108 with Brackets for Rack Installation



3.1.2.3 Installing the MP-124 in a 19-inch Rack

The MP-124 is installed into a standard 19-inch rack by the addition of two short (equal-length) supplied brackets. The MP-124 with brackets for rack installation is shown in [Figure 3-3](#).

➤ **To install the MP-124 in a 19-inch rack, take these 7 steps:**

1. Remove the two screws on one side of the device nearest the front panel.
2. Insert the peg on one of the brackets into the third air vent down on the column of air vents nearest the front panel.
3. Swivel the bracket until the holes in the bracket line up with the two empty screw holes on the device.
4. Use the screws found in the devices' package to attach the bracket to the side of the device.
5. Repeat steps 1 to 4 to attach the second bracket to the other side of the device.
6. Position the device in the rack and line up the bracket holes with the rack frame holes.
7. Use four standard rack screws to attach the device to the rack. These screws are not provided with the device.

Figure 3-3: MP-124 with Brackets for Rack Installation

3.1.2.4 Mounting the MP-10x on a Wall

The MP-10x is mounted on a wall by the addition of two short (equal-length) supplied brackets. The MP-102 with brackets for wall mount is shown in [Figure 3-4](#).

➤ **To mount the MP-10x on a wall, take these 7 steps:**

1. Remove the screw on the side of the device that is nearest the bottom and the front panel.
2. Insert the peg on the bracket into the third air vent down on the column of air vents nearest the front panel.
3. Swivel the bracket so that the side of the bracket is aligned with the base of the device and the hole in the bracket line up with the empty screw hole.
4. Attach the bracket using one of the screws provided in the device package.
5. Repeat steps 1 to 4 to attach the second bracket to the other side of the device.
6. Position the device on the wall with the base of the device next to the wall.
7. Use four screws to attach the device to the wall. These screws are not provided with the device.

Figure 3-4: MP-102 Wall Mount



3.1.3 Cabling the MP-1xx

Verify that you have the cables listed under column ‘Cable’ in [Table 3-1](#) before beginning to cable the MP-1xx according to the column ‘Cabling Procedure’. For detailed information on the MP-1xx rear panel connectors, refer to [Section 2.1.2](#) on page 19.

Table 3-1: Cables and Cabling Procedure

Cable	Cabling Procedure	
RJ-45 Ethernet cable	Connect the Ethernet connection on the MP-1xx directly to the network using a standard RJ-45 Ethernet cable. For connector’s pinout refer to Figure 3-5 on page 31. Note that when assigning an IP address to the MP-1xx using HTTP (under Step 1 in Section 4.1.1), you may be required to disconnect this cable and re-cable it differently.	
RJ-11 two-wire telephone cords	Connect the RJ-11 connectors on the rear panel of the MP-10x/FXS to fax machine, modem, or phones (refer to Figure 3-6). Connect RJ-11 connectors on the MP-10x/FXO rear panel to telephone exchange analog lines or PBX extensions (Figure 3-6). MP-124/FXS ports are usually distributed using an MDF Adaptor Block (<i>special order option</i>). Refer to Figure 3-8 for details.	Ensure that FXS & FXO are connected to the correct devices, otherwise damage can occur.
Lifeline cable	For detailed information on setting up the Lifeline, refer to the procedure under Section 3.1.3.2 on page 33.	
50-pin Telco cable (MP-124 devices only).	Refer to the MP-124 Safety Notice below. <ol style="list-style-type: none"> 1. Wire the 50-pin Telco connectors according to the pinout in Figure 3-7 on page 31, and Figure 3-8 on page 32. 2. Attach each pair of wires from a 25-pair Octopus cable to its corresponding socket on the MDF Adaptor Block’s rear. 3. Connect the wire-pairs at the other end of the cable to a male 50-pin Telco 	

Cable	Cabling Procedure
	<p>connector.</p> <ol style="list-style-type: none"> Insert and fasten this connector to the female 50-pin Telco connector on the MP-124 rear panel (labeled Analog Lines 1-24). Connect the telephone lines from the Adaptor Block to a fax machine, modem, or telephones by inserting each RJ-11 connector on the 2-wire line cords of the POTS phones into the RJ-11 sockets on the front of an MDF Adaptor Block as shown in Figure 3-8 on page 32. <p>An Octopus cable is not included with the MP-124 package.</p>
RS-232 serial cable	For detailed information on connecting the MP-1xx RS-232 port to your PC, refer to Section 3.1.3.1 on page 32.
Protective earthing strap	Connect an earthed strap to the chassis protective earthing screw and fasten it securely according to the safety standards.
AC Power cable	Connect the MP-1xx power socket to the mains.



MP-124 Safety Notice

To protect against electrical shock and fire, use a minimum size 26 AWG line cord to connect analog FXS lines to the 50-pin Telco connector.

Figure 3-5: RJ-45 Ethernet Connector Pinout

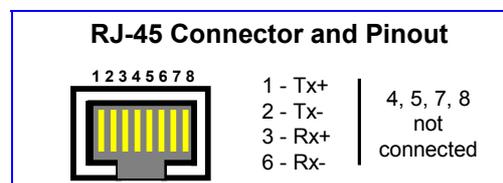


Figure 3-6: RJ-11 Phone Connector Pinout

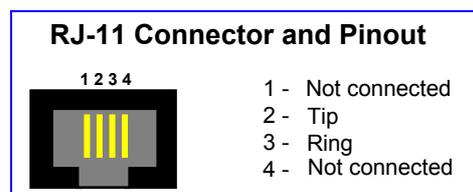


Figure 3-7: 50-pin Telco Connector (MP-124/FXS only)

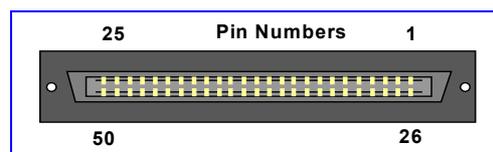


Figure 3-8: MP-124 in a 19-inch Rack with MDF Adaptor

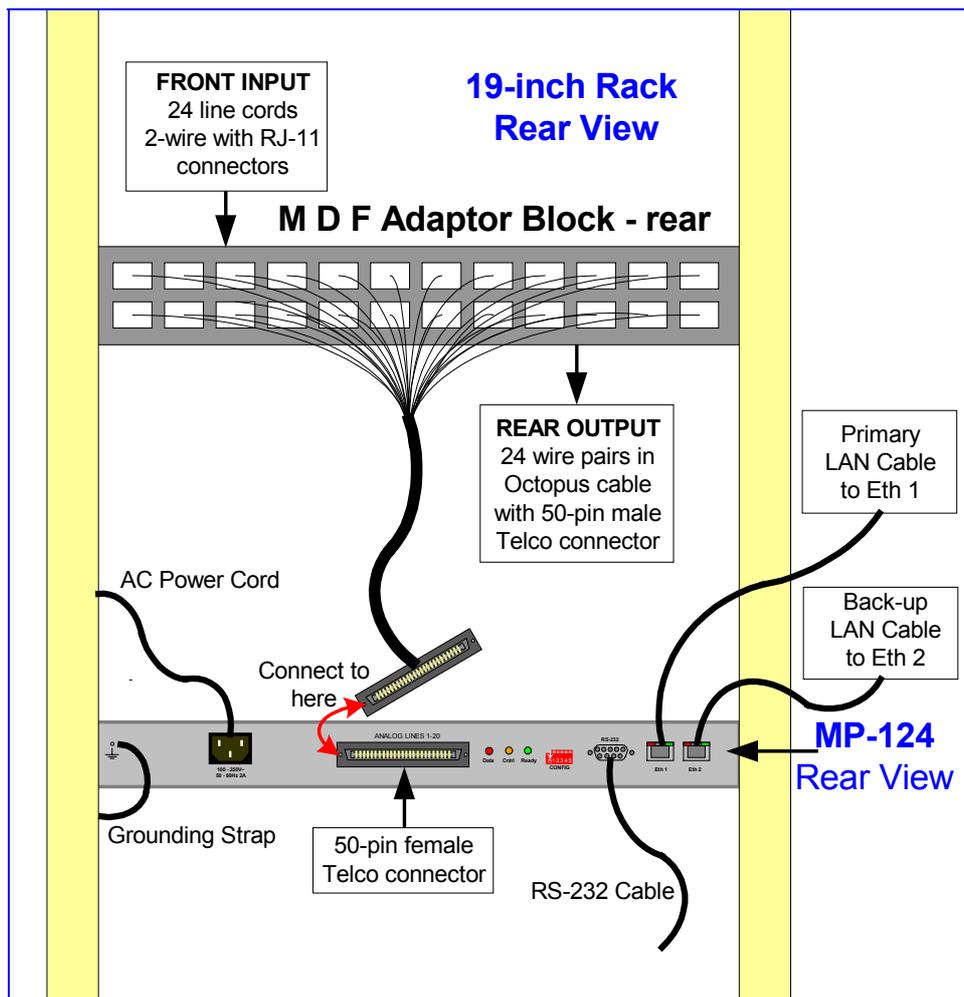


Table 3-2: Pin Allocation in the 50-pin Telco Connector

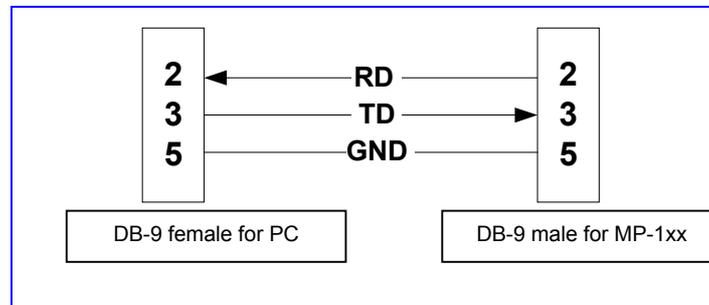
Phone Channel	Connector Pins	Phone Channel	Connector Pins
1	1/26	13	13/38
2	2/27	14	14/39
3	3/28	15	15/40
4	4/29	16	16/41
5	5/30	17	17/42
6	6/31	18	18/43
7	7/32	19	19/44
8	8/33	20	20/45
9	9/34	21	21/46
10	10/35	22	22/47
11	11/36	23	23/48
12	12/37	24	24/49

3.1.3.1 Connecting the MP-1xx RS-232 Port to Your PC

Using a standard RS-232 straight cable (not a cross-over cable) with DB-9 connectors, connect the MP-1xx RS-232 port to either COM1 or COM2 RS-232 communication port on your PC. The required connector pinout and gender are shown below in [Figure 3-9](#).

The RS-232 port is mainly used internally by service personnel. Advanced users can also use this feature for SMDI and to access the embedded command line interface (CLI) and refer to Section 8.7 on page 175. **A DB-9 to DB-9 cable is not included with the MP-1xx package.**

Figure 3-9: RS-232 Cable Wiring



3.1.3.2 Cabling the Lifeline Telephone

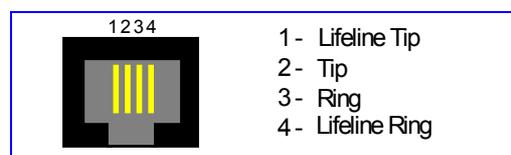
The Lifeline telephone provides a wired analog POTS phone connection to any PSTN or PBX FXS port when there is no power, or when the network connection fails. Users can therefore use the Lifeline phone even when the MP-1xx is not powered on or not connected to the network. With the MP-108/FXS and MP-104/FXS the Lifeline connection is provided on port #4 (refer to Figure 3-11). With the MP-102/FXS the Lifeline connection is provided on port #2.



Note: The MP-124 and MP-10x/FXO do NOT support the Lifeline.

The Lifeline telephone Splitter connects pins #1 and #4 to another source of an FXS port, and pins #2 and #3 to the POTS phone. Refer to the Lifeline Splitter pinout in Figure 3-10.

Figure 3-10: Lifeline Splitter Pinout & RJ-11 Connector for MP-10x/FXS



➤ To cable the MP-10x/FXS Lifeline phone, take these 3 steps:

1. Connect the Lifeline Splitter to port #4 (on the MP-104/FXS or MP-108/FXS) or to port #2 (on the MP-102/FXS).
2. Connect the Lifeline phone to Port A on the Lifeline Splitter.
3. Connect an analog PSTN line to Port B on the Lifeline Splitter.



Note: The use of the Lifeline on network failure can be disabled using the 'LifeLineType' ini file parameter (described in 11.1.4 on page 214).

Figure 3-11: MP-104/FXS Lifeline Setup

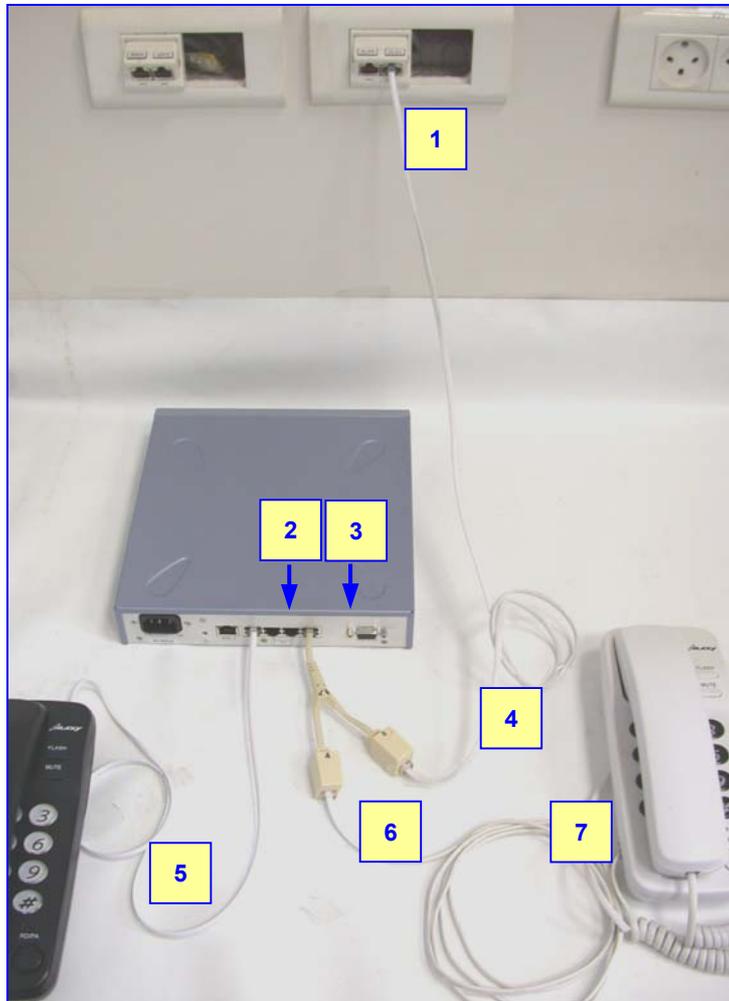


Table 3-3: MP-104/FXS Lifeline Setup Component Descriptions

Item #	Component Description
1	B: To PSTN wall port.
2	Phone to Port 1.
3	Lifeline to Port 4.
4	PSTN to Splitter (B).
5	Phone to Port 1.
6	Lifeline phone to Splitter (A).
7	Lifeline phone.



Note: This concludes the MP-1xx installation procedure. Continue with Section 4 on page 41

3.2 Installing the MP-11x

➤ **To install the MP-11x, take these 4 steps:**

1. Unpack the MP-11x (refer to Section 3.2.1 below).
2. Check the package contents (refer to Section 3.2.2 below).
3. Mount the MP-11x (refer to Section 3.2.4 on page 36).
4. Cable the MP-11x (refer to Section 3.2.5 on page 30).

After connecting the MP-11x to the power source, the Ready and Power LEDs on the front panel turn to green (after a self-testing period of about 2 minutes). Any malfunction in the startup procedure changes the Fail LED to red and the Ready LED is turned off (refer to Table 2-7 on page 22 for details on the MP-11x LEDs).

3.2.1 Unpacking

➤ **To unpack the MP-11x, take these 6 steps:**

1. Open the carton and remove the packing materials.
2. Remove the MP-11x gateway from the carton.
3. Check that there is no equipment damage.
4. Check, retain and process any documents.
5. Notify AudioCodes or your local supplier of any damage or discrepancies.
6. Retain any diskettes or CDs.

3.2.2 Package Contents

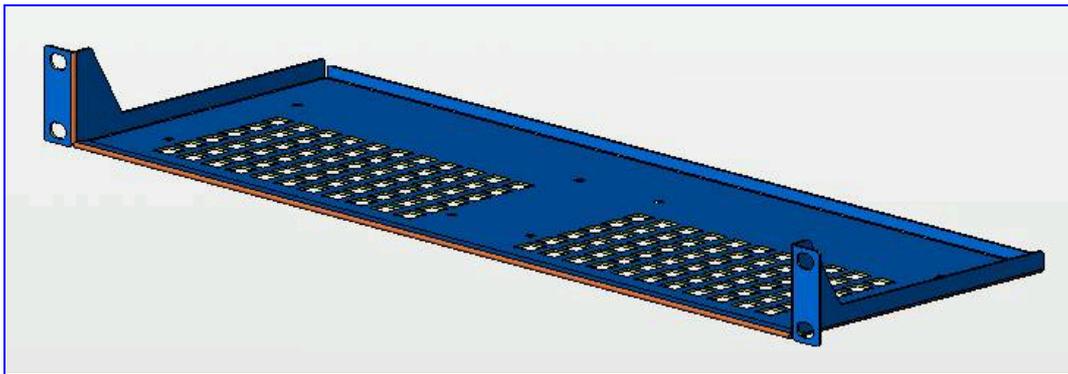
Ensure that in addition to the MP-11x, the package contains:

- AC power cable.
- Small plastic bag containing four anti-slide bumpers for desktop installation.
- Lifeline cable (RJ-11 adaptor cable for 1 to 2 with MP-118 and MP-114 only, by special order).
- A CD with software and documentation may be included.
- The MP-11x Fast Track Installation Guide.

3.2.3 19-inch Rack Installation Package

Additional option is available for installing the MP-11x in a 19-inch rack. The 19-inch rack installation package contains a single shelf (shown in Figure 3-12 below) and eight shelf-to-device screws.

Figure 3-12: 19-inch Rack Shelf



3.2.4 Mounting the MP-11x

The MP-11x can be mounted on a desktop (refer to Section 3.2.4.1 below), on a wall (refer to Section 3.2.4.2) or installed in a standard 19-inch rack (refer to Section 3.2.4.2).

Figure 3-13 below describes the design of the MP-11x base.

Figure 3-13: View of the MP-11x Base

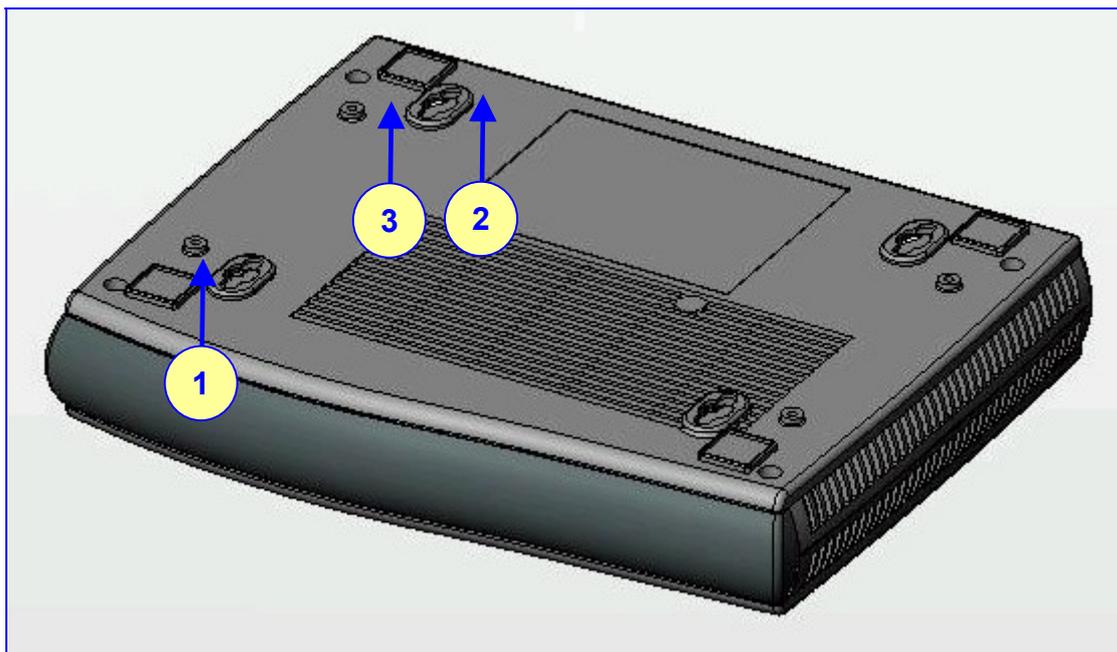


Table 3-4: View of the MP-11x Base

Item #	Functionality
1	Square slot used to attach anti-slide bumpers (for desktop mounting)
2	Oval notch used to attach the MP-11x to a wall
3	Screw opening used to attach the MP-11x to a 19-inch shelf rack

3.2.4.1 Mounting the MP-11x on a Desktop

Attach the four (supplied) anti-slide bumpers to the base of the MP-11x (refer to item #1 in Figure 3-13) and place it on the desktop in the position you require.

3.2.4.2 Mounting the MP-11x on a Wall

➤ **To mount the MP-11x on a wall, take these 4 steps:**

1. Drill four holes according to the following dimensions:
 - Side-to-side distance 140 mm.
 - Front-to-back distance 101.4 mm.
2. Insert a wall anchor of the appropriate size into each hole.
3. Fasten a DIN 96 3.5X20 wood screw (not supplied) into each of the wall anchors.
4. Position the four oval notches located on the base of the MP-11x (refer to item #2 in Figure 3-13) over the four screws and hang the MP-11x on them.

3.2.4.3 Installing the MP-11x in a 19-inch Rack

The MP-11x is installed in a standard 19-inch rack by placing it on a shelf preinstalled in the rack. This shelf can be ordered separately from AudioCodes.

Figure 3-14: MP-11x Rack Mount

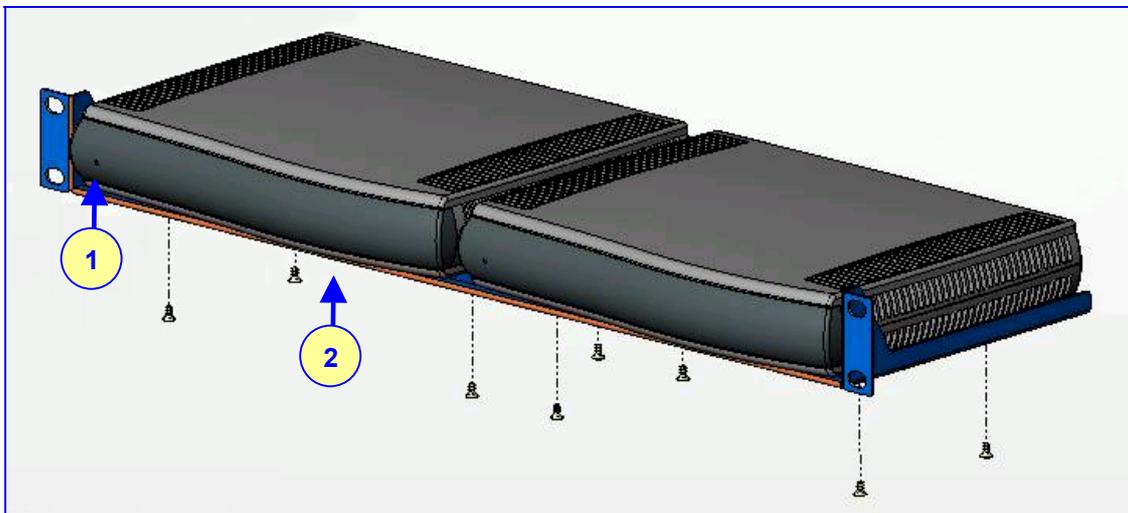


Table 3-5: MP-11x Rack Mount

Item #	Functionality
1	Standard rack holes used to attach the shelf to the rack
2	Eight shelf-to-device screws

➤ **To install the MP-11x in a 19-inch rack, take these 3 steps:**

1. Use the shelf-to-device screws found in the package to attach one or two MP-11x devices to the shelf.
2. Position the shelf in the rack and line up its side holes with the rack frame holes.
3. Use four standard rack screws to attach the shelf to the rack. These screws are not provided.

3.2.5 Cabling the MP-11x

Cable your MP-11x according to each section of [Table 3-6](#). For detailed information on the MP-11x rear panel connectors, refer to [Table 2-8](#) on page 23.

Table 3-6: Cables and Cabling Procedure

Cable	Cabling Procedure	
RJ-45 Ethernet cable	Connect the Ethernet connection on the MP-11x directly to the network using a standard RJ-45 Ethernet cable. For connector's pinout refer to Figure 3-15 on page 38. Note that when assigning an IP address to the MP-11x using HTTP (under Step 1 in Section 4.1.1), you may be required to disconnect this cable and re-cable it differently.	
RJ-11 two-wire telephone cords	Connect the RJ-11 connectors on the rear panel of the MP-11x to fax machine, modem, or phones (refer to Figure 3-6).	Ensure that the FXS ports are connected to the correct devices, otherwise damage can occur.
Lifeline	For detailed information on setting up the Lifeline, refer to the procedure under Section 3.2.5.2 on page 39.	
RS-232 serial cable	For detailed information on connecting the MP-11x RS-232 port to your PC, refer to Section 3.2.5.1 on page 39.	
AC Power cable	Connect the MP-11x power socket to the mains.	

Figure 3-15: RJ-45 Ethernet Connector Pinout

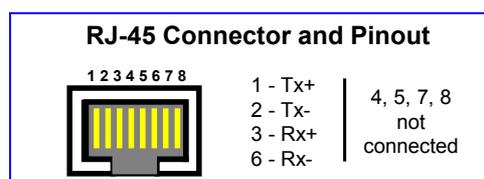
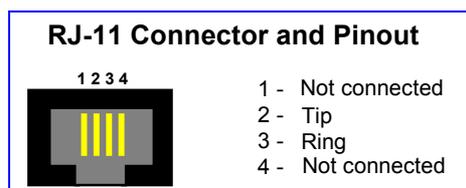


Figure 3-16: RJ-11 Phone Connector Pinout



3.2.5.1 Connecting the MP-11x RS-232 Port to Your PC

Using a standard RS-232 straight cable (not a cross-over cable) with DB-9 connectors, connect the MP-11x RS-232 port (using a DB-9 to PS/2 adaptor) to either COM1 or COM2 RS-232 communication port on your PC. The pinout of the PS/2 connector is shown below in [Figure 3-17](#). **A PS/2 to DB-9 cable is not included with the MP-11x package.**

The RS-232 port is mainly used internally by service personnel. Advanced users can also use this feature to access the embedded command line interface (refer to Section 8.7 on page 175).

Figure 3-17: PS/2 Pinout

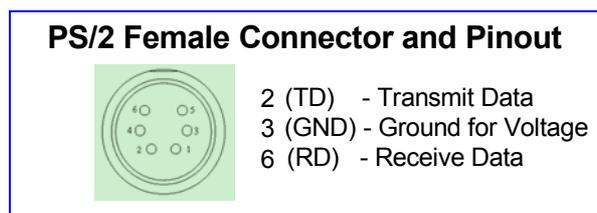
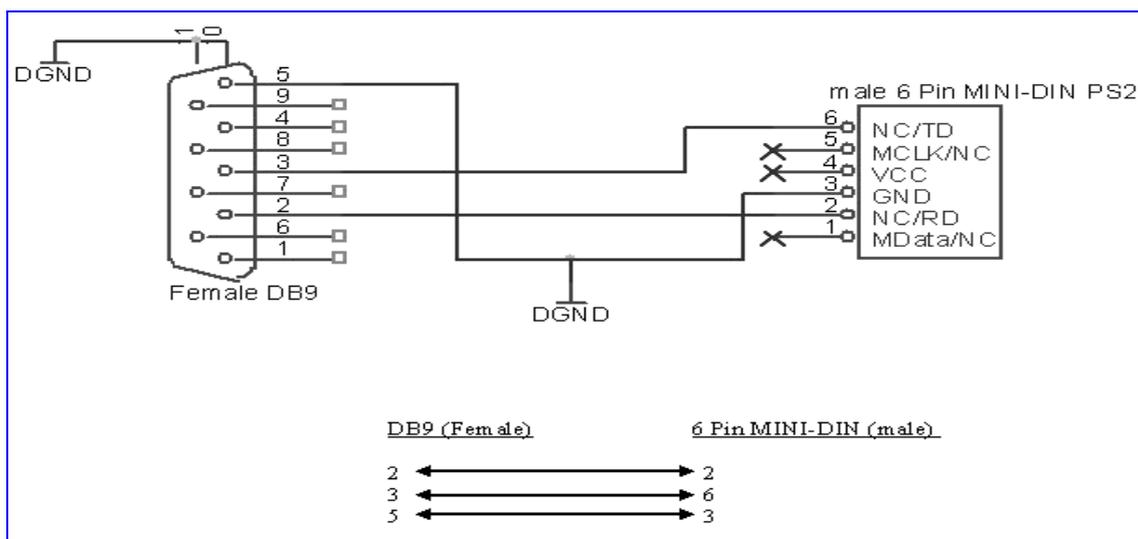


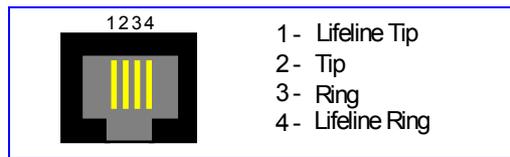
Figure 3-18: PS/2 to DB-9 Pinout



3.2.5.2 Cabling the MP-11x Lifeline Telephone

The Lifeline telephone (connected to port #1) provides a wired analog POTS phone connection to any PSTN or PBX FXS port when there is no power, or the when network connection fails. Users can therefore use the Lifeline phone even when the MP-11x is not powered on or not connected to the network.

The Lifeline telephone Splitter connects pins #1 and #4 to another source of an FXS port, and pins #2 and #3 to the POTS phone. Refer to the Lifeline Splitter pinout in [Figure 3-19](#).

Figure 3-19: Lifeline Splitter Pinout & RJ-11 Connector


➤ **To cable the MP-11x Lifeline, take these 3 steps:**

1. Connect the Lifeline Splitter to port #1 on the MP-11x.
2. Connect the Lifeline phone to Port A on the Lifeline Splitter.
3. Connect an analog PSTN line to Port B on the Lifeline Splitter.



Note: The use of the Lifeline on network failure can be disabled using the 'LifeLineType' *ini* file parameter (described in Section 11.1.4 on page 214).

4 Getting Started



Note: MediaPack refers collectively to both the MP-1xx Series and the MP-11x the MP-11x Series

The MediaPack is supplied with application software already resident in its flash memory (with factory default parameters).

Section 4.1 below describes how to assign an IP address to the MediaPack.

For detailed information on how to *fully* configure the gateway, refer to the Web Interface, described in Section 7.3 on page 114.

4.1 Assigning the MediaPack IP Address

To assign an IP address to the MediaPack use one of the following methods:

- HTTP using a Web browser (refer to Section 4.1.1 below).
- BootP (refer to Section 4.1.2 on page 43).
- DHCP (refer to Section 5.3 on page 46).
- Embedded command line interface (refer to Section 8.7 on page 175).
- The default networking parameters are show in Table 4-1.

You can use the 'Reset' button to restore the MediaPack networking parameters to their factory default values (refer to Section 4.2 on page 44).

Table 4-1: MediaPack Default Networking Parameters

FXS or FXO	Default Value
FXS	10.1.10.10
FXO	10.1.10.11
MediaPack default subnet mask is 255.255.0.0, default gateway IP address is 0.0.0.0	

4.1.1 Assigning an IP Address Using HTTP

➤ **To assign an IP address using HTTP, take these 8 steps:**

1. Disconnect the MediaPack from the network and reconnect it to your PC using one of the following two methods:
 - Use a standard Ethernet cable to connect the network interface on your PC to a port on a network hub / switch. Use a second standard Ethernet cable to connect the MediaPack to another port on the same network hub / switch.
 - Use an Ethernet cross-over cable (for the MP-1xx) or a standard (straight) Ethernet cable (for the MP-11x) to directly connect the network interface on

your PC to the MediaPack.



Note: For PC connection, the MP-1xx Series uses an Ethernet cross-over cable and MP-11x Series uses an Ethernet straight cable.

2. Change your PC's IP address and subnet mask to correspond with the MediaPack factory default IP address and subnet mask, shown in [Table 4-1](#). For details on changing the IP address and subnet mask of your PC, refer to Windows™ Online Help (Start>Help).
3. Access the MediaPack Embedded Web Server (refer to Section 7.3.4 on page 117).
4. In the 'Quick Setup' screen (shown in Figure 7-3), set the MediaPack 'IP Address', 'Subnet Mask' and 'Default Gateway IP Address' fields under 'IP Configuration' to *correspond with your network IP settings*. If your network doesn't feature a default gateway, enter a dummy value in the 'Default Gateway IP Address' field.
5. Click the **Reset** button and click **OK** in the prompt; the MediaPack applies the changes and restarts.



Tip: Record and retain the IP address and subnet mask you assign the MediaPack. Do the same when defining new username or password. If the Embedded Web Server is unavailable (for example, if you've lost your username and password), use the BootP/TFTP (Trivial File Transfer Protocol) configuration utility to access the device, "reflash" the load and reset the password (refer to Appendix A - BootP/TFTP Server on page [185](#) for detailed information on using a BootP/TFTP configuration utility to access the device).

6. Disconnect your PC from the MediaPack or from the hub / switch (depending on the connection method you used in step [1](#)).
7. Reconnect the MediaPack and your PC (if necessary) to the LAN.
8. Restore your PC's IP address & subnet mask to what they originally were. If necessary, restart your PC and re-access the MediaPack via the Embedded Web Server with its new assigned IP address.

4.1.2 Assigning an IP Address Using BootP



Note: BootP procedure can also be performed using any standard compatible BootP server.



Tip: You can also use BootP to load the auxiliary files to the MediaPack (refer to Section 5.4.2 on page 58).

➤ **To assign an IP address using BootP, take these 3 steps:**

1. Open the BootP application (supplied with the MediaPack software package).
2. Add client configuration for the MediaPack, refer to Appendix A - BootP/TFTP Server on page 185.
3. Reset the gateway *physically* causing it to use BootP; the MediaPack changes its network parameters to the values provided by the BootP.

4.2 Restoring Networking Parameters to their Initial State

You can use the 'Reset' button to restore the MediaPack networking parameters to their factory default values (described in [Table 4-1](#)) and to reset the username and password.

Note that the MediaPack returns to the software version burned in flash. This process also restores the MediaPack parameters to their factory settings, therefore you must load your previously backed-up *ini* file, or the default *ini* file (received with the software kit) to set them to their correct values.

➤ To restore the networking parameters of the MediaPack to their initial state, take these 5 steps:

1. Disconnect the MediaPack from the power and network cables.
2. Reconnect the power cable; the gateway is powered up. After approximately 45 seconds the Ready LED turns to green and the Control LED blinks for about 3 seconds.
3. While the Control LED is blinking, press shortly on the reset button (located on the left side of the front panel); the gateway resets a second time and is restored with factory default parameters (username: "Admin", password: "Admin").
4. Reconnect the network cable.
5. Assign the MediaPack IP address (refer to [Section 4.1](#) on page 41).

➤ To restore the networking parameters of the MP-11x to their initial state, take these 4 steps:

1. Press in the 'Reset' button uninterruptedly for a duration of more than six seconds; the gateway is restored to its factory settings (username: 'Admin', password: 'Admin').
2. Assign the MP-11x IP address (refer to [Section 4.1](#) on page 41).
3. Load your previously backed-up *ini* file, or the default *ini* file (received with the software kit). To load the *ini* file via the Embedded Web Server, refer to the MP-11x User's Manual.
4. Press again on the 'Reset' button (this time for a short period).

5 MediaPack Initialization & Configuration Files

This section describes the configuration options and Initialization procedures for the MediaPack. It includes:

- Boot Firmware & Operational Firmware (refer to "Boot Firmware & Operational Firmware" on page 45)
- Startup Process (refer to 'MediaPack Startup')
- BootP/DHCP (refer to "Using BootP/DHCP" on page 46')
- Configuration Parameters and Files (refer to "Configuration Parameters and Files" on page 50)

5.1 Boot Firmware & Operational Firmware

The MediaPack runs two distinct software programs: Boot firmware and operational firmware.

1. Boot firmware - Boot firmware (also known as flash software) resides in the MediaPack's non-volatile memory. When the MediaPack is reset, Boot software is initialized and the operational software is loaded into the SDRAM from a TFTP server or integral non-volatile memory. Boot software is also responsible for obtaining the MediaPack's IP parameters and *ini* file name (used to obtain the MediaPack's configuration parameters) via integral BootP or DHCP clients. The Boot firmware version can be viewed on the Embedded Web Server's GUI ('Embedded Web Server' on page 114'). The last step the Boot firmware performs is to jump to the first line of code in the operational software.
2. *cmp* and *hex* Operational firmware files - The operational firmware, in the form of a *cmp* file (the software image file) and *hex* file (the uncompressed software image file), is supplied in the MediaPack's software package contained on the CD accompanying the MediaPack. These files contain the MediaPack's main software, providing all the services described in this manual. The *cmp* file is usually burned into the MediaPack's non-volatile memory so that it does not need to be externally loaded each time the MediaPack is reset.

5.2 MediaPack Startup

The MediaPack's startup process begins when the MediaPack is reset. The startup process ends when the operational firmware is running. The startup process includes how the MediaPack obtains its IP parameters, firmware and configuration files.

The MediaPack is reset when one of the following scenarios occurs:

1. the power is reset
2. `acOpenRemoteBoard()` is called with `RemoteOpenBoardOperationMode` set to Full Configuration Mode (valid for VopLib API users only)
3. There is a device irregularity

4. Users perform a reset in the Embedded Web Server GUI or SNMP manager

5.3 Using BootP/DHCP

The MediaPack uses BootP (Bootstrap protocol) and DHCP to configure the MediaPack's initial parameters. BootP/DHCP enables network administrators to manage the basic configuration of the MediaPack from a central server.

RFCs (IETF Requests for Comment) 951, 1542, and 2132 describe BootP in detail. The protocol has been extended to enable BootP/DHCP to configure additional parameters specific to the MediaPack.

As the flow chart in the figure above illustrates, a BootP/DHCP request is issued after a power reset, a device exception, or when calling `acResetRemoteBoard()` API (assuming that the MediaPack was not reset by an `acOpenBoard()` API).



Note: BootP is normally used to configure the initial parameters of the MediaPack. Thereafter, BootP is no longer required as all parameters can be stored in the MediaPack's non-volatile memory and used when BootP is inaccessible. BootP is required again (for example) to change the IP address of the MediaPack.

5.3.1 BootP/DHCP Server Parameters

BootP/DHCP can be used to provision the following parameters (included in the BootP/DHCP reply. Note that some parameters are optional):

- **IP address, IP subnet mask** - These parameters are mandatory and are supplied by the server to the MediaPack every time a BootP/DHCP process takes place.
- **Default Gateway IP address** - This configuration parameter is optional. The default Gateway IP address is supplied to the MediaPack by BootP/DHCP only if the field is defined/configured in the server.
- **TFTP server IP address** - This optional parameter contains the address of the TFTP server from which the firmware file and *ini* file are loaded.
- **DNS Server IP Address (Primary and Secondary)** - These optional parameters contain the IP addresses of the DNS servers. These parameters are available only in DHCP and from Boot version 1.92. A DNS server can only be used by an MGCP configured device.
- **Firmware file name** - When the MediaPack detects that this optional parameter is defined/configured in BootP/DHCP, it initiates a TFTP process to load the file. If the firmware file name is not specified in the BootP/TFTP server, the MediaPack uses the last image stored in its non-volatile memory.
- **Command Line Switches**

In the BootP/TFTP Server, you can add command line switches in the Boot File field (in the Client Configuration screen). Command line switches are used for various tasks, such as to determine if the firmware should be burned on the non-volatile memory or not. The table below describes the different command line switches.

➤ **To use a command line switch, take these 4 steps:**

1. In the **Boot File** field, leave the file name defined in the field as it is (e.g., *ramxxx.cmp*).
2. Place your cursor after *cmp*.
3. Press the space bar.
4. Type in the switch you require (refer to the table below).

Example: **ramxxx.cmp -fb** to burn flash memory

ramxxx.cmp -fb -em 4 to burn flash memory and for Ethernet Mode 4 (auto-negotiate)

The table below lists and describes the available switches.

Table 5-1: Command Line Switch Descriptions

Switch	Description
-fb	Burn ram.cmp in non-volatile memory. Only the <i>cmp</i> file (the compressed firmware file) can be burned to the MediaPack's non-volatile memory. The <i>hex</i> file (the uncompressed firmware file) can not be burned.
-em#	Use this switch to set Ethernet mode. 0 = 10 Base-T half-duplex 1 = 10 Base-T full-duplex 2 = 100 Base-TX half-duplex 3 = 100 Base-TX full-duplex 4 = auto-negotiate (default) Auto-negotiate falls back to half-duplex mode when the opposite port is not in auto-negotiate but the speed (10 Base-T or 100 Base-TX) in this mode is always configured correctly.
-br	BootP retries: 1 = 1 BootP retry, 1 sec 2 = 2 BootP retries, 3 sec 3 = 3 BootP retries, 6 sec 4 = 10 BootP retries, 30 sec 5 = 20 BootP retries, 60 sec 6 = 40 BootP retries, 120 sec 7 = 100 BootP retries, 300 sec 15 = BootP retries indefinitely Use this switch to set the number of BootP retries that the MediaPack sends during start-up. The MediaPack stops issuing BootP requests when either an AA122BootP reply is received or Number Of Retries is reached. This switch takes effect only from the next MediaPack reset.

Table 5-1: Command Line Switch Descriptions

Switch	Description
-bd	BootP delays. 1 = 1 sec (default), 2 = 10 sec, 3 = 30 sec, 4 = 60 sec, 5 = 120 sec. This sets the delay from the MediaPack's reset until the first BootP request is issued by the MediaPack. The switch only takes effect from the next reset of the MediaPack.
-bs	Selective BootP
-be	Use -be 1 for the MediaPack to send client information that can be viewed in the main screen of the BootP/TFTP Server, under column 'Client Info' (refer to Figure A-3, on page 165, showing BootP/TFTP Server's main screen with the column 'Client Info' on the extreme right). 'Client Info' can include IP address, number of channels (in the case of AudioCodes' media gateways), which <i>cmp</i> file is burned into the MediaPack's non-volatile memory, etc.



Note: After programming a new *cmp* software image file, all configuration parameters and tables are erased. Reprogram them by downloading the *ini* file.

- Configuration (*ini*) file name** - The *ini* file is a proprietary configuration file with an *ini* extension, containing configuration parameters and tables. For more information on this file, refer to "Configuration Parameters and Files" on page 50. When the MediaPack detects that this optional parameter field is defined in BootP, it initiates a TFTP process to load the file into the MediaPack. The new configuration contained in the *ini* file can be stored in the MediaPack's integral non-volatile memory. Whenever the MediaPack is reset and no BootP reply is sent to the board or the *ini* file name is missing in the BootP reply, the MediaPack uses the previously stored *ini* file.

5.3.2 Host Name Support

From Boot software version 1.92, the MediaPack registers a device-specific Host Name on the DNS server by defining the Host Name field of the DHCP request. The host name is set to **acl_nnnnnnnn**, where nnnnnnnn is the serial number of the MediaPack (the serial number is equal to the last 6 digits of the MAC address converted from Hex to decimal). The DHCP server registers this Host Name on the DNS server. This feature allows users to configure the MediaPack via the Web Browser by providing the following URL: **http://ACL_<serial number>** (instead of using the boards' IP address).

5.3.3 Selective BootP

The Selective BootP mechanism, available from Boot version 1.92, allows the integral BootP client to filter out unsolicited BootP replies. This can be beneficial for environments where more than one BootP server is available and only one BootP server is used to configure devices.

- To activate this feature, add the command line switch **-bs 1** to the Firmware File Name field.
- To deactivate, use **-bs 0**. When activated, the MediaPack accepts only BootP replies containing the text AUDC in the Vendor Specific Information field.

5.3.4 Vendor Specific Information

The MediaPack uses the Vendor Specific Information field in the BootP server to provide device-related initial startup parameters (according to RFC 1533). This field is not available in DHCP servers. The field is disabled by default.

To enable / disable this feature user can do one of the following:

- a. Set the *ini* file parameter 'ExtBootPReqEnable' = **0** to disable, or **1** to enable.
- b. Use the **-be** command line switch in the Boot file field in the BootP server as follows:
ramxxx.cmp -be 0 to disable, or **-be 1** to enable.

The table below details the Vendor Specific Information field according to the MP-11x:

Table 5-2: Vendor Specific Information Field

Tag #	Description	Value	Length
220	Board Type	#10 = MP-102 #11 = MP-104 #12 = MP-108 #13 = MP-124 #14 = MP-118 #15 = MP-114 #16 = MP-112	1
221	Current IP Address	XXX.XXX.XXX.XXX	4
222	Burned Boot Software Version	X.XX	4
223	Burned CMP Software Version	XXXXXXXXXXXX	12
224	Geographical Address	VENDOR-SPECIFIC-VAR2	1
225	Chassis Geographical Address	VENDOR-SPECIFIC-VAR2	1
226	TPM ID	VENDOR-SPECIFIC-VAR3	1
227	Rear I/O Version	VENDOR-SPECIFIC-VAR4	1
228	In door - Out door (In door is valid for FXS only. FXO is always Out door.)	VENDOR-SPECIFIC-VAR5	1
229	E&M	N/A	1
230	Analog Channels	2 / 4 / 8 / 24	1

The structure of the Vendor Specific Information field is demonstrated in the table below.

Table 5-3: Vendor Specific Information Fields

Vendor-Specific Information Code	Length Total	Tag Num	Length	Value	Tab Num	Length	Value	Tag Num	Length	Value (1)	Value (2)	Value (3)	Value (4)	Tag End
42	12	220	1	14	227	1	1	221	4	10	2	70	1	255

5.3.5 Microsoft™ DHCP/BootP Server

The MediaPack can be configured with a third-party BootP server (besides AudioCodes' BootP/TFTP Server), including the Microsoft™ DHCP server, to provide the BOARDNAME with an IP address and other initial parameter configurations.

To configure the Microsoft™ Windows™ NT DHCP Server to configure an IP address to BootP clients, add a reservation for each BootP client.

For information on how to add a reservation, view the "Managing Client Reservations Help" topic in the DHCP Manager.

The reservation builds an association between MAC address (12 digits), provided in accompanying product documentation) and the IP address. Windows™ NT Server provides the IP address based on the BOARDNAME MAC address in the BootP request frame.

To configure the Microsoft™ Windows™ NT DHCP server to provide Boot File information to BootP clients, edit the BootP Table in the DHCP Manager. The BootP Table is located in the Server Properties dialog, accessed from the Server menu. For information on editing the BootP Table, view the "BootP Table" Help topic in the DHCP Manager.

The following parameters must be specified:

- **Local IP address** - The MediaPack's IP address
- **Subnet mask**
- **Gateway IP address** - Default Gateway IP address
- **BootP File name** - Optional (refer to the following Note)



Note: The BootP File field should normally not be used. The field is only used for software upgrade (refer to "Upgrading MediaPack Software" on page 76).

5.4 Configuration Parameters and Files

The MediaPack's configuration is stored in two file groups.

- The configuration file - an initialization (*ini*) text file containing configuration parameters of the MediaPack.
- The auxiliary files - *dat* files containing the raw data used for various tasks such as Call Progress Tones, Voice Prompts, logo image, etc.

These files contain factory-pre-configured parameter defaults when supplied with the MediaPack and are stored in the MediaPack's non-volatile memory. The MediaPack is started up initially with this default configuration. Subsequently, these files can be modified and reloaded using any of the following methods:

- via BootP/TFTP during the startup process (refer to "Using BootP/DHCP" on page 46' and the Appendix, "BootP/TFTP Server" on page 185).
- via the Embedded Web Server (refer to "Embedded Web Server" on page 114).

The modified auxiliary files can be burned into the non-volatile memory (refer to the SaveConfiguration parameter in "Downloading Auxiliary Files" on page 58) so that the modified configuration is utilized with subsequent resets. The configuration file is always stored on the non-volatile memory. There is no need to repeatedly reload the modified files with reset.



Note 1: Users who configure the MediaPack with the Embedded Web Server do not require downloading the *ini* file and have no need to utilize a TFTP server.

Note 2: SNMP users configure the MediaPack via SNMP. Therefore a very small *ini* file is required which contains the IP address for the SNMP traps.

5.4.1 Initialization (*ini*) Files

The *ini* file can contain a number of parameters. The *ini* file structure supports the following parameter value constructs:

- **Parameter = Value** (refer to "Parameter = Value Constructs" on page 169) The lists of parameters are provided in the Appendix, "Individual '*ini*' File Parameters" on page 195.
- **Tables of Parameter Value** (refer to 'Table of Parameter Value Constructs').

Below is an example of the general structure of the *ini* file for both the Parameter = Value and Tables of Parameter Value Constructs.

```

[Sub Section Name]
Parameter_Name = Parameter_Value
Parameter_Name = Parameter_Value
.
..

; REMARK

  [Sub Section Name]
  ...

; Tables Format Rules:
[Table_Name]
; Fields declaration
Format Index_Name_1 ... Index_Name_N = Param_Name_1 ... Param_Name_M
; Table's Lines (repeat for each line)
Table_Name Index_1_val ... Index_N_val = Param_Val_1 ... Param_Val_M
[\Table_Name]
  
```

5.4.1.1 Parameter = Value Construct

The following are the rules in the *ini* File Structure for individual *ini* file parameters (Parameter = Value):

- Lines beginning with a semi-colon ';' (as the first character) are ignored.
- An Enter must be the final character of each line.
- The number of spaces before and after "=" is not relevant.
- If there is a syntax error in the parameter name, the value is ignored.
- Syntax errors in the parameter value field can cause unexpected errors (because parameters may be set to the incorrect values).
- Sub-section names are optional.
- String parameters, representing file names, for example, CallProgressTonesFileName, must be placed between two inverted commas ('...').
- The parameter name is NOT case sensitive; the parameter value is not case sensitive except for coder names.
- Numeric parameter values should be entered only in decimal format.
- The *ini* file should be ended with one or more Enters.

5.4.1.2 *ini* File Examples

Below is an example of an *ini* file for MGCP.

```
[MGCP]
EndpointName = 'ACgw'
CallAgentIP = 192.1.10.3
CallAgentPort = 2427
BaseUDPPort = 4000

RingOnPeriod = 1000
RingOffPeriod = 3000
FlashHookPeriod = 700

[Channel Params]
DJBufferMinDelay = 75
RTPRedundancyDepth = 1

[Files]
CallProgressTonesFilename = 'CPUSA.dat'
VoicePromptsFilename = 'tpdemo_723.dat'
FXSLOOPCHARACTERISTICCSFILENAME = 'coeff.dat'
```



Note: Before loading an *ini* file to the MediaPack, make sure that the extension of the *ini* file saved on your PC is correct: Verify that the checkbox Hide extension for known file types (My Computer>Tools>Folder Options>View) is unchecked. Then, verify that the *ini* file name extension is *xxx.ini* and NOT erroneously *xxx.ini.ini* or *xxx~.ini*.

The lists of individual *ini* file parameters are provided in the Appendix, "Individual '*ini*' File Parameters" on page 195.

5.4.1.3 Tables of Parameter Value Construct

Tables of Parameter Values group related parameters of a given entity and handle them together. Tables are composed of rows and columns. The columns represent parameter types, while each row represents an entity. The parameters in each row are called the line attributes. Rows in table may represent (for example) a trunk, SS7 Link, list of timers for a given application, etc.

The tables below provide useful examples for reference.



Note: The tables below are provided as examples for the purpose of illustration only and are NOT actually implemented in MediaPack.

Table 5-4: Table of Parameter Values Example - Remote Management Connections

Index Fields:				
1. Connection Number				
Connection Number	User Name	User Password	Time Connected (msec)	Permissions
0	Admin	Yellow9	0	All
1	Gillian	Red5	1266656	Read Only
2	David	Orange6	0	Read Write

Table 5-5: Table of Parameter Values Example - Port-to-Port Connections

Index Fields:				
1. Source Ports				
2. Destination IP				
3. Destination Port				
Source Port	Destination IP	Destination Port	Connection Name	Application Type
2020	10.4.1.50	2020	ATM_TEST_EQ	LAB_EQ
2314	212.199.201.20	4050	ATM_ITROP_LOOP	LAB_EQ
6010	10.3.3.41	6010	REMOTE_MGMT	MGMT

5.4.1.3.1 Table Indices

Each row in a table must be unique. For this reason, each table defines one or more Index fields. The combination of the Index fields determines the 'line-tag'. Each line-tag may appear only once.

In the example provided in the table above, 'Table of Parameter Values Example - Remote Management Connections', there is only one index field. This is the simplest way to mark rows.

In the example provided in the table above, 'Table of Parameter Values Example - Port-to-Port Connections', there are three Index fields. This more complicated method is a result of the application it represents.

5.4.1.3.2 Table Permissions

Each field in a line has a 'permission' attribute, which determines if and when the user may modify the field.

There are several types of permissions:

- **Read** - The user may read the value of a field (true for all fields).
- **Write** - The user may modify the value of the field at any time.
- **Create** - The user must provide a value for the field at creation time.
- The default values set for all fields already determine the initial values.
- **Maintenance write** - The user may modify the value of the field only when the entity represented by the line is in maintenance state.

Each table includes rules to determine when it is in a maintenance state.

In the 'Table of Parameter Values Example - Remote Management Connections' above, the 'User Name' and 'User Password' fields have Read-Create permissions. The 'Time Connected' field has Read-Only permission, and the 'Permissions' field has a Read-Create-Maintenance_write permission.

5.4.1.4 Rules in the *ini* File Structure for the Tables of Parameter Value Construct

The *ini* file allows you to add/modify parameters in tables. When using tables, Read-Only parameters are not uploaded, since the Read-Only parameters cause an error when trying to download the uploaded file. Therefore read-only parameters should not be included in tables in the *ini* file. Consequently, tables are uploaded with all parameters having at least one of the following permissions:

- Write
- Create
- Maintenance write

The 'format-line' rule defines which fields of the table are to be modified by the given *ini* file (this may vary among *ini* files for the same table). The 'format-line' must only include fields, which can be modified (which are all parameters that are not specified as read-only).

One exception is the index-fields, which are ALWAYS mandatory fields. In the 'Table of Parameter Values Example - Remote Management Connections' above, all fields except the 'Time Connected' field are uploaded.

5.4.1.4.1 Tables Structure Rules

Tables are composed of four elements:

- **Table-Title** - The Table's string name in square brackets (e.g., [MY_TABLE_NAME]).
- **Format Line** - This line specifies the table's fields by their string names.
 - The first word MUST be "FORMAT", followed by indices field names, and after '=' sign, all data fields names should be listed.
 - Items must be separated by ',' sign.

- The Format Line must end with ';' sign.
- Data Line(s) - The actual values for parameters are specified in each Data line. The values are interpreted according to the format line. The first word must be the table's string name.
 - Items must be separated by a ',' sign.
 - A Data Line must end with a ';' sign.
- End-of-Table-Mark: Marks the end of a table. Same as Table title, but string name is preceded by '\'.

Below is an example of the table structure in an *ini* file.

```

; Table: Items Table.
; Fields: Item_Name, Item_Serial_Number, Item_Color,
Item_weight.
; NOTE: Item_Color is not specified. It will be given default
value.
[Items_Table]
; Fields declaration
Format Item_Index = Item_Name, Item_Serial_Number,
Item_weight;
Items_Table 0 = Computer, 678678, 6;
Items_Table 6 = Computer-screen, 127979, 9;
Items_Table 2 = Computer-pad, 111111, $$;
[\\Items_Table]
  
```

- Indices (in both the Format line and the Data lines) must all appear in order, as determined by the table's specific documentation. The Index field must NOT be omitted.
- Data fields in the Format line may use a sub-set of all of the configurable fields in a table only. In this case, all other fields are assigned with the pre-defined default value for each configured line.
- The order of the Data fields in the Format line is not significant (unlike the Index-fields). Field values in Data lines are interpreted according to the order specified in the Format line.
- The sign '\$\$' in the Data line means that the user wants the pre-defined default value assigned to the field for the given line.
- The order of 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 should be in exactly the same order.
- A line in a table is identified by its table-name and its indices. Each such line may appear only once in the *ini* file.
- Tables' dependencies:

Certain tables may depend on other tables. For example, one table may include a field, which specifies an entry in another table, 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 order of dependency (i.e., if Table X is referred to by Table Y, then Table X must appear in the *ini* file before Table Y).

5.4.1.4.2 Dynamic Tables versus Static Tables

Static Table

The Static table type does not support adding new lines or removing (deleting) an existing line. All lines in a Static table are pre-configured with default values. Users may modify values in existing lines. After reset, all lines in a Static table are available.

Dynamic Table

The Dynamic table type supports adding and removing lines. It is always initialized as an empty table, with no lines. Users should add lines to the Dynamic table via the *ini* file or at run-time.



Note: Certain Dynamic tables may initialize one or more lines at start-up time. If so, it is documented in the table's specific section.

5.4.1.4.3 Tables in the Uploaded *ini* File

Tables are grouped according to the applications they configure. For example, several tables are required to configure SS7, and other tables are required to configure ATM.

When uploading the *ini* file, the policy is to include only tables that belong to applications, which have been configured (Dynamic tables of other applications are empty, but static tables are not). The trigger for uploading tables is further documented in the applications' specific sections.

5.4.1.4.4 Secret Tables

A table is defined as a secret table if it contains at least one secret data field or if it depends on such a table. A secret data field is a field that must not be revealed to the user. An example of a secret field can be found in an IPSEC application. The IPsec tables are defined as secret tables because the IKE table contains a pre-shared key field, which must not be revealed to the user. The SPD table depends on the IKE table. Therefore, the SPD table is defined as a secret table.

There are two major differences between tables and secret tables:

- The secret field itself can not be viewed via SNMP, Web Server or any other tool.
- *ini* File behavior: These tables are never uploaded in the ini File (e.g., 'Get INI-File from WEB'). Instead, there is a commented title that states that the secret table is present at the board, and is not to be revealed.

Secret tables are always kept in the board's non-volatile memory, and may be overwritten by new tables that should be provided in a new *ini* File. If a secret table appears in an *ini* File, it replaces the current table regardless of its content. The way to delete a secret table from a board is, for example, to provide an empty table of that type (with no data lines) as part of a new *ini* File. The empty table replaces the previous table in the board.

5.4.1.5 Secured Configuration File Download

The *ini* file contains sensitive information required for appropriate functioning of the MediaPack. The *ini* file is uploaded to the MediaPack or downloaded from the gateway using TFTP or HTTP protocols. These protocols are unsecured (and thus vulnerable to a potential hacker). Conversely, if the *ini* file is encoded, the *ini* file would be significantly less vulnerable to outside harm.

5.4.1.5.1 Encoding Mechanism

The *ini* file to be loaded and retrieved is available "as is" or encoded. When an encoded *ini* file is downloaded to the MediaPack, it is also retrieved encoded from the MediaPack. When a decoded file is downloaded to the MediaPack, it is also retrieved decoded from the MediaPack.

In order to create an encoded *ini* file, the user must first create an *ini* file and then apply the **DConvert** utility to it in order to encode it. (Refer to the Appendix, "Utilities" on page 245 for detailed instruction on *ini* file encoding.)

In order to decode an encoded *ini* file retrieved from the MediaPack, the user must retrieve an encoded *ini* file from the MediaPack using the Web server (refer to 'Downloading Auxiliary Files' below) and then use the **DConvert** utility in order to decode it. (Refer to the 'Appendix, "Utilities" on page 245' for detailed instruction on decoding the *ini* file.)

Downloading the *ini* file "as is" or as encoded may be performed by utilizing either TFTP or HTTP.

5.4.2 Auxiliary Files

The auxiliary files are *dat* files each containing the raw data used for a certain task such as Call Progress Tones, Voice Prompts, logo image, etc. *dat* files can be created using the DConvert utility (refer to the Appendix, "Utilities" on page 245) and are downloaded to the MediaPack using TFTP or HTTP via the Software Upgrade Wizard (refer to "Upgrading MediaPack Software" on page 76. This section describes the various types of auxiliary files.

5.4.2.1 Downloading Auxiliary Files

Each auxiliary file has a corresponding *ini* file parameter in the form of [AuxiliaryFileType]FileName. This parameter takes the name of the auxiliary file to be downloaded to the . If the *ini* file does not contain a parameter for a specific auxiliary file type, the uses the last auxiliary file that was stored on the non-volatile memory. The SaveConfiguration *ini* file parameter enables storing the auxiliary files on the non-volatile memory.

The following list contains the *ini* file parameters for the different types of auxiliary files that can be downloaded to the :

- "VoicePromptsFileName" - The name (and path) of the file containing the voice prompts. This file should be constructed using the "TrunkPack Conversion Utility" supplied as part of the software package on the CD accompanying the . The Voice Prompt buffer size in the board is 1 Mbyte.
- "CallProgressTonesFilename" - The name (and path) of the file containing the Call Progress and User-Defined Tones definition.
- "PrerecordedTonesFileName" - The name (and path) of the file containing the

Prerecorded Tones. This file should be constructed using the "TrunkPack Conversion Utility" supplied as part of the software package on the CD accompanying the

- "FXSLoopCharacteristicsFileName" - The name (and path) of the file providing the FXS line characteristic parameters.
- "FXOLoopCharacteristicsFileName" - The name (and path) of the file providing the FXO line characteristic parameters.
- SaveConfiguration - (default = 1 = enabled) This parameter replaces the following parameters: BlastCallProgressSetupFile, BlastVoicePromptsFile. When enabled, all configuration and downloadable files are stored in non-volatile memory.

5.4.2.2 Call Progress Tones, User-Defined Tones and Distinctive Ringing

The Call Progress Tones, User-Defined Tones Configuration and Distinctive Ringing file consists of 3 parts. The first 2 parts contains the definitions of the Call Progress Tones and User-Defined Tones to be detected/generated by the MediaPack. The Call Progress Tones are mostly used for Telephony In-Band Signaling applications (e.g. Ring Back tone).

Each tone may be configured as one of the following types:

- Continuous
- Cadence (up to 4 cadences)
- Burst

A tone may also be configured to be Amplitude Modulated (only 8 of the Call Progress Tones can be AM tones). The Call Progress Tones frequency range is 300 Hz to 1890 Hz. The User-Defined Tones are general purpose tones to be defined by the user. They can be only continues and their frequency range is 300 Hz to 3800 Hz. The maximum amount of tones that may be configured in the User Defined and Call Progress Tones together is 32. The maximum frequencies that may be configured in the User Defined and Call Progress Tones together is 64.

The third part contains the configuration of the Distinctive Ringing patterns to be generated by the MediaPack. Users can use the MediaPack sample configuration files supplied by AudioCodes to construct their own file.

The Call Progress Tones, User-Defined Tones and Distinctive Ringing Configuration file used by the MediaPack is a binary file with the extension *tone.dat*. Only this binary *tone.dat* file can be loaded to a MediaPack. Users can generate their own *tone.dat* file by opening the modifiable *tone.ini* file (supplied with the *tone.dat* file as part of the software package on the CD accompanying the MediaPack) in any text editor, modify it, and convert the modified *tone.ini* back into a binary *tones.dat* file using the DConversion Utility supplied with the MediaPack software package. (Refer to "TrunkPack Downloadable Conversion Utility" on page 245 in the Appendix, "Utilities" for a description of the procedure for generating and downloading the Call Progress Tone file using this utility.)

To load the Call Progress Tones, User-Defined Tones and Distinctive Ringing configuration file to the MediaPack, correctly define their parameters in the MediaPack's *ini* file. (Refer to 'Initialization (*ini*) Files' on page 51 for the *ini* file structure rules and *ini* file example.)



Note: the MP-10x and MP-124 Rev B and MP-124 Rev C have the following limitations regarding the Call Progress and User Defined Tones configurations:

- A call progress tone may consist of up to 2 cadences only.
- Burst tone type is not supported.
- AM tones are not supported.
- Up to 16 tones of any kind are allowed to be configured only.
- Up to 15 different frequencies only may be used.

5.4.2.3 Format of the Call Progress Tones Section

The Call Progress Tones section of the *ini* file format starts from the following string:

[NUMBER OF CALL PROGRESS TONES] - containing the following key only:

- **Number of Call Progress Tones** - defines the number of Call Progress Tones to be 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 -1 defined in the first section) using the following keys:

- **Tone Type** - Call Progress Tone type

Basic Tone Type Indices

1. Dial Tone
2. Ringback Tone
3. Busy Tone
4. Congestion Tone
5. N/A
6. Warning Tone
7. Reorder Tone
8. Confirmation Tone
9. Call Waiting Tone

For a full tone indices list, refer to enum definition in the “VoPLib API Reference Manual”, Document #: LTRT-840xx.

- **Tone Modulation Type** – The tone may be either Amplitude Modulated (1) or regular (0).
- **Tone Form** – The format of the tone may be one of the following indices:
 - Continuous
 - Cadence
 - Burst
- **Low Freq [Hz]** - Frequency in Hertz of the lower tone component for a dual frequency tone, or the frequency of the tone for a single tone. This parameter is relevant only in case the tone is not Amplitude Modulated.

- **High Freq [Hz]** - Frequency in Hertz of the higher tone component for of a dual frequency tone, or zero (0) for a single tone. This parameter is relevant only in case the tone is not modulated.
- **Low Freq Level [-dBm]** - Generation level 0 dBm to -31 dBm. This parameter is relevant only in case the tone is not Amplitude Modulated.
- **High Freq Level [-dBm]** - Generation level. 0 to -31 dBm. The value should be zero (0) for a single tone. This parameter is relevant only in case the tone is not Amplitude Modulated.
- **First Signal On Time [10 msec]** - "Signal On" period (in 10 msec units) for the first cadence ON-OFF cycle, for cadence tone. When a tone is configured to be continuous, this parameter defines the tone On event detection time. When a tone is configured to be burst tone, 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 tone. In case of burst tone, this parameter defines the off time required after burst tone ended until the tone detection is reported. For a continuous tone, this parameter is ignored.
- **Second Signal On Time [10 msec]** - "Signal On" period (in 10 msec units) for the second cadence ON-OFF cycle. This may be omitted if there is no second cadence.
- **Second Signal Off Time [10 msec]** - "Signal Off" period (in 10 msec units) for the second cadence ON-OFF cycle. This may be omitted if there is no second cadence.
- **Third Signal On Time [10 msec]** - "Signal On" period (in 10 msec units) for the third cadence ON-OFF cycle. This may be omitted if there is no third cadence.
- **Third Signal Off Time [10 msec]** - "Signal Off" period (in 10 msec units) for the third cadence ON-OFF cycle. This may be omitted if there is no third cadence.
- **Forth Signal On Time [10 msec]** - "Signal On" period (in 10 msec units) for the forth cadence ON-OFF cycle. This may be omitted if there is no forth cadence.
- **Forth Signal Off Time [10 msec]** - "Signal Off" period (in 10 msec units) for the forth cadence ON-OFF cycle. This may be omitted if there is no forth cadence.
- **Carrier Freq [Hz]** – the Carrier signal frequency in case the tone is Amplitude Modulated.
- **Modulation Freq [Hz]** – The Modulated signal frequency in case the tone is Amplitude Modulated (valid range from 1 Hz to 128 Hz).
- **Signal Level [-dBm]** – the tone level in case the tone is Amplitude Modulated.
- **AM Factor [steps of 0.02]** – Amplitude modulation factor. Valid values: 1 to 50. Recommended values: 10 to 25.
- **Default Duration [msec]** - The default duration (in 1 msec units) of the generated tone.



Note 1: When defining the same frequencies for both a continuous tone and a cadence tone, the Signal On Time parameter of the continuous tone should 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.

Note 2: The tone frequency should differ by at least 40 Hz from one tone to other defined tones.

Note 3: For more information on generating the Call Progress Tones Configuration file, refer to "Converting a CPT '*ini*' File to a Binary '*dat*' File" on page 247 in the Appendix, 'Utilities'.

Note 4: When constructing a CPT *dat* file, the **Use dBm units for Tone levels** checkbox must be marked. This checkbox enables defining the levels in [-dBm] units.

5.4.2.4 Format of the User Defined Tones Section

The User Defined Tones section of the *ini* file format starts from the following string:

[NUMBER OF USER DEFINED TONES] - containing the following key only:

- Number of User Defined Tones - defines the number of User Defined Tones to be defined in the file.

[USER DEFINED TONE #X] - containing the Xth tone definition (starting from 0 and not exceeding the number of User Defined Tones -1 defined in the first section) using the following keys:

- Tone Type – User Defined Tone type

Basic Tone Type Indices

1. Dial Tone
2. Ringback Tone
3. Busy Tone
4. Congestion Tone
5. N/A
6. Warning Tone
7. Reorder Tone
8. Confirmation Tone
9. Call Waiting Tone

For a full tone indices list, refer to enum definition in the "VoPLib API Reference Manual", Document #: LTRT-840xx.

- **Low Freq [Hz]** - Frequency in Hertz of the lower tone component for a dual frequency tone, or the frequency of the tone for a single tone.
- **High Freq [Hz]** - Frequency in Hertz of the higher tone component for of a dual frequency tone, or zero (0) for a single tone.
- **Low Freq Level [-dBm]** - Generation level 0 dBm to -31 dBm.
- **High Freq Level [-dBm]** - Generation level. 0 to -31 dBm. The value should be zero

(0) for a single tone.

- **Default Duration [msec]** - The default duration (in 1 msec units) of the generated tone.

5.4.2.5 Format of the Distinctive Ringing Section

The distinctive ringing section of the *ini* file format starts from string:

[NUMBER OF DISTINCTIVE RINGING PATTERNS] - Contains the following key only:

- Number of Distinctive Ringing patterns - Defines the number of Call Progress Tones to be defined in the file.
- *[Ringing Pattern #X]* - Contains the Xth ringing pattern definition (starting from 1 and not exceeding 16 using the following keys:
 - **Ring Type** - Ring type is equal to the Ringing Pattern number.
 - **Freq [Hz]** - Frequency in Hertz of the ringing tone.
 - **First Ring On Time [10 msec]** - “Ring On” period (in 10 msec units) for the first cadence ON-OFF cycle.
 - **First Ring Off Time [10 msec]** - “Ring Off” period (in 10 msec units) for the first cadence ON-OFF cycle.
 - **Second Ring On Time [10 msec]** - “Ring On” period (in 10 msec units) for the second cadence on-off cycle.
 - **Second Ring Off Time [10 msec]** - “Ring Off” period (in 10 msec units) for the second cadence ON-OFF cycle.
 - **Third Ring On Time [10 msec]** - “Ring On” period (in 10 msec units) for the third cadence ON-OFF cycle.
 - **Third Ring Off Time [10 msec]** - “Ring Off” period (in 10 msec units) for the third cadence ON-OFF cycle.
 - **Fourth Ring Off Time [10 msec]** - “Ring Off” period (in 10 msec units) for the forth cadence ON-OFF cycle.
 - **Fourth Ring Off Time [10 msec]** - “Ring Off” period (in 10 msec units) for the forth cadence ON-OFF cycle.
 - **Burst** - 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/Forth” string and the “Ring On/Off Time”

Using this configuration file, you can create up to 16 different distinctive ringing patterns. Every ringing pattern configures the ringing tone frequency and up to 4 ringing cadences. The same ringing frequency is used for all the ringing pattern cadences. The ringing frequency can be configured in the range from 10 Hz up to 200 Hz with a 5 Hz resolution. Each of the ringing pattern cadences is specified by the following parameters:

- Burst cadence is specified by the “Burst” string. 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.

5.4.2.6 Default Template for Call Progress Tones

The MediaPack is initialized with the default Call Progress Tones configuration. To change one of the tones, edit the default call *progress.txt* file.

For example: to change the dial tone to 440 Hz only, replace the #Dial tone section in the table below with the following text:

```
#Dial tone
[CALL PROGRESS TONE #1]
Tone Type=1
Tone Form = 1
Low Freq [Hz]=440
High Freq [Hz]=0
Low Freq Level [-dBm]=10 (-10dBm)
High Freq Level [-dBm]=0
First Signal On Time [10msec]=300; the dial tone is detected after 3 sec
```

Users can specify several tones of the same type using Tone Type definition. These additional tones are used only for tone detection. Generation of specific tone is according to the first definition of the specific tone. For example, the user can define an additional dial tone by appending the second dial tone definition lines to the tone *ini* file. The MediaPack reports dial tone detection if either one of the two tones is detected.

Table 5-6: Call Progress Tones

[NUMBER OF CALL PROGRESS TONES]	
Number of Call Progress Tones=9	
#Dial tone [CALL PROGRESS TONE #0]	Tone Type=1 Tone Form = 1 (Continuous) Low Freq [Hz]=350 High Freq [Hz]=440 Low Freq Level [-dBm]=13 (-13dBm) High Freq Level [-dBm]=13 First Signal On Time [10msec]=300

Table 5-6: Call Progress Tones

[NUMBER OF CALL PROGRESS TONES]	
Number of Call Progress Tones=9	
#Dial tone [CALL PROGRESS TONE #1]	Tone Type=1 Tone Form = 1 (Continuous) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=10 (-10dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=300
#Ringback [CALL PROGRESS TONE #2]	Tone Type=2 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=480 Low Freq Level [-dBm]=19 (-19dBm) High Freq Level [-dBm]=19 First Signal On Time [10msec]=200 First Signal Off Time [10msec]=400
#Ringback [CALL PROGRESS TONE #3]	Tone Type=2 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=16 (-16dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=100 First Signal Off Time [10msec]=300
#Busy [CALL PROGRESS TONE #4]	Tone Type=3 Tone Form = 2 (Cadence) Low Freq [Hz]=480 High Freq [Hz]=620 Low Freq Level [-dBm]=24 (-24dBm) High Freq Level [-dBm]=24 First Signal On Time [10msec]=50 First Signal Off Time [10msec]=50

Table 5-6: Call Progress Tones

[NUMBER OF CALL PROGRESS TONES]	
Number of Call Progress Tones=9	
#Busy [CALL PROGRESS TONE #5]	Tone Type=3 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=20 (-20dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=50 First Signal Off Time [10msec]=50
#Reorder tone [CALL PROGRESS TONE #6]	Tone Type=7 Tone Form = 2 (Cadence) Low Freq [Hz]=480 High Freq [Hz]=620 Low Freq Level [-dBm]=24 (-24dBm) High Freq Level [-dBm]=24 First Signal On Time [10msec]=25 First Signal Off Time [10msec]=25
#Confirmation tone [CALL PROGRESS TONE #7]	Tone Type=8 Tone Form = 2 (Cadence) Low Freq [Hz]=350 High Freq [Hz]=440 Low Freq Level [-dBm]=20 (-20dBm) High Freq Level [-dBm]=20 First Signal On Time [10msec]=10 First Signal Off Time [10msec]=10
#Call Waiting Tone [CALL PROGRESS TONE #8]	Tone Type=9 Tone Form = 2 (Cadence) Low Freq [Hz]=440 High Freq [Hz]=0 Low Freq Level [-dBm]=20 (-20dBm) High Freq Level [-dBm]=0 First Signal On Time [10msec]=30 First Signal Off Time [10msec]=900

5.4.2.7 Default Template for Distinctive Ringing Patterns

The MediaPack is initialized with the default Distinctive Ringing Patterns configuration (refer to the table below). To change one of the tones, copy the call progress *txt* file and edit the default distinctive ringing section.

For example: to change the Ringing Pattern 2 to frequency of 35 Hz with a burst initial ringing of 300 msec on and 300 msec off

- Replace the ring Freq = 35
- Add 2 new lines with First Burst Ring On/Off Time = 30
- Replace the previous "First Ring On/Off Time" to "Second Ring On/Off Time"

Table 5-7: Number Of Distinctive Ringing Patterns

[NUMBER OF DISTINCTIVE RINGING PATTERNS]
Number of Ringing Patterns=14
#Regular North American Ringing Pattern
[Ringing Pattern #0]
Ring Type=0
Freq [Hz]=20
First Ring On Time [10msec]=200
First Ring Off Time [10msec]=400
#GR-506-CORE Ringing Pattern 1
[Ringing Pattern #1]
Ring Type=1
Freq [Hz]=20
First Ring On Time [10msec]=200
First Ring Off Time [10msec]=400
#GR-506-CORE Ringing Pattern 2
[Ringing Pattern #2]
Ring Type=2
Freq [Hz]=20
First Ring On Time [10msec]=80
First Ring Off Time [10msec]=40
Second Ring On Time [10msec]=80
Second Ring Off Time [10msec]=400

Table 5-7: Number Of Distinctive Ringing Patterns

[NUMBER OF DISTINCTIVE RINGING PATTERNS]
#GR-506-CORE Ringing Pattern 3
[Ringing Pattern #3]
Ring Type=3
Freq [Hz]=20
First Ring On Time [10msec]=40
First Ring Off Time [10msec]=20
Second Ring On Time [10msec]=40
Second Ring Off Time [10msec]=20
Third Ring On Time [10msec]=80
Third Ring Off Time [10msec]=400
#GR-506-CORE Ringing Pattern 4
[Ringing Pattern #4]
Ring Type=4
Freq [Hz]=20
First Ring On Time [10msec]=30
First Ring Off Time [10msec]=20
Second Ring On Time [10msec]=100
Second Ring Off Time [10msec]=20
Third Ring On Time [10msec]=30
Third Ring Off Time [10msec]=400
#GR-506-CORE Ringing Pattern 5 - One single Burst of 500 ms
[Ringing Pattern #5]
Ring Type=5
Freq [Hz]=20
First Burst Ring On Time [10msec]=50
First Burst Ring Off Time [10msec]=50
#EN 300 001 Ring - Belgium
[Ringing Pattern #6]
Ring Type=6
Freq [Hz]=25

Table 5-7: Number Of Distinctive Ringing Patterns

[NUMBER OF DISTINCTIVE RINGING PATTERNS]
First Ring On Time [10msec]=100
First Ring Off Time [10msec]=300
#EN 300 001 Ring - Finland
[Ringing Pattern #7]
Ring Type=7
Freq [Hz]=25
First Ring On Time [10msec]=50
First Ring Off Time [10msec]=550
#EN 300 001 Ring - Germany
[Ringing Pattern #8]
Ring Type=8
Freq [Hz]=25
First Ring On Time [10msec]=95
First Ring Off Time [10msec]=450
#EN 300 001 Ring - Italy
[Ringing Pattern #9]
Ring Type=9
Freq [Hz]=35
First Ring On Time [10msec]=100
First Ring Off Time [10msec]=400
#EN 300 001 Ring - Netherlands & Norway
[Ringing Pattern #10]
Ring Type=10
Freq [Hz]=25
First Ring On Time [10msec]=100
First Ring Off Time [10msec]=400
#EN 300 001 Ring - Sweden
[Ringing Pattern #11]
Ring Type=11

Table 5-7: Number Of Distinctive Ringing Patterns

[NUMBER OF DISTINCTIVE RINGING PATTERNS]
Freq [Hz]=35
First Ring On Time [10msec]= 100
First Ring Off Time [10msec]=500
#EN 300 001 Ring - UK
[Ringing Pattern #12]
Ring Type=12
Freq [Hz]=20
First Ring On Time [10msec]= 40
First Ring Off Time [10msec]= 20
Second Ring On Time [10msec]=40
Second Ring Off Time [10msec]=200
#EN 300 001 Ring - Finland
(informative ringing nr. 3: three ringing bursts preceding cyclic ringing)
[Ringing Pattern #13]
Ring Type=13
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]=400

5.4.2.8 Automatic Update Facility

The MediaPack is capable of automatically downloading updates to the configuration files and firmware image. Any standard web server may be used to host these files.

The Automatic Update processing is performed:

- Upon MediaPack start-up (after the MediaPack is operational)
- At a configurable time of the day, e.g., 18:00 (disabled by default)

- At fixed intervals, e.g., every 60 minutes (disabled by default)

The Automatic Update process is entirely controlled by configuration parameters in the ini file. During the Automatic Update process, the MediaPack contacts the external web server and requests the latest version of a given set of URLs. Configuration ini files are downloaded only if they were modified since the last update.

Below is an example of an ini file activating the Automatic Update facility.

```
# DNS is required for specifying domain names in URLs
DnsPriServerIP = 10.1.1.11

# Load extra configuration ini file using HTTP
INIFILEURL = 'http://webserver.corp.com/AudioCodes/inifile.ini'
# Load call progress tones using HTTPS
# Note: HTTPS is not available on MP-104, MP-108, MP-124 platforms
CPTFILEURL = 'https://10.31.2.17/usa_tones.dat'
# Load voice prompts, using user "root" and password "wheel"
VPFILEURL = 'https://root:wheel@webserver.corp.com/vp.dat'

# Update every day at 03:00 AM
AutoUpdatePredefinedTime = '03:00'
```

Notes on Configuration URLs:

- Additional URLs may be specified, as described in the 'System Parameters' table.
- Updates to non-ini files are performed only once. To update a previously-loaded binary file, you must update the ini file containing the URL for the file.
- To provide differential configuration for each of the devices in a network, add the string "<MAC>" to the URL. This mnemonic is replaced with the hardware (MAC) address of the MediaPack.
- To update the firmware image using the Automatic Update facility, use the CMPFILEURL parameter to point to the image file. As a precaution (in order to protect the MediaPack from an accidental update), you must also set AUTOUPDATECMPFILE to 1.

The following example illustrates how to utilize Automatic Updates for deploying devices with minimum manual configuration, for an "out of the box" experience.

➤ To utilize Automatic Updates for deploying the MP-11x with minimum manual configuration, take these 4 steps:

1. Set up a web server (in this example it is <http://www.corp.com/>) where all the configuration files are to be stored.
2. On each device, pre-configure the following setting: (DHCP/DNS are assumed)

```
INIFILEURL = 'http://www.corp.com/master_configuration.ini'
```

3. Create a file named **master_configuration.ini**, with the following text:

```

# Common configuration for all devices
# -----
CptFileURL = 'http://www.corp.com/call_progress.dat'
# Check for updates every 60 minutes
AutoUpdateFrequency = 60

# Additional configuration per device
# -----
# Each device will load a file named after its MAC address,
# e.g. config_00908F033512.ini
IniFileTemplateURL = 'http://www.corp.com/config_<MAC>.ini'

# Reset the device after configuration has been updated.
# The device will reset after all files were processed.
RESETNOW = 1
  
```

4. You may modify the `master_configuration.ini` file (or any of the `config_<MAC>.ini` files) at any time. The MP-11x queries for the latest version every 60 minutes, and applies the new settings immediately.

5.4.2.9 Modifying the Call Progress Tones File & Distinctive Ringing File

Customers are supplied with a modifiable Call Progress Tone, Distinctive Ringing *ini* file and a non-modifiable Call Progress Tone, Distinctive Ringing *dat* binary file in the software package.

Only the binary *dat* file can be sent to the MediaPack.

In the *ini* file, customers can modify Call Progress Tone levels, Call Progress Tone frequencies and the characteristics of the Distinctive Ringing signal to be detected/generated by the MediaPack, to suit customer-specific requirements. An example of a Call Progress Tone *ini* file name is *usa_tones.ini*. Note that the word 'tones' is defined in the Call Progress Tone and Distinctive Ringing *ini* file name, to differentiate it from the MediaPack's *ini* file.

➤ **To modify these *ini* files and send the *dat* file to the MediaPack, take these 4 steps:**

1. Open the CPT *ini* file (it opens in **Notepad** or in a customer-defined text file editor.)
2. Modify the file in the text file editor according to your specific requirements.
3. Save your modifications and close the file.
4. Convert the file with the DConversion Utility into a binary *dat* file (refer to 'Converting a Modified CPT *ini* File to a *dat* File with the Download Conversion Utility' below).

5.4.2.10 Converting a Modified CPT ini File to a dat File with the Download Conversion Utility

After modifying the original CPT *ini* file (supplied with the MediaPack's software package), you can use the Download Conversion Utility to convert the modified file into a *dat* binary file. You can only send the *dat* file to the MediaPack. The *ini* file cannot be sent.

To convert a modified CPT *ini* file to a binary *dat* file, Run the executable Download Conversion Utility file, *DConvert240.exe*. For more information, refer to the Appendix, 'Utilities' on page 245.

After making the *dat* file, send it to the MediaPack using either:

- The Embedded Web Server GUI's Auxiliary Files. (Refer to "Auxiliary Files Download" on page 161.)

or

- The BootP/TFTP Server to send to the MediaPack the MediaPack's ini file (which simultaneously downloads the Call Progress Tone *dat* file, provided that the MediaPack's ini file parameter CallProgressTonesFilename is defined and provided that both files are located in the same directory.) (Refer to the Appendix, "BootP/TFTP Server" on page 185).

5.4.2.11 Playing Prerecorded Tones (PRT)

The Call Progress Tones and the User-Defined Tones mechanisms have several limitations such as limited number of predefined tones, or limited number of frequency integrations in one tone. To solve these problems and provide a more flexible tone generation capability, prerecorded tones and play can be downloaded to the MediaPack and be played using regular tones generation commands.

5.4.2.12 PRT File Configuration

The PRT file that should be downloaded to the MediaPack is a binary *dat* file, which was created using AudioCodes' DConvert utility. The tones should be recorded (or created using a Signaling Editor) if the user intends to download them in separate PCM files. The PCM files should include the following characteristics:

- Coder: G711 A-law, G711 μ -law or Linear PCM.
- Rate: 8 kHz
- Resolution: 8-bit
- Channels: mono

The PRT module plays the recorded tone repeatedly. This provides the ability to record only part of the tone, while still playing it for a full duration. For example, if a tone has a cadence of 2 seconds on and 4 seconds off, the recorded file should contain only the 6 seconds of the cadence. The PRT module repeatedly plays this cadence for the configured duration. In the same manner, a continuous tone can be played by repeating only part of it.

After the PCM files are properly prepared, these files should be converted into one *dat* file using the DConvert utility. For more information regarding the DConvert utility, and how to make a *dat* PRT file, refer to the Appendix, "BootP/TFTP Server" on page 185.



Note: The maximum number of prerecorded tones that can be stored in one *dat* file is 40.

5.4.2.13 Downloading the PRT *dat* File

Downloading the PRT *dat* file into the MediaPack can be done using one of the following:

- HTTP
- TFTP
- VoPLib API

For HTTP and TFTP download, refer to "Software Upgrade Wizard" on page 155.

For VoPLib API download, refer to the Playing Prerecorded Tones (PRT) section of the VoPLib Application Developer's Manual, Document #: LTRT-844xx.



Note 1: The maximum PRT buffer size is 100KB.

Note 2: If the same tone type was defined as PRT and as Call Progress Tone or User-Defined Tone, the MediaPack plays it using the PRT module.

5.4.2.14 Downloading the dat File to a MediaPack

The purpose of the *coeff.dat* configuration file is to provide the best termination and transmission quality adaptation for different line types. The file consists of a set of parameters for the signal processor of the loop interface devices. This parameter set provides control of the following AC and DC interface parameters:

- DC (V / I curve and max current)
- AC impedance matching
- Transmit gain
- Receive gain
- Hybrid balance
- Frequency response in transmit and receive direction
- Hook thresholds (FXS only)
- Ringing generation and detection parameters
- Metering parameters

This means, for example, that changing impedance matching or hybrid balance requires no hardware modifications, so that a single MediaPack can meet customer-specific requirements. The digital nature of the filters and gain stages also ensures high reliability, no drifts (over temperature or time) and simple variations between different line types.

The *.dat* configuration file is produced by AudioCodes for each market after comprehensive performance analysis and testing and can be modified on request. The current file supports US line type of 600 ohm AC impedance (and for FXS, 40 V RMS ringing voltage for REN = 2).

The following list describes which *coeff.dat* file is to be used with which MP device. The files are located in the Analog_Coefficients_Files folder:

For MP-11x FXS coefficients file types:

- *Mp11x01-1-fxs16khz.dat* - Used for the MP-112/114/118 FXS Media Gateway for 16 kHz metering tone. Impedance and Line Characteristics Matching according to American standard.

For MP-1xx FXO coefficients file types:

- *MP1xx12-1-12khz-fxo.dat* - Used for any MP-1xx, support detection of 12 KHz metering tone.
- *MP1xx12-1-16khz-fxo.dat* - Used for any MP-1xx, support detection of 16 KHz metering tone.
- *MP1xx10-2-16khz-TBR21-fxo.dat* - Used for any MP-1xx , support detection of 16 KHz metering tone, comply with TBR21 standard (Pan European).
- *MP1xx10-4-16khz-fxo-low-frq-ring.dat* - Used for any MP-1xx, support detection of 16 KHz metering tone, enable detection of low ring frequencies (under 20Hz).

Where the case metering type (16Khz or 12 KHz) is not important, use *MP1xx12-1-16khz-fxo.dat*.

For MP-1xx FXS coefficients file types:

- *MP124B10-1-fxs.dat* - Used for MP124 RevB, support generation of 16 KHz metering tone.
- *MP1xx13-1-fxs16khz.dat* - Used for any MP1XX (beside MP124 RevB), support generation of 16 KHz metering tone.
- *MP1xx13-1-fxs12khz.dat* - Used for any MP1XX (beside MP124 RevB), support generation of 12 KHz metering tone.

Where case metering type (16Khz or 12 KHz) is not important, use *MP1xx13-1-fxs16khz.dat*.

The *dat* configuration file is produced by AudioCodes for each market after comprehensive performance analysis and testing, and can be modified on request. The current file supports US line type of 600 ohm AC impedance and 40 V RMS ringing voltage for REN = 2.

In future software releases, it is to be expanded to consist of different sets of line parameters, which can be selected in the *ini* file, for each port.

To support different types of countries and markets, it is necessary to support loading of a new *Coefficients.ini* file. This file consist of AC and DC line parameters for the peripheral devices.

➤ **To send the *Coeff.dat* file to the MP-11x, take this step:**

- Use either the Embedded Web Server GUI's Auxiliary Files. (Refer to "Software Upgrade Wizard" on page 155

or

- The BootP/TFTP Server to send to the MP-11x the MP-11x's *ini* file (which simultaneously downloads the Call Progress Tone *ini* file, provided that the MP-11x's *ini* file parameter CallProgressTonesFilename is defined, and provided that both *ini* files are located in the same directory.) (Refer to 'Appendix, 'BootP/TFTP Server" on page 185).

5.5 Backup Copies of ini and Auxiliary Files

Be sure to separately store a copy of the *ini* file and all auxiliary files, as well as a note of the software version for use should a board require replacement.

5.6 Upgrading MediaPack Software

To upgrade the MediaPack's firmware, load the upgraded firmware cmp file into the MediaPack (and optionally burn it into integral non-volatile memory) using either:

- Embedded Web Server - For a complete description of this option refer to "Software Upgrade Wizard" on page [155](#).
- BootP/TFTP Server - By using the -fb BootP command line switch, the user can direct the board to burn the firmware on the non-volatile memory. The board thereby downloads the specified firmware name via TFTP and also "burns" the firmware on the non-volatile memory. Refer to the Appendix, "BootP/TFTP Server" on page [185](#).



Note: Upgrading the MediaPack's firmware requires reloading the *ini* file and reburning the configuration files. A Software Upgrade Key may be required if the new firmware's version is greater than that listed in the Software Upgrade Key menu (refer to 'Software Upgrade Key Screen').

6 Standard Control Protocols

6.1 General

MediaPack can be controlled from a Media Gateway Controller (MGC)/Call Agent using standard MGCP (Media Gateway Control Protocol), MEGACO (Media Gateway Control) protocol and AudioCodes proprietary TPNCP (TrunkPack Network Control Protocol).

For information on TPNCP, refer to the section on TPNCP in VoPLib Application Developer's Manual, Document #: LTRT-844xx).

MediaPack can be controlled from a Media Gateway Controller (MGC)/Call Agent using standard MGCP.

6.2 MGCP Control Protocol

6.2.1 MGCP Overview

MGCP (Media Gateway Control Protocol) is a standards-based network control protocol (based on the IETF RFC 3435 and RFC 3660 located on the IETF web site). MGCP assumes a call control architecture where the call control intelligence is outside the MediaPack and handled by an external Call Agent. MGCP is a master/slave protocol, where the MediaPack is expected to execute commands sent by the Call Agent.

Since this is a standards-based control protocol, AudioCodes does not provide any special software library to enable users to construct their own Call Agent. (The user is able to choose any one of many such stacks available in the market).



Note: MGCP and MEGACO protocols cannot coexist on the same MediaPack.

The MediaPack currently supports MGCP described in the IETF RFC 2705, located in the IETF web site: '<http://www.ietf.org/rfc/>' <http://www.ietf.org/rfc/>.

6.2.2 MGCP Operation

6.2.2.1 Executing MGCP Commands

MGCP commands, received from an external Call Agent through the IP network, are decoded and executed in the MediaPack. Commands can create new connections, delete connections, or modify the connection parameters.

Several commands support the basic operations required to control a MediaPack:

- Connection commands - Allow the application to create new connections, delete existing connections inside the MediaPack, and modify connection parameters.

- Notify commands - Using notifications, the MediaPack can inform the Call Agent of events occurring on one of the Endpoints. Notify commands can also generate signals on the Endpoints.
- Audit commands - These commands are used to query the MediaPack about Endpoint configuration and state. This information helps in managing and controlling the MediaPack.

Address Array or MGCPCallAgentIPAddr parameter in the ini file. This setting is used only until the first command is received from an actual Call Agent (that is, only for the RSIP message). If the RSIP message is not in use, set this parameter to 0. From then on, the MediaPack uses the address of the “real” Call Agent.

If a Call Agent fails, a redundant Call Agent can immediately take control of the MediaPack by stating to send commands to the MediaPack gateway. For correct operation, only a single Call Agent should control the MediaPack gateway at the same instant.

6.2.3 Using DNS with MGCP

Instead of defining an IP address, a domain name for the Call Agent IP using the 'CallAgentDomainName' and 'RedundantCallAgentDomainName' parameters can be used. DNS (Domain Name System) converts domain names into IP addresses. When the DNS is defined, 'DNSPRISERVERIP' and 'DNSSECSERVERIP' parameters must be configured. While working with domain name, the media gateway MediaPack resolves the name during MediaPack initialization only.

Using the DNS format for notified an entity is not supported. the MediaPack rejects all commands with notified entity in the DNS format.

DNS *ini* file configuration:

```
CallAgentDomainName = 'domain name'
RedundantCallAgentDomainName = 'domain name'
DNSPRISERVERIP = IP address
DNSSECSERVERIP = IP address
CallAgentIP = 0
RedundantAgentIP = 0
```

6.2.4 MGCP KeepAlive Mechanism

The MediaPack does not initialize commands unless it is asked to do so. Therefore, there is an interval of time until the MediaPack notices that its Call Agent is no longer active (the default time interval is 12 sec). The KeepAlive mechanism maintains a constant connection with the Call Agent. In case of Call Agent failure, the MediaPack enters disconnected mode and switches over to its redundant Call Agent. Moreover, since constant transportation is running between the Call Agent and MediaPack, using KeepAlive gives VoIP networks the ability to work with NAT machines.

While the KeepAlive mechanism is enabled, the MediaPack sends an RSIP command when it detects a time interval without commands received from the Call Agent.

The KeepAlive mechanism deactivates itself when the MediaPack loses connection with the Call Agent. KeepAlive messages are sent immediately following the reestablishment of the connection and when no other commands are received during the KeepAlive interval.

ini file parameters:

KeepAliveEnabled = 1 (on) or 0 (off, default) - This parameter can be used to enable a KeepAlive message (NOP ServiceChange).

KeepAliveInterval = 12 (sec, default) - This parameter is used to define the interval in seconds of a KeepAlive message

KeepAlive examples:

While working in endpoint naming conversions:

```
RSIP 2200 *@audiocodes.com MGCP 1.0
```

```
RM: X-KeepAlive
```

While working in trunk naming conversions:

```
RSIP 2420 ds/tr/*/*@audiocodes.com MGCP 1.0
```

```
RM: X-KeepAlive
```

6.2.5 MediaPack Distinctive Ringing Mechanism

MediaPack supports a new advanced Distinctive-Ringing mechanism. This feature configures the ringing frequency and multiple ringing cadences.

The ringing types are configured inside the Call Progress Tone file. For configuration and call progress tone creation refer to, "Modifying the Call Progress Tones File & Distinctive Ringing File" on page 72.

For backward compatibility, the user can ignore this distinctive ringing feature and use the *ini* file parameters for setting ON \ OFF durations and the Call Progress Tone file must not contain distinctive ringing parameters.

Rg signal - "RingOffPeriod", "RingOnPeriod"

R0 - R7 "RingOffPeriod0"-7, "RingOnPeriod0"-7

For example, when setting ring type to 3, the phone rings 1500 msec and then is silent for 3000 msec. This pattern is played for 18000 msec or until the off-hook:

RingOffPeriod3 = 1500

RingOnPeriod3 = 3000

Using the Call Progress Tone file is recommended for the ringing configuration.

6.2.6 SDP Support in MGCP

MGCP supports basic SDP (Session Description Protocol), as defined in RFC 2327. It also supports SDP-ATM, as defined in RFC 3108. However, the only supported attributes in the SDP are:

■ RTPMAP

Used for dynamic payload mapping, to map the number to the coder. The format is:

```
a=rtpmap: 97 G723/8000/1
```

Where: 97 is the payload number to be used

G723 is the encoding name

8000 is the clock rate (optional)

1 is the number of channels (optional)

■ FMTP

Used for dynamic payload mapping, to define coder specific parameters. The format is:

```
a=fmtp: 97 bitrate=5.3
```

Where: 97 is the payload number to be used
 Bitrate is a parameter of the G.723 coder.
 Other supported parameters are:
 mode-set - Defines which mode is used for the AMR and the X-NETCODER coder (0-7)
 annexa - Refers to G.723 if silence suppression is on (yes or no)
 annexb - Refers to G.729 if silence suppression is on (yes or no)

6.2.7 MGCP FAX

6.2.7.1 MGCP Fax Configuration

MGCP offers the following fax configurations.

- MGCP fax package
- Proprietary change-fax-transport type in the local connection options (refer to "Fax Transport Type Setting with Local Connection Options" on page 85) – enables changing the fax transport type without using the T.38 fax package.
- MGCP fax profile "Display Fax Port on Second SDP M Line" (refer to "MGCP Profiling" on page 85). enables negotiating the T.38 fax port without using the T.38 fax package.

Table 6-1: MGCP fax package Loose Mode MP-118

Gateway CH 0	Call Agent	Gateway CH 1
NTFY 2095 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 O: hd	200 2095 OK	
200 16823 OK	RQNT 16823 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 S: L/dl R: D/X(D) D: 2xxx	
NTFY 2096 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 O: 2580	200 2096 OK	
200 16824 OK I: 39	CRCX 16824 ACgw0@[10.4.4.129] MGCP 1.0	

Table 6-1: MGCP fax package Loose Mode MP-118

Gateway CH 0	Call Agent	Gateway CH 1
v=0 o=- 1932071854 0 IN IP4 10.4.4.129 s=- c=IN IP4 10.4.4.129 t=0 0 m=audio 4000 RTP/AVP 18 a=fmtp:18 annexb=yes a=snq: 21 a=cdsc: 1 audio RTP/AVP 18 a=cdsc: 2 image udptl t38 a=T38FaxUdpEC:t38UDPre dundancy a=fmtp:18 annexb=no	C: 1 X: 12 L: a:G729 , fxr/fx:t38 M: recvonly R: fxr/t38	
	CRCX 16825 ACgw1@[10.4.4.129] MGCP 1.0 C: 1 X: 12 L: a:G729 , fxr/fx:t38 M: sendrecv R: fxr/t38 S: L/rg v=0 c=IN IP4 10.4.4.129 m=audio 4000 RTP/AVP 18 a=snq: 0 a=cdsc: 1 audio RTP/AVP 18 a=cdsc: 2 image udptl t38	200 16825 OK l: 40 v=0 o=- 1895854000 0 IN IP4 10.4.4.129 s=- c=IN IP4 10.4.4.129 t=0 0 m=audio 4010 RTP/AVP 18 a=fmtp:18 annexb=yes a=snq: 22 a=cdsc: 1 audio RTP/AVP 18 a=cdsc: 2 image udptl t38 a=T38FaxUdpEC:t38UDPredu ndancy a=fmtp:18 annexb=no
	200 2097 OK	NTFY 2097 ACgw1@[10.4.4.129] MGCP 1.0 X: 12

Table 6-1: MGCP fax package Loose Mode MP-118

Gateway CH 0	Call Agent	Gateway CH 1
		O: hd
200 16826 OK v=0 o=- 1932071854 1 IN IP4 10.4.4.129 s=- c=IN IP4 10.4.4.129 t=0 0 m=audio 4000 RTP/AVP 18 a=fmtp:18 annexb=yes a=sqn: 23 a=cdsc: 1 audio RTP/AVP 18 a=cdsc: 2 image udptl t38 a=T38FaxUdpEC:t38UDPre dundancy a=fmtp:18 annexb=no	MDCX 16826 ACgw0@[10.4.4.129] MGCP 1.0 C: 1 I: 39 X: 12 R: fxr/t38 L: a:G729 M: sendrecv v=0 c=IN IP4 10.4.4.129 m=audio 4010 RTP/AVP 18 a=sqn: 0 a=cdsc: 1 audio RTP/AVP 18 a=cdsc: 2 image udptl t38	
	200 2098 OK	NTFY 2098 ACgw1@[10.4.4.129] MGCP 1.0 X: 12 O: FXR/t38(start)
NTFY 2099 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 O: FXR/t38(start)	200 2099 OK	
200 16827 OK v=0 o=- 1932071854 2 IN IP4 10.4.4.129 s=- c=IN IP4 10.4.4.129 t=0 0 m=image 4002 udptl t38 a=sqn: 24	MDCX 16827 ACgw0@[10.4.4.129] MGCP 1.0 C: 1 I: 39 X: 12 R: fxr/t38 L: a:G729 M: sendrecv	

Table 6-1: MGCP fax package Loose Mode MP-118

Gateway CH 0	Call Agent	Gateway CH 1
a=cdsc: 1 audio RTP/AVP 0 a=cdsc: 2 image udptl t38 a=T38FaxUdpEC:t38UDPre dundancy	v=0 c=IN IP4 10.4.4.129 m=image 4012 udptl t38 a=sqn: 0 a=cdsc: 1 audio RTP/AVP 18 a=cdsc: 2 image udptl t38	
NTFY 2100 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 O: FXR/t38(start)	200 2100 OK	
	MDCX 16828 ACgw1@[10.4.4.129] MGCP 1.0 C: 1 I: 40 X: 12 R: fxr/t38 L: a:G729 M: sendrecv v=0 c=IN IP4 10.4.4.129 m=image 4002 udptl t38 a=sqn: 0 a=cdsc: 1 audio RTP/AVP 18 a=cdsc: 2 image udptl t38	200 16828 OK v=0 o=- 1895854000 1 IN IP4 10.4.4.129 s=- c=IN IP4 10.4.4.129 t=0 0 m=image 4012 udptl t38 a=sqn: 25 a=cdsc: 1 audio RTP/AVP 0 a=cdsc: 2 image udptl t38 a=T38FaxUdpEC:t38UDPredu ndancy
NTFY 2101 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 O: FXR/t38(stop)	200 2101 OK	
	200 2102 OK	NTFY 2102 ACgw1@[10.4.4.129] MGCP 1.0 X: 12 O: FXR/t38(start)

Table 6-1: MGCP fax package Loose Mode MP-118

Gateway CH 0	Call Agent	Gateway CH 1
RQNT 16829 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 R: fxr/t38	200 16829 OK	
	200 16830 OK	RQNT 16830 ACgw1@[10.4.4.129] MGCP 1.0 X: 12 R: fxr/t38
NTFY 2103 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 O: FXR/t38(start)	200 2103 OK	
	200 2104 OK	NTFY 2104 ACgw1@[10.4.4.129] MGCP 1.0 X: 12 O: FXR/t38(stop)
NTFY 2105 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 O: FXR/t38(stop)	200 2105 OK	
NTFY 2106 ACgw0@[10.4.4.129] MGCP 1.0 X: 12 O: hu	200 2106 OK	
	200 2107 OK	NTFY 2107 ACgw1@[10.4.4.129] MGCP 1.0 X: 12 O: hu
DLCX 16831 ACgw0@[10.4.4.129] MGCP 1.0	250 16831 OK	
	250 16832 OK	DLCX 16832 ACgw1@[10.4.4.129] MGCP 1.0

6.2.8 Fax Transport Type Setting with Local Connection Options

In addition to the T.38 fax package described in "Fax Package Definition - FXR" on page 97, the parameter, "x-faxtranstype" can set the Fax Transport Type of each connection to either Transparent, Relay or Transparent with Events. If this parameter is not placed in the Local Connection Options, (LCO) command, the default value configured by the *ini* file parameter is set.

Table 6-2: Fax Transport Type

Fax Mode	Description
x-faxtranstype:transparent	Fax events are ignored
x-faxtranstype:relay	Faxes are transmitted on T.38
x-faxtranstype:transparentwithevents	Fax is transmitted in-band and fax events are detected

6.2.8.1 Display Fax Port on Second M Line

This feature enables users to negotiate the T.38 fax port without using the T.38 fax package. To set this feature, the FaxTransportType parameter is configure to relay T.38. Avoid setting the fax transport type through the MGCP local connects options field (such as in 'Fax Transport Type Setting with Local Connection Options' above).

When this feature is enabled, an SDP response includes an additional media line such as:

```
m=image 4342 udptl t38
```

This example indicates the T.38 fax port 4342 is used.

6.2.9 MGCP Profiling

MGCP has many profiles used for saving backward compatibility. MGCP profile can be set through the *ini* file parameter "MGCPCompatibilityProfile". MGCP profile is bit field therefore each MGCP profile is independent and does not affect the other profiles.

While using the *ini* file parameter each bit should be expressed in decimal numbers.

6.2.10 TGCP Compatibility

To use Trunking Gateway Control Protocol (TGCP) conventions, the user must set the MediaPack to the TGCP profile, e.g., adding MGCPCompatibilityProfile = 32 to the MediaPack's *ini* file.

The following lists the supported TGCP additions:

- Endpoint Naming Scheme - Supports wild card and Endpoint naming conventions.
- Endpoint Name Retrieval - Wild-carded Audit endpoint command supports MaxEndPointIDs, and NumEndPoints parameters.

- Supported Versions - The RestartInProgress response and the AuditEndpoint command have been extended with a VersionSupported parameter to enable Media Gateway controllers and MediaPacks to determine which protocol versions each supports.
- Error Codes - Supports 532 and 533 error codes.

6.2.11 MGCP Coder Negotiation

6.2.11.1 General Background

Control protocols such as MGCP and MEGACO use a special protocol to define the stream characteristics. This protocol is called SDP – “Simple Session Description Protocol” – and it is defined in RFC 2327. The SDP defines (among other things) the IP address and port for the session (or ATM address in case of an ATM session), the media type (audio for voice, data for fax), and codecs to be used for this session. Every codec is represented with the encode method and payload number.

There are two kinds of RTP payloads:

The first type is the fixed payload that was assigned to a known codec. When this kind of payload is used, there is no need for further data, as the number is world wide accepted. Refer to the Appendix, "RTP/RTCP Payload Types" on page 229 for the complete list of fixed coders.

The second type is the dynamic payload, and it is used to define any codec. The range of the dynamic payloads is 96 to 127. When defining a dynamic payload, extra data is needed to map the number to a known codec. This data can be found in the MIME registration of each codec. Currently, the dynamic payloads are not handled in the control protocols, therefore its implementation is described here.

Since MGCP does not have local SDP, it uses Local Connection Options to handle the Dynamic Payload type and uses the advanced coder features.

6.2.11.2 MGCP Coder Negotiation (RFC 3435)

RFC 3435** defines three lists for coder negotiation:

- Internal coders list – this list contains the coders supported by the gateway.
- LCO list – list supplied by the Call Agent.
- RCO list – list supplied by the remote side.

While negotiating coders, the gateway must use the following methodology:

- a. If the Call Agent supplies an LCO list, the media gateway takes an intersection of the LCO and the internal coders lists.
If no match is found, an Error 534 is returned indicating a coder negotiation error.
- b. If the Call Agent supplies both an LCO and an RCO, the media gateway takes an intersection of the list from step a (above) and the RCO list.
If no match is found, an Error 534 is returned indicating a coder negotiation error.
- c. If a match is found, e.g., coders are supported by the board and appear in both lists, the media gateway uses the first voice coder. This coder appears first in the SDP response.

* RFC 3435, Section 2.6, 'Use of Local Connection Options and Connection Descriptors'

- d. If the RCO list is supplied, an intersection is made between the RCO list and internal list.
If no match is found, an Error 505 is returned, indicating an unsupported remote connection descriptor error.
- e. If no LCO list and no RCO list were provided, the media gateway responds with all of its supported coder list e.g., Internal coder list.
The default coder configured in the *ini* file is the first in list.

MGCP and SDP RFCs distinguish between two type of coders: voice coders (G.711, G.729 , GSM, etc.) and non-voice coders (RFC 2833, Comfort noise, etc.). Coder negotiation fails if no voice coder is found during the coder negotiation process.

If several voice coders and non-voice coders are supplied. In the SDP response, voice coder are first in list and non-voice coders are next in list. Coder negotiation are performed on both voice coders and non-voice coders.

RFC 3435, Section 2.6, 'Use of Local Connection Options and Connection Descriptors'

6.2.11.3 Coder Negotiation Configurations

The default coder can be modified in the ini file parameter, 'MGCPDefaultCoder'. An example is: MGCPDefaultCoder='G726'.

Default dynamic payload types are preset. To use proprietary fixed payloads, use the ini file parameter MGCP compatibility profile = 4096 (decimal).

When using the ini file parameter, 'UseNewFormatCoderNegotiaion', according to coder negotiation, if no coder is reported in the LCO, the default coder is used and all supported coders are reported in the SDP response. When the parameter is set to 1 (default), the internal coder list is reported. To prevent the gateway from sending this list, set the parameter to 0 in the ini file.

6.2.11.4 Mapping of Payload Numbers to Coders

The table below shows the default mapping between payload numbers and coders, when the dynamic payload assignment is not used. Coders are supported according to selected DSPVersion templates - DSPVersionTemplateNumber *ini* file parameter.

Table 6-3: MGCP Mapping of Payload Numbers to Coders

Coder	Encoding Name	Default Payload Number
AMR (10.2)	"AMR_10_2", "AMR1020"	70
AMR (12.2)	"AMR_12_2", "AMR1220"	71
AMR (4.75)	"AMR_4_75", "AMR475"	64
AMR (5.15)	"AMR_5_15", "AMR515"	65
AMR (5.9)	"AMR_5_9", "AMR590"	66
AMR (6.7)	"AMR_6_7", "AMR670"	67
AMR (7.4)	"AMR_7_4", "AMR740"	68
AMR (7.95)	"AMR_7_95", "AMR795"	69

Table 6-3: MGCP Mapping of Payload Numbers to Coders

Coder	Encoding Name	Default Payload Number
Comfort Noise	"CN", "COMFORT-NOISE"	13
EVRC	"EVRC"	60
EVRC (TFO)	"X-EVRC_TFO"	81
EVRC (TTY)	"X-EVRC_TTY"	85
G.711 μ law	"PCMU", "G711", "G.711", "G.711U", "G.711MULAW", "G711MULAW"	0
G.726_32	"G726_32"	2
G.729E	"G729E", "G.729E"	63
G.711 A law_64	"PCMA", "G.711A", "G.711ALAW"	8
G.723 (High)	"G723" "G.723" , "G723", "G723HIGH"	4
G.723 (Low)	G723LOW	80
G.726_16	"G726_16"	35
G.726_24	"G726_24"	36
G.726_40	"G726_40"	38
G.727_16	"X-G727_16", "G727"	39
G.727_24	"X-G727_24"	41
G.727_24_16	"X-G727_24_16"	40
G.727_32	"X-G727_32"	44
G.727_32_16	"X-G727_32_16"	42
G.727_32_24	"X-G727_32_24"	43
G.727_40_16	"X-G727_40_16"	45
G.727_40_24	"X-G727_40_24"	46
G.727_40_32	"X-G727_40_32"	47
G.728	"G728"	15
G.729	"G729", "G.729", "G729A"	18
GSM	"GSM"	3
GSM-EFR	"GSM-EFR"	84
NetCoder_4_8	"X-NETCODER_4_8", "NETCODER_4_8"	49
NetCoder_5_6	"X-NETCODER_5_6", "NETCODER_5_6"	50
NetCoder_6_4	"X-NETCODER_6_4", "NETCODER_6_4"	51
NetCoder_7_2	"X-NETCODER_7_2", "NETCODER_7_2"	52

Table 6-3: MGCP Mapping of Payload Numbers to Coders

Coder	Encoding Name	Default Payload Number
NetCoder_8	"X-NETCODER_8", "NETCODER_8"	53
NetCoder_8_8	"X-NETCODER_8_8", "NETCODER_8_8"	54
NetCoder_9_6	"X-NETCODER_9_6", "NETCODER_9_6"	55
QCELP_13	"QCELP"	62
QCELP_13_TFO	"X-QCELP_TFO"	83
QCELP_8	"X-QCELP_8"	61
QCELP_8_TFO	"X-QCELP_8_TFO"	82
Redundancy per RFC 2198	"RED"	104
RFC 2833	"telephone-event"	96
T.38 Fax	"IMAGE/T38"	No Payload
Transparent	"X-CCD", "TRANSPARENT"	56

The MediaPack MGCP supports LINE, DTMF, Generic and handset emulation packages.

Notes for all MGCP Package tables:

R: An x appears in this column if the event can be requested by the Call Agent.

S: If nothing appears in this column for an event, then the event cannot be signaled on command by the Call Agent.

Otherwise, the following symbols identify the type of event:

OO signal: The On/Off signal is turned ON until commanded by the Call Agent to switch it OFF, and vice versa.

TO signal: The Timeout signal lasts for a given duration unless it is superseded by a new signal.

BR signal: The Brief signal event has a short, known duration.

Duration: Specifies the duration of TO signals. Signal duration can be changed by adding time out parameter to signal e.g. L/dl(to=18000) , time units are 1 msec.

When using a digit map, the following notations can be used:

R: D/X(D) **D:** 2xxx|88#|7xx|3xxT|5x.T|93x.#

A map of up to 32 digits can be specified per each Endpoint.

6.2.12 Supported MGCP Packages

6.2.12.1 Generic Media Package - G

Table 6-4: Generic Media Package - G

Symbol	Definition	R	S	Duration
mt	Modem detected	x		
ft	Fax tone detected	x		
rt	Ring back tone		TO	
rbk	Ring back on connection		TO	180 sec

6.2.12.2 DTMF Package - D

Table 6-5: DTMF Package - D

Symbol	Definition	R	S	Duration
0	DTMF 0	x	BR	
1	DTMF 1	x	BR	
2	DTMF 2	x	BR	
3	DTMF 3	x	BR	
4	DTMF 4	x	BR	
5	DTMF 5	x	BR	
6	DTMF 6	x	BR	
7	DTMF 7	x	BR	
8	DTMF 8	x	BR	
9	DTMF 9	x	BR	
#	DTMF #	x	BR	
*	DTMF *	x	BR	
a	DTMF A	x	BR	
b	DTMF B	x	BR	
c	DTMF C	x	BR	
d	DTMF D	x	BR	
t	Inter-digit Timer	x		4 sec

Table 6-5: DTMF Package - D

Symbol	Definition	R	S	Duration
x	Wildcard, match any digit 0 to 9	x		
of	Report Failure	x		

6.2.12.3 Line Package - L

Table 6-6: Line Package - L

Symbol	Definition	R	S	Duration
0-9, #, *, ABCD	DTMF tones		BR	
hd*	Off hook transition	x		
hu*	On hook transition	x		
hf	Flash hook	x		
bz	Busy tone		TO	30 sec
ft	Fax tone event	x		
mt	Modem tones	x		
dl	Dial tone		TO	16 sec
ro	Reorder tone		TO	30 sec
rt	Ring back tone		TO	180 sec
rg	Ringing		TO	180 sec
cf	Confirmation tone		BR	
oc	Report on completion of TO	x		
wt, wt1, wt2, wt3, wt4	Call waiting tones	x	BR	
ci (ti,nu,na)	Caller ID (ci(time, number, name) Time = MM/DD/HH/MN		BR	
sup(addr("digits"))	DTMF dialing		BR	
of	Report Failure	x		
Lsa	Line Side Answer Supervision	x	TO	Infinite
OSI	Network Disconnect		TO	900 ms

Table 6-6: Line Package - L

Symbol	Definition	R	S	Duration
VMWI	Visual Message Waiting Indicator	x	OO	

* Persistence Events

VMWI Signal

A VMWI signal can be generated as an analog signal, e.g. when an analog device raises the voltage on the telephone line, or the VMWI can be played as FSK modem signal, e.g. VMWI is transmitted in same way as Caller ID is played. The user can configure the VMWI method using the "CPPlayDigitalVMWI" *ini* file parameter, 0 = Analog VMWI turn the line voltage high (default), 1 = play FSK signal like caller ID.

It is highly recommended to play an FSK VMWI signal with a ringing signal since most of handsets that support digital VMWI feature detects the FSK signal only after the first ring.

The analog VMWI signal can be turned ON/OFF asynchronously with no relation to other signals.

Network Disconnect (OSI)

Signal Generation - Network Disconnect signal can be played on MediaPack FXS boards only. The Hook current is disconnected according to INI file parameter CurrentDisconnectDuration.

Signal Detection - Network Disconnect signal can be detected on MediaPack FXO boards only. Network disconnect can be detected by: polarity reversal, current disconnect and call progress tone.

The FarEndDisconnectType *ini* file parameter selects which of the methods is to be used: 1:CPT 2:PolarityReversal or 4:CurrentDisconnect

If cpt is selected, the user must specify the tone type using DisconnectToneType = call progress tone type.

For example, DisconnectToneType = 1 means DialTone triggers the network disconnected event. DisconnectToneType = 3 means BusyTone triggers the network disconnected event.

6.2.12.4 Handset Emulation Package - H

Table 6-7: Handset Emulation Package - H

Symbol	Definition	R	S	Duration/Comment
hd	Off hook transition	x	OO	
hu	On hook transition	x	OO	
hf	Flash hook		BR	
bz	Busy tone	x		

Table 6-7: Handset Emulation Package - H

Symbol	Definition	R	S	Duration/Comment
wt, wt1, wt2,wt3,wt4	Call waiting tones	x	BR	
dl	Dial tone (350 Hz & 440 Hz)	x		
nbz	Network busy (fast cycle busy)	x		
rg	Ringing	x		
ro	Reorder tone	x		
oc	Report on completion	x		
ot	Off hook warning tone	x		
sup(addr ("digits"))	DTMF dialing		BR	Example: Supp(addr(2,3,5))
of	Report Failure	x		
Lsa	Line Side Answer Supervision	x	TO	Infinite
OSI	Network Disconnect	x	TO	900 ms

6.2.12.5 PacketCable (NCS) Line Package - L

Table 6-8: PacketCable (NCS) Line Package - L

Symbol	Definition	R	S	Duration/Comment
0-9,*,#,a,b,c,d	DTMF tones	x	BR	
aw	Answer tone	x		
bz	Busy tone		TO	30 sec
cf	Confirmation tone		BR	
ci(ti, nu,na)	Caller ID		BR	ti denotes time nu denotes number na denotes name
dl	Dial tone		TO	
ft	Fax tone	x		
hd	Off-hook transition	P,S		
hf	Flash hook	P		

Table 6-8: PacketCable (NCS) Line Package - L

Symbol	Definition	R	S	Duration/Comment
hu	On-hook transition	P,S		
mt	Modem tones	x		
mwi	Message waiting indicator		TO	16 sec
oc	Operation complete	x		
of	Operation failure	x		
ot	Off-hook warning tone	x		Time-out = infinite
r0, r1, r2, r3, r4, r5, r6 or r7	Distinctive ringing (0...7)		TO	
rg	Ringing		TO	180 sec
ro	Reorder tone		TO	180 sec
rt	Ring back tone		TO	30 sec
sl	Stutter dial tone		C,TO	180 sec
wt, wt1, wt2, wt3, wt4	Call waiting tones	x	BR	
x	DTMF tones wildcard	x		Matches any of the digits "0-9"
OSI	Network Disconnect		TO	900 ms
VMWI	Visual Message Waiting Indicator	x	OO	

6.2.12.6 Announcement Package - A

Table 6-9: Generic Media Package - G

Symbol	Definition	R	S	Duration/Comment
Ann (index)	Play an announcement		TO	Variable
oc	Report on completion			
of	Report failure	x		

6.2.12.7 RTP Package - R

Table 6-10: RTP Package - R

Symbol	Definition	R	S	Duration/Comment
ma	Media Start	C	X	
Rto	RTP/RTCP Timeout	C	X	

RTP/RTCP Timeout (rto(<timeout>,st=<start-time>)):

- time out - optional parameter, increase in 100 msec steps. Maximum value is 12800 msec.
- start-time - optional parameter, default value is "ra".
- If the user does not utilize the event parameters, defaults could be set through *ini* file:
- timeout - "BrokenConnectionEventTimeOut". Default value is 300 msec. Parameter can be changed in 100 msec steps.
- Start-time - "BrokenConnectionEventActivationMode". Default value is 1 - starts after first incoming RTCP packet. While set to zero the timer starts at once.

Event example

```
RQNT 2001 ds/ds1-3/6@gw-o.whatever.net MGCP 1.0
X: 1
R: r/rto(N)
```

In this case a notification occurs if there is a period of time when no RTP or RTCP packets have been received for BrokenConnectionEventTimeOut*100.

The resulting NTFY with observed events would be as follows:

```
NTFY 3002 ds/ds1-3/6@gw-o.whatever.net MGCP 1.0
X: 1
O: r/rto(300)
Another option could be:
RQNT 2001 ds/ds1-3/6@gw-o.whatever.net MGCP 1.0
X: 1
R: r/rto(N)(4000,st=im)
```

In case no RTP is received 4 seconds from the time the event was received, remote disconnected event is generated:

```
NTFY 3002 ds/ds1-3/6@gw-o.whatever.net MGCP 1.0
```

```
X: 1
O: r/rto(300)
```

6.2.12.8 Media Format Parameter Package - FM

Supported FMTP Formats

According to the Media Format Parameter Package, AudioCodes supports the following FMTP formats:

- L:a:codec1;codec2, fmp:"codec1 formatX", fmp:"codec2 formatY"
- L:a:codec1;codec2, fmp:"codec1 formatX";"codec2 formatY"
- L:a:codec1;codec1, fmp:"codec1 formatX"
- L:a:codec1;codec1, fmp:"codec1:2 formatX"

Redundancy

- fmp "red codename1/codename2/.../codenameN"

AMR Family

- fmp: "AMR mode-set=0" (bitrate=4.75)
- fmp: "AMR mode-set=1" (bitrate=5.15)
- fmp: "AMR mode-set=2" (bitrate=5.9)
- fmp: "AMR mode-set=3" (bitrate=6.7)
- fmp: "AMR mode-set=4" (bitrate=7.4)
- fmp: "AMR mode-set=5" (bitrate=7.95)
- fmp: "AMR mode-set=6" (bitrate=10.2)
- fmp: "AMR mode-set=7" (bitrate=12.2)

G.723 Family

- fmp: "G723 bitrate=5.3" Low
- fmp: "G723 bitrate=6.3" High
- fmp: "G723 annexb=yes" VAD on - Voice Activity Detection on
- fmp: "G723 annexb=no" VAD off - Voice Activity Detection off

NetCoder Family

- fmp: "NETCODER mode-set=0" (bitrate=4.75)
- fmp: "NETCODER mode-set=1" (bitrate=5.15)
- fmp: "NETCODER mode-set=2" (bitrate=5.9)
- fmp: "NETCODER mode-set=3" (bitrate=6.7)
- fmp: "NETCODER mode-set=4" (bitrate=7.4)
- fmp: "NETCODER mode-set=5" (bitrate=7.95)
- fmp: "NETCODER mode-set=6" (bitrate=10.2)

G.729 Family

- fntp: "G729 annexb=yes" (VAD on - Voice Activity Detection on)
- fntp: "G729 annexb=no" (VAD off - Voice Activity Detection off)

6.2.12.9 Fax Package Definition - FXR**Table 6-11: Fax Package Definition - FXR**

Symbol	Definition	R	S	Duration/Comment
gwfax	Gateway controlled fax	x		Device controlled fax handling (See below)
nopfax	No special fax handling	x		No special fax handling upon fax (See below)
t38	T.38 fax relay	x		Call Agent controlled T.38 fax relay (See below)

Supported events parameters

- Device Controlled Fax (gwfax) - Device controlled fax handling. The device handled fax event is parameterized with one of the following:
 - Start device handled fax was initiated
 - Stop device handled fax ended normally
 - Failure - The procedure ended abnormally
- No Special Fax Handling (nopfax) - The no special fax handling event is parameterized with one of the following:
 - Start no special fax handling was in place "O: fxr/nopfax(start)"
- T.38 fax relay (t38) Call Agent controlled T.38 fax relay - The Call Agent controlled T.38 fax relay event is parameterized with one of the following:
 - Start Call Agent controlled T.38 fax relay was initiated
 - Stop Call Agent controlled T.38 fax relay

Failure Call Agent controlled T.38 fax relay ended abnormally

6.2.12.10 Extended Line Package - XL**Table 6-12: Extended Line Package - XL**

Symbol	Definition	R	S	Duration/Comment
rev	activates or switches off line reversal on an endpoint	x	TO	Infinite

7 MediaPack Management

Two types of MediaPack management are detailed in this section:

- SNMP-Based Client Program - Refer to 'Using SNMP' below
- Web interface - Refer to "Embedded Web Server" on page 114

7.1 Using SNMP

Simple Network Management Protocol (SNMP) is a standards-based network control protocol for managing elements in a network. The SNMP Manager (usually implemented by a network Management System (NMS) or an Element Management System (EMS)) connects to an SNMP Agent (embedded on a remote Network Element (NE)) to perform network element Operation, Administration and Maintenance (OAM).

Both the SNMP Manager and the NE refer to the same database to retrieve information or configure parameters. This database is referred to as the Management Information Base (MIB), and is a set of statistical and control values. Apart from the standard MIBs documented in IETF RFCs, SNMP additionally enables the use of proprietary MIBs, containing a non-standard information set (specific functionality provided by the Network Element).

Directives, issued by the SNMP Manager to an SNMP Agent, consist of the identifiers of SNMP variables (referred to as MIB object identifiers or MIB variables) along with instructions to either get the value for that identifier, or set the identifier to a new value (configuration). The SNMP Agent can also send unsolicited events towards the EMS, called SNMP traps.

The definitions of MIB variables supported by a particular agent are incorporated in descriptor files, written in Abstract Syntax Notation (ASN.1) format, made available to EMS client programs so that they can become aware of MIB variables and their usage.

The MediaPack contains an embedded SNMP Agent supporting both general network MIBs (such as the IP MIB), VoP-specific MIBs (such as RTP) and AudioCodes' proprietary MIBs (AcBoard, acGateway, AcAlarm and other MIBs) enabling a deeper probe into the inter-working of the Gateway. All supported MIB files are supplied to Customers as part of the release.

7.1.1 About SNMP

7.1.1.1 SNMP Message Standard

Four types of SNMP messages are defined:

- Get - A request that returns the value of a named object.
- Get-Next - A request that returns the next name (and value) of the "next" object supported by a network device given a valid SNMP name.
- Set - A request that sets a named object to a specific value.
- Trap - A message generated asynchronously by network devices. It notifies the network manager of a problem apart from the polling of the device.

Each of these message types fulfills a particular requirement of network managers:

- **Get Request** - Specific values can be fetched via the "get" request to determine the performance and state of the device. Typically, many different values and parameters can be determined via SNMP without the overhead associated with logging into the device, or establishing a TCP connection with the device.
- **Get Next Request** - Enables the SNMP standard network managers to "walk" through all SNMP values of a device (via the "get-next" request) to determine all names and values that a device supports. This is accomplished by beginning with the first SNMP object to be fetched, fetching the next name with a "get-next", and repeating this operation.
- **Set Request** - The SNMP standard provides a action method for a device (via the "set" request) to accomplish activities such as disabling interfaces, disconnecting users, clearing registers, etc. This provides a way of configuring and controlling network devices via SNMP.
- **Trap Message** - The SNMP standard furnishes a mechanism for a device to "reach out" to a network manager on their own (via the "trap" message) to notify or alert the manager of a problem with the device. This typically requires each device on the network to be configured to issue SNMP traps to one or more network devices that are awaiting these traps.

The above message types are all encoded into messages referred to as "Protocol Data Units" (PDUs) that are interchanged between SNMP devices.

7.1.1.2 SNMP MIB Objects

The SNMP MIB is arranged in a tree-structure, similar to a disk directory structure of files. The top level SNMP branch begins with the ISO "internet" directory, which contains four main branches:

- The "mgmt" SNMP branch - Contains the standard SNMP objects usually supported (at least in part) by all network devices.
- The "private" SNMP branch - Contains those "extended" SNMP objects defined by network equipment vendors.
- The "experimental" and "directory" SNMP branches - Also defined within the "internet" root directory, are usually devoid of any meaningful data or objects.

The "tree" structure described above is an integral part of the SNMP standard, though the most pertinent parts of the tree are the "leaf" objects of the tree that provide actual management data regarding the device. Generally, SNMP leaf objects can be partitioned into two similar but slightly different types that reflect the organization of the tree structure:

- **Discrete MIB Objects** - Contain one precise piece of management data. These objects are often distinguished from "Table" items (below) by adding a ".0" (dot-zero) extension to their names. The operator must merely know the name of the object and no other information.
- **Table MIB Objects** - Contain multiple pieces of management data. These objects are distinguished from "Discrete" items (above) by requiring a "." (dot) extension to their names that uniquely distinguishes the particular value being referenced. The "." (dot) extension is the "instance" number of an SNMP object. For "Discrete" objects, this instance number is zero. For "Table" objects, this instance number is the index into the SNMP table. SNMP tables are special types of SNMP objects, which allow parallel arrays of information to be supported. Tables are distinguished from scalar objects, such that tables can grow without bounds. For example, SNMP defines the "ifDescr" object (as a standard SNMP object) that indicates the text description of each

interface supported by a particular device. Since network devices can be configured with more than one interface, this object can only be represented as an array.

By convention, SNMP objects are always grouped in an "Entry" directory, within an object with a "Table" suffix. (The "ifDescr" object described above resides in the "ifEntry" directory contained in the "ifTable" directory).

7.1.1.3 SNMP Extensibility Feature

One of the principal components of an SNMP manager is a "MIB Compiler", which allows new MIB objects to be added to the management system. When a MIB is compiled into an SNMP manager, the manager is made "aware" of new objects that are supported by agents on the network. The concept is similar to adding a new schema to a database.

Typically, when a MIB is compiled into the system, the manager creates new folders or directories that correspond to the objects. These folders or directories can typically be viewed with a "MIB Browser", which is a traditional SNMP management tool incorporated into virtually all network management systems.

The act of compiling the MIB allows the manager to know about the special objects supported by the agent and access these objects as part of the standard object set.

7.1.2 Carrier-Grade Alarm System

The basic alarm system has been extended to a carrier-grade alarm system. A carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account element management system outages, network outages, and transport mechanism such as SNMP over UDP.

A carrier-grade alarm system is characterized by the following:

- The device allows an EMS to determine which alarms are currently active in the device. That is, the device maintains an active alarm table.
- The device allows an EMS to detect lost alarms and clear notifications. [sequence number in trap, current sequence number MIB object]
- The device allows an EMS to recover lost alarm raise and clear notifications [maintains a log history]
- The device sends a cold start trap to indicate that it is starting. This allows the EMS to synchronize its view of the device's active alarms.

When the SNMP alarm traps are sent, the carrier-grade alarm system does not add or delete alarm traps as part of the feature. This system provides the mechanism for viewing of history and current active alarm information.

7.1.2.1 Active Alarm Table

The board maintains an active alarm table to allow an EMS to determine which alarms are currently active in the device. Two views of the active alarm table are supported by the agent:

- acActiveAlarmTable in the enterprise AcAlarm
- alarmActiveTable and alarmActiveVariableTable in the IETF standard AcAlarm MIB (rooted in the MIB tree)

The acActiveAlarmTable is a simple, one-row per alarm table that is easy to view with a MIB browser.

The AcAlarm MIB is currently a draft standard and therefore, has no OID assigned to it. In the current software release, the MIB is rooted in the <ProductName> MIB subtree. In a future release, after the MIB has been ratified and an OID assigned to it, it is to be moved to the official OID.

7.1.2.2 Alarm History

The board maintains a history of alarms that have been raised and traps that have been cleared to allow an EMS to recover any lost raise or clear traps. Two views of the alarm history table are supported by the agent:

- acAlarmHistoryTable in the enterprise AcAlarm
- nlmLogTable and nlmLogVariableTable in the standard NOTIFICATION-LOG-MIB

As with the acActiveAlarmTable, the acAlarmHistoryTable is a simple, one-row per alarm table, that is easy to view with a MIB browser.

7.1.3 Cold Start Trap

MediaPack technology supports a cold start trap to indicate that the unit is starting. This allows the EMS to synchronize its view of the unit's active alarms. In fact, two different traps are sent at start-up:

- The standard coldStart trap - iso(1).org(3).dod(6).internet(1).snmpV2(6).snmpModules(3).snmpMIB(1).snmpMIBObjects(1).snmpTraps(5).coldStart(1) sent at system initialization.
- The enterprise acBoardEvBoardStarted, which is generated at the end of system initialization. This is more of an "application-level" cold start sent after all the initializing process is over and all the modules are ready.

7.1.4 Performance Measurements for a Third-Party System

Performance Measurements are available for a Third-Party Performance Monitoring System through an SNMP interface and can be polled at scheduled intervals by an external poller or utility in the management server or other off board system.

The MediaPack provides performance measurements in the form of two types:

1. **Gauges** - Gauges represent the current state of activities on the media server. Gauges unlike counters can decrease in value and like counters, can increase. The value of a gauge is the current value or a snapshot of the current activity on the media server at that moment.
2. **Counters** - Counters always increase in value and are cumulative. Counters, unlike gauges, never decrease in value unless the server is reset and then the counters are zeroed.

The MediaPack performance measurements are provided by several proprietary MIBs (located under the "acPerformance" sub tree:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).AudioCodes(5003).acPerformance(10).

There are two formats of Performance Monitoring MIBs:

1. Older Format - replaced from version 4.6

Each MIB is made up of a list of single MIB objects, each relating to a separate attribute within a gauge or counter. All counters and gauges give the current time value only.

- **acPerfMediaGateway** - a generic-type of PM MIB that covers:
 - ◆ Control protocol
 - ◆ RTP stream
 - ◆ System packets statistics
- **acPerfMediaServices** - Media services devices specific performance MIB.

2. New Format - includes new MIBs.

They all have an identical structure, which includes two major subtrees:

- **Configuration sub tree** - allows configuration of general attributes of the MIB and specific attributes of the monitored objects.
- **Data sub tree**

The monitoring results are presented in tables. There are one or two indices in each table. If there are two - the first is a sub-set in the table (Example: trunk number) and the second (or the single where there is only one) index represents the interval number (present - 0, previous - 1 and the one before - 2).

The MIBs are:

- **acPMedia** - for media (voice) related monitoring such as RTP and DSP.
- **acPMControl** - for Control Protocol related monitoring such as connections, commands.
- **acPMSystem** - for general (system related) monitoring.

The log trap, acPerformanceMonitoringThresholdCrossing (non-alarm) is sent out every time the threshold of a Performance Monitored object is crossed. The severity field is 'indeterminate' when the crossing is above the threshold and 'cleared' when it goes back under the threshold. The 'source' varbind in the trap indicates the object for which the threshold is being crossed.

7.1.4.1 TrunkPack-VoP Series Supported MIBs - ALL

The TrunkPack-VoP Series contains an embedded SNMP Agent supporting the following MIBs:

- **The Standard MIB (MIB-2)** - The various SNMP values in the standard MIB are defined in RFC 1213. The standard MIB includes various objects to measure and monitor IP activity, TCP activity, UDP activity, IP routes, TCP connections, interfaces, and general system description.
- **RTP MIB** - The RTP MIB is supported according to RFC 2959. It contains objects relevant to the RTP streams generated and terminated by the board and to the RTCP information related to these streams.
- **Notification Log MIB** - This standard MIB (RFC 3014 - iso.org.dod.internet.mgmt.mib-2) is supported as part of AudioCodes' implementation of Carrier Grade Alarms.
- **AcAlarm MIB** - This is an IETF proposed MIB also supported as part of AudioCodes' implementation of Carrier Grade Alarms. This MIB is still not standard and therefore is under the audioCodes.acExperimental branch.

- **SNMP Target MIB** - This MIB is partially supported, (RFC 2273). It allows for configuration of trap destinations and trusted managers only.
- **SNMP Research International enterprise MIBs** - The MediaPack support two SNMP Research International MIBs: SR-COMMUNITY-MIB and TGT-ADDRESS-MASK-MIB. These MIBs are used in configuration of SNMPv2c community strings and trusted managers.



Note: Support for the SR-COMMUNITY-MIB is to be discontinued and it is to be replaced by the standard snmpCommunity MIB in the next applicable version.

In addition to the standard MIBs, the complete product series contains several proprietary MIBs:

- **AcBoard MIB** - This proprietary MIB contains objects related to configuration of the board and channels as well as to run-time information. Through this MIB, users can set up the board configuration parameters, reset the board, monitor the board's operational robustness and quality of service during run-time and receive traps.



Note: The AcBoard MIB is being phased out. It is still supported, but it is being replaced by an updated proprietary MIBs.

The AcBoard MIB has the following Groups:

- boardConfiguration
- boardInformation
- channelConfiguration
- channelStatus
- reset
- acTrap

As noted above, new AudioCodes proprietary MIBs cover the general parameters in the board.

They each contain a Configuration subtree, for configuring the related parameters. In some there also are Status and Action subtrees.

The new AudioCodes proprietary MIBs are:

- **AcAnalog MIB**
- **acControl MIB**
- **acMedia MIB**
- **acPSTN MIB**
- **acSystem MIB**

Other proprietary MIBs are:

- **AcAlarm** - This is a proprietary carrier-grade alarm MIB. It is a simpler implementation of the notificationLogMIB and the IETF suggested alarmMIB (both also supported in all AudioCodes boards).

The acAlarm MIB has the following groups:

- **ActiveAlarm** - straight forward (single indexed) table listing all currently active Alarms together with their bindings (the Alarm bindings are defined in acAlarm. acAlarmVarbinds and also in acBoard.acTrap. acBoardTrapDefinitions. oid_1_3_6_1_4_1_5003_9_10_1_21_2_0).
- **acAlarmHistory** - straight forward (single indexed) table listing all recently raised Alarms together with their bindings (the Alarm bindings are defined in acAlarm. acAlarmVarbinds and also in acBoard.acTrap. acBoardTrapDefinitions. oid_1_3_6_1_4_1_5003_9_10_1_21_2_0).

The table size can be altered via notificationLogMIB.notificationLogMIBObjects.nlmConfig.nlmConfigGlobalEntryLimit or notificationLogMIB.notificationLogMIBObjects.nlmConfig.nlmConfigLogTable.nlmConfigLogEntry.nlmConfigLogEntryLimit.

The table size can be any value between 10 to 100 and the default is 100.



Note 1: The following are special notes pertaining to MIBs:

- A detailed explanation of each parameter can be viewed in an SNMP browser in the MIB Description field.
- Not all groups in the MIB are functional. Refer to version release notes.
- Certain parameters are non-functional. Their MIB status is marked 'obsolete'.
- When a parameter is SET to a new value via SNMP, the change may affect board functionality immediately or may require that the board be soft reset for the change to take effect. This depends on the parameter type.

Note 2: The current (updated) board configuration parameters are programmed into the board provided that the user does not load an *ini* file to the board after reset. Loading an *ini* file after reset overrides the updated parameters.

Additional MIBs are to be supported in future releases.

■ Traps



Note: As of this version all traps are sent out from the SNMP port (default 161). This is part of the NAT traversal solution.

Full AudioCodes proprietary trap definitions and trap Varbinds are found in AcBoard MIB and AcAlarm MIB. For a detailed inventory of traps, refer to the Appendix, "SNMP Alarm Traps" on page [273](#).

The following proprietary traps are supported in the MediaPack:

- **acBoardFatalError** - Sent whenever a fatal board error occurs.
- **acBoardEvResettingBoard** - Sent after a board is reset.
- **acBoardEvBoardstarted** - Sent after a board is successfully restored and initialized following reset.

- **acFeatureKeyError** - Development pending. Intended to relay Feature Key errors etc. (To be supported in the next applicable version)
- **acBoardEthernetLinkAlarm** - Ethernet Link or links are down.
- **acActiveAlarmTableOverflow** - An active alarm could not be placed in the active alarm table because the table is full.
- **acAudioProvisioningAlarm** - Raised if the MediaPack is unable to provision its audio.
- **acOperationalStateChange** - Raised if the operational state of the node goes to disabled. Cleared when the operational state of the node goes to enabled.
- **acKeepAlive** – part of the NAT traversal mechanism. If the STUN application in the MediaPack detects a NAT then this trap is sent out on a regular time laps - 9/10 of the acSysSTUNBindingLifeTime object. The AdditionalInfo1 varbind has the MAC address of the MediaPack.
- **acNATTraversalAlarm** - When the NAT is placed in front a MediaPack, it is identified as a symmetric NAT - this alarm is raised. It is cleared when a non-symmetric NAT or no NAT replace the symmetric one.
- **acEnhancedBITStatus** - This trap is used to for the status of the BIT (Built In Test). The information in the trap contains board hardware elements being tested and their status. The information is presented in the additional info fields.
- **acPerformanceMonitoringThresholdCrossing** - This log trap is sent out for every time the threshold of a Performance Monitored object is crossed. The severity field is 'indeterminate' when the crossing is above the threshold and 'cleared' when it goes back under the threshold. The 'source' varbind in the trap indicates the object for which the threshold is being crossed.

In addition to the listed traps the Board also supports the following standard traps:

- **authenticationFailure**
- **coldStart**

7.1.5 SNMP Interface Details

This section describes details of the SNMP interface needed when developing an Element Management System (EMS) for any of the TrunkPack-VoP Series products, or to manage a device with a MIB browser.

SNMP can be encoded over IPSec. For more details, refer to the Appendix, 'Security' on page 237.

For *ini* file encoding, refer to the Appendix "Utilities" on page 245.

7.1.5.1 SNMP Community Names

By default, the board uses a single, read-only community string of "public" and a single read-write community string of "private".

One can configure up to 5 read-only community strings and up to 5 read-write community strings, and a single trap community string is supported:

7.1.5.1.1 Configuration of Community Strings via the *ini* File

```
SNMPREADONLYCOMMUNITYSTRING_<x> = '#####'
```

SNMPREADWRITECOMMUNITYSTRING_<x> = '#####'

Where <x> is a number between 0 and 4, inclusive. Note that the '#' character represents any alphanumeric character. The maximum length of the string is 20 characters.

7.1.5.1.2 Configuration of Community Strings via SNMP

To configure read-only and read-write community strings, the EM must use the srCommunityMIB. To configure the trap community string, the EM must also use the snmpVacmMIB and the snmpTargetMIB.



Note: Support for the SR-COMMUNITY-MIB is to be discontinued and it is to be replaced by the standard snmpCommunity MIB in the next applicable version.

- **To add a read-only community string, v2user, take this step:**
 - Add a new row to the srCommunityTable with CommunityName v2user and GroupName ReadGroup.
- **To delete the read-only community string, v2user, take these 2 steps:**
 1. If v2user is being used as the trap community string, follow the procedure for changing the trap community string. (See below.)
 2. Delete the srCommunityTable row with CommunityName v2user.
- **To add a read-write community string, v2admin, take this step:**
 - Add a new row to the srCommunityTable with CommunityName of v2admin and GroupName ReadWriteGroup.
- **To delete the read-write community string, v2admin, take these 2 steps:**
 1. If v2admin is being used as the trap community string, follow the procedure for changing the trap community string. (See below.)
 2. Delete the srCommunityTable row with a CommunityName of v2admin and GroupName of ReadWriteGroup.
- **To change the only read-write community string from v2admin to v2mgr, take these 4 steps:**
 1. Follow the procedure above to add a read-write community string to a row for v2mgr.
 2. Set up the EM such that subsequent set requests use the new community string, v2mgr.
 3. If v2admin is being used as the trap community string, follow the procedure to change the trap community string. (See below.)
 4. Follow the procedure above to delete a read-write community name in the row for v2admin.

➤ **To change the trap community string, take these 2 steps:**

The following procedure assumes that a row already exists in the `srCommunityTable` for the new trap community string. The trap community string can be part of the `TrapGroup`, `ReadGroup` or `ReadWriteGroup`. If the trap community string is used solely for sending traps (recommended), then it should be made part of the `TrapGroup`.

1. Add a row to the `vacmSecurityToGroupTable` with these values: `SecurityModel=2`, `SecurityName=the new trap community string`, `GroupName=TrapGroup`, `ReadGroup` or `ReadWriteGroup`. The `SecurityModel` and `SecurityName` objects are row indices.



Note: You must add `GroupName` and `RowStatus` on the same set.

2. Modify the **SecurityName** field in the appropriate row of the `snmpTargetParamsTable`.

7.1.5.2 Trusted Managers

By default, the agent accepts get and set requests from any IP address, as long as the correct community string is used in the request. Security can be enhanced via the use of Trusted Managers. A Trusted Manager is an IP address from which the SNMP agent accepts and process get and set requests. An EM can be used to configure up to 5 Trusted Managers.



Note: If Trusted Managers are defined, then all community strings works from all Trusted Managers. That is, there is no way to associate a community string with particular trusted managers.

7.1.5.2.1 Configuration of Trusted Managers via *ini* File

To set the Trusted Managers table from start up, write the following in the *ini* file:

```
SNMPTRUSTEDMGR_X = D.D.D.D
```

Where X is any integer between 0 and 4 (0 sets the first table entry, 1 sets the second and so on), and D is an integer between 0 and 255.

7.1.5.2.2 Configuration of Trusted Managers via SNMP

To configure Trusted Managers, the EM must use the `srCommunityMIB`, the `snmpTargetMIB` and the `TGT-ADDRESS-MASK-MIB`.

➤ **To add the first Trusted Manager, take these 3 steps:**

The following procedure assumes that there is at least one configured read-write community. There are currently no Trusted Managers. The taglist for columns for all `srCommunityTable` rows are currently empty.

1. Add a row to the `snmpTargetAddrTable` with these values: `Name=mgr0`, `TagList=MGR`, `Params=v2cparams`.
2. Add a row to the `tgtAddressMaskTable` table with these values: `Name=mgr0`, `tgtAddressMask=255.255.255.255:0`. The agent does not allow creation of a row in

this table unless a corresponding row exists in the snmpTargetAddrTable.

3. Set the value of the TransportLabel field on each non-TrapGroup row in the srCommunityTable to MGR.

➤ **To add a subsequent Trusted Manager, take these 2 steps:**

The following procedure assumes that there is at least one configured read-write community. There are currently one or more Trusted Managers. The taglist for columns for all rows in the srCommunityTable are currently set to MGR. This procedure must be done from one of the existing Trusted Managers.

1. Add a row to the snmpTargetAddrTable with these values: Name=mgrN, TagList=MGR, Params=v2cparams, where N is an unused number between 0 and 4.
2. Add a row to the tgtAddressMaskTable table with these values: Name=mgrN, tgtAddressMask=255.255.255.255:0.

An alternative to the above procedure is to set the tgtAddressMask column while you are creating other rows in the table.

➤ **To delete a Trusted Manager (not the final one), take this step:**

The following procedure assumes that there is at least one configured read-write community. There are currently two or more Trusted Managers. The taglist for columns for all rows in the srCommunityTable are currently set to MGR. This procedure must be done from one of the existing trusted managers, but not the one that is being deleted.

- Remove the appropriate row from the snmpTargetAddrTable.

The change takes affect immediately. The deleted trusted manager cannot access the board. The agent automatically removes the row in the tgtAddressMaskTable.

➤ **To delete the final Trusted Manager, take these 2 steps:**

The following procedure assumes that there is at least one configured read-write community. There is currently only one Trusted Manager. The taglist for columns for all rows in the srCommunityTable are currently set to MGR. This procedure must be done from the final Trusted Manager.

1. Set the value of the TransportLabel field on each row in the srCommunityTable to the empty string.
2. Remove the appropriate row from the snmpTargetAddrTable

The change takes affect immediately. All managers can now access the board.

7.1.5.3 SNMP Ports

The SNMP Request Port is 161 and Trap Port is 162

These ports can be changed by setting parameters in the board *ini* file. The parameter name is:

SNMPPort = <port_number>
Valid UDP port number; default = 161

This parameter specifies the port number for SNMP requests and responses.

Usually it should not be specified. Use the default.

7.1.5.4 Multiple SNMP Trap Destinations

An agent can now send traps to up to five managers. For each manager the user needs to set the manager IP and trap receiving port along with enabling the sending to that manager.

7.1.5.5 Trap Manager Configuration via Host Name

A trap manager can be set using the manager's host name. This is currently supported via *ini* file only, using the parameter name, `SNMPTrapManagerHostName`.

When this parameter value is set for this trap, the board at start up tries to resolve the host name. Once the name is resolved (IP is found) the bottom entry in the trap manager's table (and also in the `snmpTargetAddrTable` in the `snmpTargetMIB`) is updated with the IP.

The port is 162 unless specified otherwise. The row is marked as 'used' and sending is 'enabled'.

When using 'host name' resolution, any changes made by the user to this row in either MIBs are overwritten by the board when a resolving is redone (once an hour).



Note: Some traps may be lost until the name resolving is complete.

7.1.5.5.1 Configuration via the *ini* File

In the BOARDNAME board *ini* file, parameters below can be set to enable or disable the sending of SNMP traps. Multiple trap destinations can be supported on the media server by setting multiple trap destinations in the *ini* file.

SNMPMANAGERTRAPSENDINGENABLE_<x> = 0 or 1 indicates if traps are to be sent to the specified SNMP trap manager. A value of '1' means that it is enabled, while a value of '0' means disabled.

Where <x> = a number 0, 1, 2 and is the array element index. Currently up to 5 SNMP trap managers can be supported.

Below is an example of entries in the board *ini* file regarding SNMP. The media server can be configured to send to multiple trap destinations. The lines in the file below are commented out with the ";" at the beginning of the line. All of the lines below are commented out since the first line character is a semi-colon.

```

; SNMP trap destinations
; The board maintains a table of trap destinations containing 5
; rows. The rows are numbered 0..4. Each block of 4 items below
; apply to a row in the table.
; To configure one of the rows, uncomment all 4 lines in that
; block. Supply an IP address and if necessary, change the port
; number.
; To delete a trap destination, set ISUSED to 0.
; -change these entries as needed
;SNMPMANAGERTABLEIP_0=
;SNMPMANAGERTRAPPORT_0=162
;SNMPMANAGERISUSED_0=1
;SNMPMANAGERTRAPSENDINGENABLE_0=1
;
    
```

```

;SNMPMANAGERTABLEIP_1=
;SNMPMANAGERTRAPPORT_1=162
;SNMPMANAGERISUSED_1=1
;SNMPMANAGERTRAPSENDINGENABLE_1=1
;
;SNMPMANAGERTABLEIP_2=
;SNMPMANAGERTRAPPORT_2=162
;SNMPMANAGERISUSED_2=1
;SNMPMANAGERTRAPSENDINGENABLE_2=1
;
;SNMPMANAGERTABLEIP_3=
;SNMPMANAGERTRAPPORT_3=162
;SNMPMANAGERISUSED_3=1
;SNMPMANAGERTRAPSENDINGENABLE_3=1
;
;SNMPMANAGERTABLEIP_4=
;SNMPMANAGERTRAPPORT_4=162
;SNMPMANAGERISUSED_4=1
;SNMPMANAGERTRAPSENDINGENABLE_4=1

```

The 'trap manager host name' is configured via `SNMPTrapManagerHostName`. For example:

```
;SNMPTrapManagerHostName = 'myMananger.corp.MyCompany.com'
```



Note: The same information that is configurable in the *ini* file can also be configured via the `acBoardMIB`.

7.1.5.5.2 Configuration via SNMP

There are two MIB interfaces for the trap managers. The first is via the `acBoard MIB` that has become obsolete and is to be removed from the code in the next applicable version. The second is via the standard `snmpTargetMIB`.

1. Using the `acBoard MIB`:

The following parameters, which are defined in the `snmpManagersTable`:

- `snmpTrapManagerSending`
- `snmpManagersUsed`
- `snmpManagerTrapPort`
- `snmpManagerIP`

When `snmpManagersUsed` is set to zero (not used) the other three parameters are set to zero. (The intent is to have them set to the default value, which means `TrapPort` is to be set to 162. This is to be revised in a later release.)

- ◆ `snmpManagersUsed` Default = Disable(0)

The allowed values are 0 (disable or no) and 1 (enable or yes).

- ◆ `snmpManagerIp` Default = 0.0.0.0

This is known as SNMPMANAGERTABLEIP in the *ini* file and is the IP address of the manager.

- ◆ snmpManagerTrapPort Default = 162

The valid port range for this is 100-4000.

- ◆ snmpManagerTrapSendingEnable Default = Enable(1)

The allowed values are 0 (disable) and 1 (enable).



Note 1: Each of these MIB objects is independent and can be set regardless of the state of snmpManagerIsUsed.

Note 2: If the IsUsed parameter is set to 1, then the IP address for that row should be supplied in the same SNMP PDU.

2. Using the SNMPTargetMIB:

➤ **To add a trap destination, take this step:**

- Add a row to the snmpTargetAddrTable with these values: Name=trapN, TagList=AC_TRAP, Params=v2cparams, where N is an unused number between 0 and 4

All changes to the trap destination configuration take effect immediately.

➤ **To delete a trap destination, take this step:**

- Remove the appropriate row from the snmpTargetAddrTable.

➤ **To modify a trap destination, take this step:**

You can change the IP address and or port number for an existing trap destination. The same effect can be achieved by removing a row and adding a new row.

- Modify the IP address and/or port number for the appropriate row in the snmpTargetAddrTable.

➤ **To disable a trap destination, take this step:**

- Change TagList on the appropriate row in the snmpTargetAddrTable to the empty string.

➤ **To enable a trap destination, take this step:**

- Change TagList on the appropriate row in the snmpTargetAddrTable to "AC_TRAP".

7.1.5.6 SNMP Manager Backward Compatibility

With support of the Multi Manager Trapping feature, there is also a need to support the older acSNMPManagerIP MIB object, which is synchronized with the first index in the snmpManagers MIB table. This is translated in two new features:

- SET/GET to either of the two; is for now identical.
I.e., OID 1.3.6.1.4.1.5003.9.10.1.1.2.7 is identical to OID 1.3.6.1.4.1.5003.9.10.1.1.2.21.1.1.3 as far as the SET/GET are concerned.

- When setting ANY IP to the acSNMPManagerIP (this is the older parameter, not the table parameter), two more parameters are SET to ENABLE. snmpManagerIsUsed.0 and snmpManagerTrapSendingEnable.0 are both set to 1.

7.1.6 SNMP NAT Traversal

A NAT placed between a <product Name> and the element manager calls for traversal solutions:

- **Trap source port** – all traps are sent out from the SNMP port (default – 161). A manager receiving these traps can use the binding information (in the UDP layer) to traverse the NAT back to the device. The trap destination address (port and IP) are as configured in the snmpTargetMIB.
- **acKeepAliveTrap** – this trap is designed to be a constant life signal from the device to the manager allowing the manager NAT traversal at all times. The acBoardTrapGlobalsAdditionalInfo1 varbind has the device's serial number.

The Trap is instigated in three ways:

- Via an *ini* file parameter – 'SendKeepAliveTrap = 1'. This ensures that the trap is continuously sent. The frequency is set via the 9/10 of the acSysSTUNBindingLifeTime object.
- After the STUN client has discovered a NAT (any NAT).
- If the STUN client can not contact a STUN server.



Note: The two latter options require the STUN client be enabled (*ini* file parameter – EnableSTUN).

Also, once the acKeepAlive trap is instigated it does not stop.

- The manager can see the NAT type in the MIB: audioCodes(5003).acProducts(9).acBoardMibs(10).acSystem(10).acSystemStatus(2).acSysNetwork(6).acSysNAT(2).acSysNATType(1)
- The manger also has access to the STUN client configuration: audioCodes(5003).acProducts(9).acBoardMibs(10).acSystem(10).acSystemConfiguration(1).acSysNetworkConfig(3).acSysNATTraversal(6).acSysSTUN(21)
- **acNATTraversalAlarm** - When the NAT is placed in front a device is identified as a symmetric NAT - this alarm is raised. It is cleared when a non-symmetric NAT or no NAT replace the symmetric one.

7.2 Administrative State Control

7.2.1 Node Maintenance

Node maintenance for the MediaPack is provided via an SNMP interface. The acBoardMIB provides two parameters for graceful and forced shutdowns of the MediaPack. (Refer to the note in 'Graceful Shutdown' below.) These parameters are in the acBoardMIB as acgwAdminState and acgwAdminStateLockControl.

The `acgwAdminState` is used either to request (set) a shutdown (0), undo shutdown (2), or to view (get) the gateway condition (0 = locked, 1 = shutting down, 2 = unlocked).

The `acgwAdminStateLockControl` is used to set a time limit for the shutdown (in seconds) where 0 means shutdown immediately (forced), -1 means no time limit (graceful) and x where $x > 0$ indicates a time limit in seconds (timed limit is considered a graceful shutdown).

The `acgwAdminStateLockControl` should be set first followed by the `acgwAdminState`.

7.2.2 Graceful Shutdown

`acgwAdminState` is a read-write MIB object. When a get request is sent for this object, the agent returns the current board administrative state.



Note: Graceful shutdown is currently supported in MEGACO (H.248) only.

The possible values received on a get request are:

- locked(0) - The board is locked
- shuttingDown(1) - The board is in the process of performing a graceful lock
- unlocked(2) - The board is unlocked

On a set request, the manager supplies the desired administrative state, either locked(0) or unlocked(2).

When the board changes to either shuttingDown or locked state, an `adminStateChange` alarm is raised. When the board changes to an unlocked state, the `adminStateChange` alarm is cleared.

Before setting `acgwAdminState` to perform a lock, `acgwAdminStateLockControl` should be set first to control the type of lock that is performed. The possible values are:

- 1 = Perform a graceful lock. Calls are allowed to complete. No new calls are allowed to be originated on this device.
- 0 = Perform a force lock. Calls are immediately terminated.
- Any number greater than 0 - Time in seconds before the graceful lock turns into a force lock.

7.3 Embedded Web Server

The MediaPack boards and modules contain an Embedded Web Server to be used for device configuration and for run-time monitoring. The Embedded Web Server enables users equipped with any standard Web-browsing application such as Microsoft™ Internet Explorer™ (Ver. 5.0 and higher) or Netscape™ Navigator™ (Ver. 7.2 and higher) to:

3. Provision devices (refer to "Advanced Configuration Screen" on page 163)
4. Verify configuration changes in the Status screens (refer to "Status and Diagnostic Menu" on page 148)
5. Load the *ini* file (refer to "Software Upgrade Wizard" on page 155)
6. Load the CMP, Coefficient, Voice Prompt, Prerecorded Tones, and CPT Files (refer to "Auxiliary Files Download" on page 161)

7.3.1 Embedded Web Server Protection & Security Mechanisms

Access to the Embedded Web Server is controlled by the following protection and security mechanisms:

- **Dual Access Level Username and Password** - Refer to 'Username and Password' below
- **Limiting the Web Server GUI to Read-Only Mode** - Refer to 'Limiting the Web Server GUI to Read-Only Mode' below
- **Disabling the Web Server GUI** - Refer to "Disabling the Web Server GUI" on page 116
- **Encrypted HTTP transportation (HTTPS - SSL)** - Refer to 'Encrypted HTTP transport (HTTPS - SSL)' (**Applicable to MP-118 only**)
- **Limiting Web Access to a Predefined List of Client IP Addresses** - Refer to 'Limiting Web Access to a Predefined List of Client IP Addresses' on page 117
- **Managing Web Access Using a RADIUS Server** - Refer to 'Managing Web Server Access Using a RADIUS Server'

7.3.1.1 Username and Password

Username and Password protected dual level Access is provided in the default settings.

Two levels of access are defined:

- **Administrator Level** - 'Read and Write' privileges
- **Monitoring Level** - 'Read Only' privileges

Each of the two access levels has A unique Username and Password combination.

The default Administrator access level Username and Password for all devices is:

- Username: Admin
- Password: Admin

The default Monitoring access level Username and Password for all devices is:

- Username: User
- Password: User

The Enter Network Password dialog is case-sensitive.

If the Embedded Web Server is left idle for more than 5 minutes, the session is expires. Subsequently, when a screen is accessed, you are prompted again for the Username and Password.

For more information about changing the Password and Username for each access level or resetting them to the defaults, refer to "Changing the Password" on page 147.

7.3.2 Limiting the Embedded Web Server to Read-Only Mode

Initially, the Embedded Web Server displays the default parameters that are pre-installed in the board. These parameters can be modified using the Embedded Web Server, either by modifying parameters on the various pages or by loading a text configuration file - an *ini* file to the MediaPack.

Users can limit the Web Server to read-only mode by changing the default of *ini* file parameter `DisableWebConfig`. The read-only mode feature can be used as a security measure. This security level provides protection against unauthorized access (such as Internet hacker attacks), particularly important to users without a firewall.

7.3.2.1 Limiting the Embedded Web Server to Read-Only Mode

Users can limit the Web Server to read-only mode by changing the default of *ini* file parameter `DisableWebConfig`. Use the read-only mode feature as a security measure. This security level provides protection against unauthorized access (such as Internet hacker attacks), particularly important to users without a firewall.

➤ To limit the Web Server to read-only mode:

- Set the *ini* file parameter `DisableWebConfig` to 1 (Default = 0, i.e., read-write mode) and send the modified *ini* file to the device. All Web pages are presented in read-only mode. The ability to modify configuration data is disabled. In addition, users do NOT have access to any file loading page, to the "Change Password" page, to the "SaveConfiguration", or to the "Reset" page.



Note 1: 'Read Only' policy also can be employed by setting `DisableWebConfig` to 0 and distributing the Monitoring level and Administrator level user name password pairs according to the organization's security policy.

Note 2: When `DisableWebConfig` is set to 1 the Dual Access level scheme is overridden, so that a user who is accessing the web server as an Administrator level user to view the web GUI in 'Read Only' mode.

7.3.2.2 Disabling the Embedded Web Server

You can deny access to the device's Web Server by changing the default of *ini* file parameter `DisableWebTask`. The ability to disable access to the device's Web Server via HTTP provides a high level of security in which protection against unauthorized access (such as Internet hacker attacks) is included. This is particularly important to users without a firewall.

➤ To disable the Embedded Web Server:

- Set the *ini* file parameter `DisableWebTask` to 1 (Default = 0, i.e., web task enabled). Access to the device's Web Server is denied.

7.3.2.3 Limiting Web Access to a Predefined List of Client IP Addresses

When client IP addresses are known in advance. Users can define a list of up to 10 client IP addresses that are to be accepted by the Web server. Any client that does not bear an IP address in the predefined list is unable to connect to the Web server. For further details refer to the Appendix, "Security" on page 237.

7.3.3 Correlating PC / MediaPack IP Address & Subnet Mask

Before using the Web browser to access the MediaPack's Embedded Web Server, change the PC's IP address and Subnet Mask to correspond with the MediaPack's factory default IP address and Subnet Mask shown in the table below. For details on changing the IP address and Subnet Mask, refer to the Help information provided by the Operating System used.

Table 7-1: Default IP Address and Subnet Mask

E1/T1 Trunks	IP Address	Subnet Mask
Trunks 9-16	10.1.10.10	255.255.0.0



Note: Note and retain the IP Address and Subnet Mask that you assign to the device. Do the same when defining Username and Password (refer to "Username and Password" on page 115). If the Embedded Web Server is unavailable (for example, if you have lost your Username and Password), use AudioCodes' BootP/TFTP Server to access the device, "reflash" the files and reset the password. For more information on the BootP/TFTP server, refer to the Appendix, "BootP/TFTP Server" on page 185.

7.3.4 Accessing the Embedded Web Server

➤ **To access the Embedded Web Server, take these 2 steps:**

1. Open any standard Web-browser application, such as Microsoft™ Internet Explorer™™ (Ver. 5.0 and higher) or Netscape™™ Navigator™™ (Ver. 7.2 and higher).



Note: The browser must be Java-script enabled. If java-script is disabled, a message box with notification of this is displayed.

2. Specify the IP address of the device in the browser's URL field (e.g., http://10.1.229.17 or https://10.1.229.17 for an SSL secure link). The Embedded Web Server Enter Network Password screen appears.

7.3.5 Accessing the Embedded Web Server

➤ **To access the Embedded Web Server, take these 2 steps:**

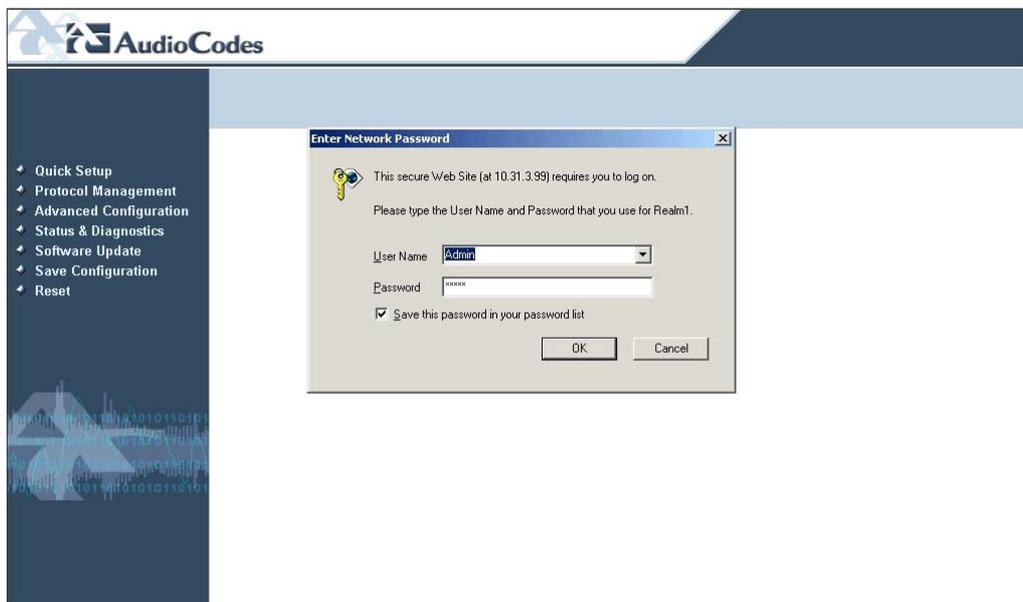
1. Open any standard Web-browser application, such as Microsoft™ Internet Explorer™™ (Ver. 5.0 and higher) or Netscape™™ Navigator™™ (Ver. 7.2 and higher).



Note: The browser must be Java-script enabled. If java-script is disabled, a message box with notification of this is displayed.

2. Specify the IP address of the device in the browser's URL field (e.g., http://10.1.229.17 or https://10.1.229.17 for an SSL secure link). The Embedded Web Server Enter Network Password screen appears.

Figure 7-1: Enter Network Password Screen



7.3.6 Using Internet Explorer to Access the Embedded Web Server

Internet Explorer's security settings may block access to the Gateway's Web browser if they're configured incorrectly. If this happens, the following message appears:

Unauthorized

Correct authorization is required for this area. Either your browser does not perform authorization or your authorization has failed. RomPager server.

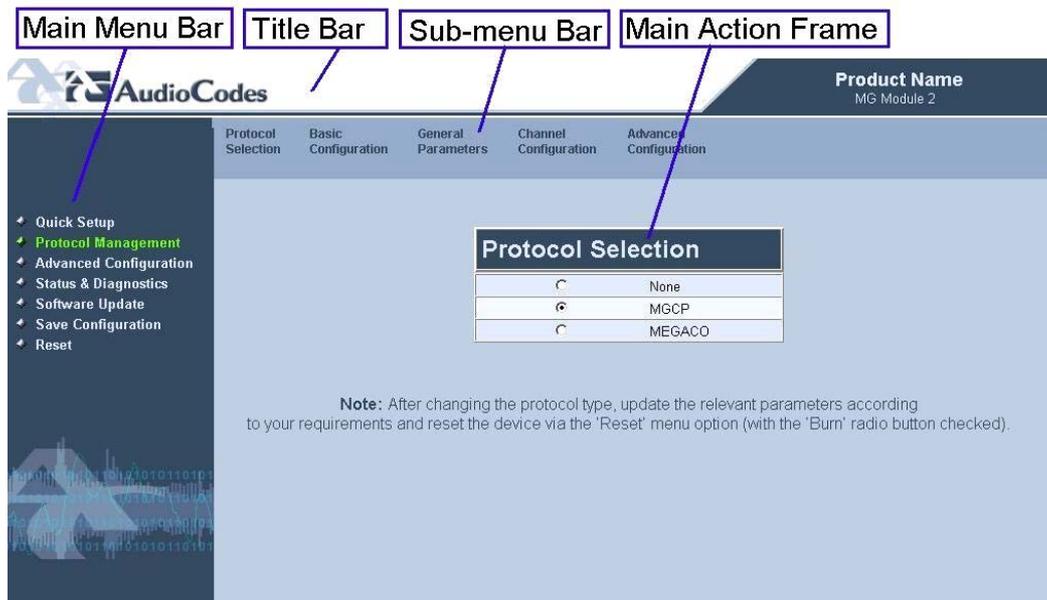
- **To troubleshoot blocked access to Internet Explorer, take these 7 steps:**
1. Delete all cookies from the Temporary Internet files folder. If this does not clear up the problem, the security settings may need to be altered. (Continue to Step 2).
 2. In Internet Explorer, from the Tools menu, select **Internet Options**. The Internet Options dialog box appears.
 3. Select the Security tab, and then, at the bottom of the dialog box, click the **Custom Level** button. The Security Settings dialog box appears.
 4. Scroll down until the Logon options are displayed and change the setting to **Prompt for user name and Password**. Then Click **OK**.
 5. Select the Advanced tab.
 6. Scroll down until the HTTP 1.1 Settings are displayed and verify that the **Use HTTP 1.1** option is checked.
 7. Restart the browser. This fixes any issues related to domain use logon policy.

7.4 Getting Acquainted with the Web Interface

7.4.1 About the Web Interface Screen

The figure below is an example of the General layout of the Web Interface screen.

Figure 7-2: Web Interface Screen - Example



The Web Interface screen contains the following parts:

- **Title bar** - contains the corporate logo, background images and product name

- **Main menu bar** - always appears to the left on every screen for quick access to the other main modules
- **Sub-menu bar** - always appears at the top on every screen and contains links to the sub-menus of the main module selected in the main menu bar to the left
- **Main action pane** - The main area of the screen in which information is viewed and configured

The Web interface is divided into the following 7 modules in the main menu bar to the left:

- **Quick Setup** - Use this module to configure the device's basic settings. (For the full list of configurable parameters go directly to the Protocol Management and Advanced Configuration menus.)
- **Protocol Management** - Use the menus in this module to configure the device's control protocol parameters.
- **Advanced Configuration** - Use the menus in this module to set the device's advanced configuration parameters (for advanced users only).
- **Status & Diagnostics** - Use the menus in this module to view and monitor the device's channels, Syslog messages and hardware / software product information.
- **Software Update** - Use the menus in this module when you want to load new software or configuration files onto the device.
- **Save Configuration** - Use this menu to save configuration changes to the non-volatile (flash) memory.
- **Reset** - Use this menu to remotely reset the device.



Note: To display a short description of a parameter, just position the cursor over the parameter name for a moment.

7.4.2 Saving Changes

To save changes to the volatile memory (RAM) press the **Submit** button (changes to parameters with on-the-fly capabilities are immediately available, other parameters are updated only after a device reset). Parameters that are only saved to the volatile memory revert to their previous settings after hardware reset (software reset i.e., via the Web Interface offers the option to save the changes to the non-volatile memory prior to the reset). To save changes so they are available after a power fail, you must save the changes to the non-volatile memory (flash). When **Save Configuration** is performed, all parameters and loaded files are saved to the non-volatile memory.

- **To save the changes to non-volatile, take the next 2 steps:**
 1. From the main menu on the left, click the **Save Configuration** link. The Save Configuration screen appears.
 2. Click the **Save Configuration** button in the middle of the screen. A confirmation message appears when the save is complete.
- **To quickly setup a MediaPack, take these 12 steps:**
 1. Access the Web Server Interface (refer to "Accessing the Embedded Web Server" on

page 118.)

2. Enter the Administrator level **Username** (default: **Admin**) and **Password** (default: **Admin**).



Note: The Username and Password fields are case-sensitive.

3. Click **OK**. The Quick Setup screen appears.

Figure 7-3: Quick Setup Screen

Quick Setup	
IP Configuration	
IP Address	10.31.3.94
Subnet Mask	255.255.0.0
Default Gateway Address	10.31.0.1
DNS Primary Server IP	0.0.0.0
DNS Secondary Server IP	0.0.0.0
Enable DHCP	Disable
Control Protocol Configuration	
Control Protocol Type	MGCP
Call Agent IP	10.3.1.41
Call Agent Port	2427
Call Agent Domain Name	
Gateway Name	[10.31.3.94]
Endpoint Name	ACgw

4. In the Quick Setup screen, enter or modify appropriate information for the IP Configuration and Control Protocol (per type).
5. In the **IP Configuration** section, **IP Address** and **Subnet Mask** fields, enter the appropriate addresses, which must correspond with your network IP Address settings, or you can enable the DHCP negotiation to start after reset. Refer to "Correlating PC /MediaPack IP Address & Subnet Mask" on page 117.
6. For the **Default Gateway Address**, **DNS Primary Server IP** and **DNS Secondary Server IP** fields, enter appropriate addresses. (If your network features a DNS server, clarify with your Network Administrator).
7. In the **Control Protocol Type** section, for the **Call Agent IP** field, if your network does not feature a DNS server that automatically defines the Call Agent's IP address, enter the appropriate IP address. If you have a DNS server, the field is optional.
8. In the **Call Agent Port** field, enter the appropriate port ID. The default is **2427** for MGCP and **2944** for MEGACO.
9. In the **Call Agent Domain Name** field, when using the DNS server option, enter the Domain Name of the Call Agent operating with the . The DNS server automatically detects the Call Agent's IP address from the Domain Name.
10. If you are working with MGCP, for the **Gateway Name** field, assign a name to the device. (For example: gateway1.com). Ensure that the name you choose is the one

that the Call Manager/Agent is configured with to identify your .

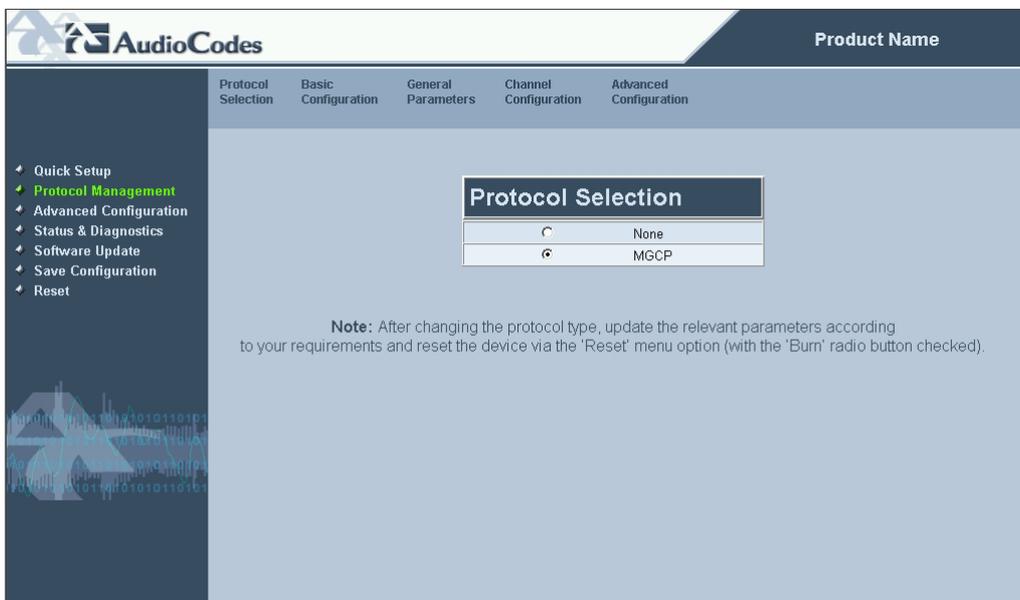
11. If you are working with MGCP, in the Endpoint naming scheme, for the Endpoint Name and Endpoint Numbering Offset fields, enter an appropriate definitions. Ensure that the definitions you choose are the definitions that the Call Manager/Agent is configured with to identify your .
12. At the bottom of the screen, click the **Reset** button. A dialog box appears in which you confirm the reset action. The new information is added to the system configuration while the system is restarted. A message informing you of the waiting period appears. On the MP-11x, the Ready and LAN LEDs are lit green.

7.4.3 Protocol Management

The Protocol Management screen offers access to the following Protocol configuration screens using the Sub-menu bar at the top of the screen:

- **Protocol Selection** - Refer to "Protocol Selection below
 - **Basic Configuration** - Refer to "Basic Configuration" on page [124](#)
 - **General Parameters** - Refer to "General Parameters" on page [125](#)
 - **Channel Configuration** - Refer to "Channel Configuration" on page [127](#)
 - **Advanced Configuration** - Refer to "Advanced Configuration" on page [127](#)
- **To access the Protocol Management menu, take this step:**
- From the main menu list on the left, click on the Protocol Management link. The Protocol Management screen with the sub-menu bar on the top is displayed.

Figure 7-4: Protocol Management Screen



7.4.3.1 Protocol Selection

➤ **To select the protocol type, take these 2 steps:**

1. From the main menu list on the left, click on the Protocol Management link. The Protocol Management screen appears.
2. Click the radio button of the desired protocol.



Note: Changing the protocol type requires a device reset. When you have completed configuring the desired parameters, the device must be reset using the Reset screen (refer to "Reset Button" on page 164) for the changes to be implemented.

7.4.3.2 Basic Configuration

➤ **To configure the Basic Configuration take these 4 steps:**

1. From the main menu list on the left, click on the Protocol Management link. The Protocol Selection screen appears.
2. From the sub-menu bar on the top, click the Basic Configuration link. The Basic Configuration screen appears.

Figure 7-5: Basic Configuration Screen (MGCP)

MGCP Basic Configuration			
Naming Parameters			
Gateway Name	tgw/		
Use Brackets with Gateway Name	Yes		
Naming Method	Endpoint Naming		
Endpoint Name	/c		
Endpoint Numbering Offset	0		
Call Agent Network Configuration			
Call Agent IP	10.10.2.77		
Call Agent Port	2427		
Call Agent Domain Name			
Redundant Call Agent IP	0.0.0.0		
Redundant Call Agent Port	2427		
Redundant Call Agent Domain Name			
Gateway MGCP Port	2427		
<input checked="" type="checkbox"/> Provisioned Call Agents			
Call Agent IP	10.10.2.77	Port	2944
Call Agent IP		Port	0
Call Agent IP		Port	0
Call Agent IP		Port	0
Call Agent IP		Port	0
Call Agent IP		Port	0
Call Agent IP		Port	0

3. Use the 'MGCP Specific Parameters table' on page 223 as a reference when configuring/modifying the Basic Configuration parameter fields in the 'Basic Configuration' screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.3.3 General Parameters

- **To configure the General Parameters take these 4 steps:**
1. From the main menu list on the left, click on the **Protocol Management** link. The Protocol Selection screen appears.
 2. From the sub-menu bar on the top, click the **General Parameters** link. The General Parameters screen appears.

Figure 7-6: General Parameters Screen (MGCP)

MGCP General Configuration	
<input checked="" type="checkbox"/> Profile	
Normal	<input type="checkbox"/>
AUDC MGCP 2	<input checked="" type="checkbox"/>
AUDC MGCP 4	<input type="checkbox"/>
Specific Endpoint (Old)	<input type="checkbox"/>
AUDC MGCP 10	<input type="checkbox"/>
NCS	<input type="checkbox"/>
AUDC MGCP 40	<input type="checkbox"/>
AUDC MGCP 80	<input type="checkbox"/>
AUDC MGCP 100	<input type="checkbox"/>
AUDC MGCP 200	<input type="checkbox"/>
Extended SDP	<input type="checkbox"/>
AUDC MGCP 800	<input type="checkbox"/>
No Dynamic Payload	<input type="checkbox"/>
AUDC MGCP 2000	<input type="checkbox"/>
AUEP Capability	<input type="checkbox"/>
Display Fax Port on Second SDP M Line	<input type="checkbox"/>
Use Evrc as EVRC TTY	<input type="checkbox"/>
Version	MGCP 1.0
Quarantine Mode Status	Loop/Discard
RSIP Parameters	
Send RSIP on Network Disconnection	Yes
Send MAC with RSIP	No
Use Wildcards with RSIP	Yes
Coder	
Default Coder	PCMU
Packetization Period	20
ID Parameters	
Randomize Transaction ID	Yes
Connection ID Base	20
Connection ID Range	999999999
Transaction ID Base	2000
Transaction ID Range	999999999

3. Use the appropriate tables in the Appendix, "Individual *ini* File Parameters" on page 195 as a reference when configuring/modifying the General Configuration parameter fields in the General Parameters screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.
5. Use the appropriate tables in the Appendix, "Individual *ini* File Parameters" on page

195 as a reference when configuring/modifying the General Configuration parameter fields in the General Parameters screen.

6. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.3.4 Channel Configuration

➤ **To configure the Channel Configuration take these 4 steps:**

1. From the main menu list on the left, click on the **Protocol Management** link. The Protocol Selection screen appears.
2. From the sub-menu bar on the top, click the **Channel Configuration** link. The Channel Configuration screen appears.

Figure 7-7: Channel Configuration Screen (MGCP)

MGCP Channel Configuration	
RTP Parameters	
Transparent Coder Payload Type	-1
RTCP Interval Duration	0
Use Single SID Packet with G.729	No
DiffServ Field Value	0
IPTOS Field Value	0
IPPrecedence Field Value	0
DTMF Signal Parameters	
DTMF Signal Time Duration [msec]	100
DTMF Signal Interval Duration [msec]	100
When to Send DTMF Notification	At End of DTMF
Use Transparent DTMF with HBR	No
Misc. Parameters	
Digit Map Timeout [sec]	-1
Time to Trigger a Long Duration on Conn. Event [sec]	3600
Call Waiting Tone Duration [msec]	12000
Enable Caller ID Type II	Enable
Play Announcement to Network Side	No

3. Use the appropriate tables in the Appendix, "Individual '*ini*' File Parameters" on page 195 as a reference when configuring/modifying the Channel Configuration parameter fields in the 'Channel Configuration' screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.3.5 Advanced Configuration

➤ **To configure the Advanced Configuration take these 4 steps:**

1. From the main menu list on the left, click on the **Protocol Management** link. The Protocol Selection screen appears.
2. From the sub-menu bar on the top, click the **Advanced Configuration** link. The Advanced Configuration screen appears.

Figure 7-8: Advanced Configuration Screen (MGCP)

MGCP Advanced Configuration	
Enable Debug Mode	Disable
Enable Keep Alive	Disable
Keep Alive Interval [sec]	12
Retransmission Timeout [msec]	200
Communication Layer Timeout [sec]	30
Use New Coder Negotiation Format	Yes
Activate all Channels on Board Initialization	No
Security	
Default Secret Key Method	Base64

3. Use the appropriate tables in the Appendix, "Individual *'ini'* File Parameters" on page 195 as a reference when configuring/modifying the Advanced Configuration parameter fields in the 'Advanced Configuration' screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.4 Advanced Configuration Screen

➤ **To access the Advanced Configuration screen take this step:**

- To access the device's advanced configuration parameters, from the main menu list on the left, click the **Advanced Configuration** link. The Advanced Configuration Parameters screen appears with the sub-menu bar on the top displaying the following menu options:
 - **Network Settings** - Contains a drop-down list with the following options:
 - ◆ **IP Settings** - Refer to "IP Settings" on page 129
 - ◆ **Application Settings** - Refer to "Application Settings" on page 130
 - ◆ **Web & Telnet Access List** - Refer to "Web & Telnet Access List" on page 131
 - **Security Settings** - Refer to "Security Settings" on page 132
 - **RTP Settings** - Refer to "RTP Settings" on page 137
 - **Routing Table** - Refer to "Routing Table" on page 138

- **Ethernet Port Information** - Refer to "Ethernet Port Information" on page [139](#)
- **VLAN Settings** - Refer to "VLAN Settings" on page [139](#)

Figure 7-9: Network Settings Drop-Down Menu



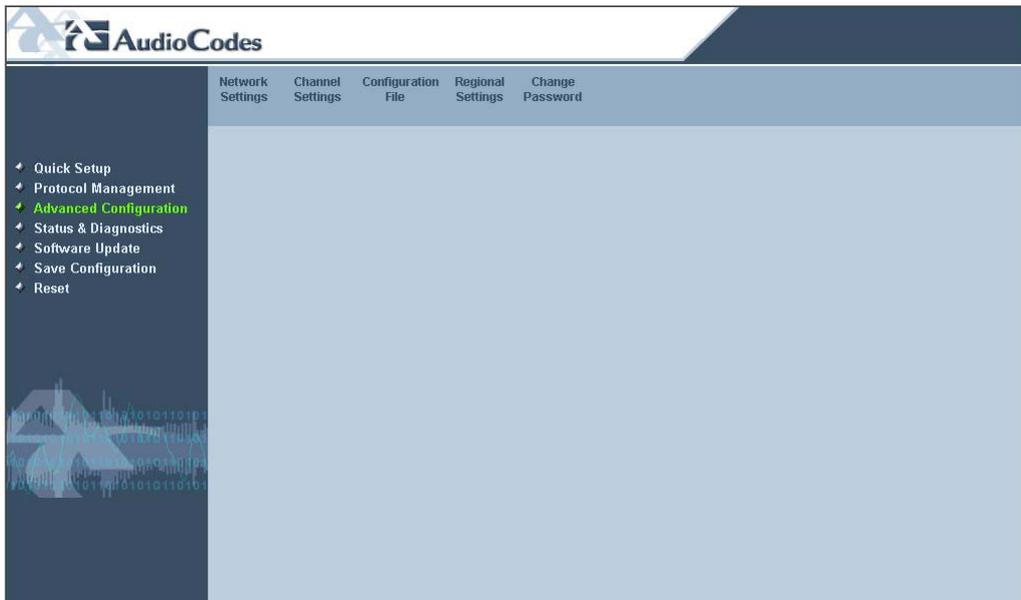
- **Channel Settings** - Contains a drop-down list with the following options:
 - ◆ **Voice Settings** - Refer to "Voice Settings" on page [140](#)
 - ◆ **Fax/Modem/CID Settings** - Refer to "Fax/Modem/CID Settings" on page [141](#)
 - ◆ **RTP Settings** - Refer to "RTP Settings" on page [142](#)
- **Hook-Flash Settings** - Refer to "Hook-Flash Settings" on page [143](#)

Figure 7-10: Channel Settings Drop-Down Menu



- **Configuration File** - Refer to "Configuration File" on page [144](#)
- **Regional Settings** - Refer to "Regional Settings" on page [145](#)
- **Change Password** - Refer to "Change Password" on page [147](#)

Figure 7-11: Advanced Configuration Parameters Screen



7.4.4.1 IP Settings

➤ **To configure the IP Settings, take these 4 steps:**

1. From the main menu list on the left, click on the Advanced Configuration link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, move the cursor on the Network Settings link. A drop-down menu appears. Click on the IP Settings option. The IP Settings screen appears.

Figure 7-12: IP Settings Screen

IP Settings	
IP Networking Mode	Single IP Network
IP Address	10.31.3.97
Subnet Mask	255.255.0.0
Default Gateway Address	10.31.0.1
DNS Settings	
DNS Primary Server IP	
DNS Secondary Server IP	
DHCP Settings	
Enable DHCP	Disable

3. Use the appropriate tables in the Appendix, "Individual *ini* File Parameters" on page 195 as a reference when configuring/modifying the IP Settings parameter fields in the IP Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.4.2 Application Settings

- **To configure the Application Settings, take these 6 steps:**
1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
 2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click on the **Application Settings** option. The Application Settings screen appears.

Figure 7-13: Application Settings Screen

Application Settings	
NTP Settings	
NTP Server IP Address	<input type="text" value="0.0.0.0"/>
NTP UTC Offset	Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/>
NTP Update Interval	Hours <input type="text" value="24"/> Minutes <input type="text" value="0"/>
Syslog Settings	
Syslog Server IP Address	<input type="text" value="10.31.2.63"/>
Enable Syslog	<input type="text" value="Enable"/>
SNMP Settings	
SNMP Managers Table	<input type="button" value="-->"/>
Enable SNMP	<input type="text" value="Enable"/>
Trap Manager Host Name	<input type="text"/>
Telnet Settings	
Embedded Telnet Server	<input type="text" value="Disable"/>
Telnet Server TCP Port	<input type="text" value="23"/>
Telnet Server Idle Timeout	<input type="text" value="0"/>

3. Use the appropriate tables in the Appendix, "Individual *ini* File Parameters" on page 195 as a reference when configuring/modifying the network parameter fields in the Application Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.
5. To access the SNMP Managers table, click the arrow button. The SNMP Manager's Table screen appears.

Figure 7-14: SNMP Manager's Table Screen

SNMP Managers Table*			
	IP Address	Trap Port	Trap Enable
<input checked="" type="checkbox"/> SNMP Manager 1	<input type="text" value="10.31.2.47"/>	<input type="text" value="162"/>	<input type="text" value="Enable"/>
<input type="checkbox"/> SNMP Manager 2	<input type="text" value="100.100.234.235"/>	<input type="text" value="173"/>	<input type="text" value="Enable"/>
<input type="checkbox"/> SNMP Manager 3	<input type="text" value="2.2.2.2"/>	<input type="text" value="162"/>	<input type="text" value="Enable"/>
<input type="checkbox"/> SNMP Manager 4	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	<input type="text" value="Enable"/>
<input type="checkbox"/> SNMP Manager 5	<input type="text" value="0.0.0.0"/>	<input type="text" value="162"/>	<input type="text" value="Enable"/>

* Parameters in this table are changed on-the-fly when SNMP is enabled (no reset is required)

The SNMP Managers table allows you to configure the SNMP managers attributes.



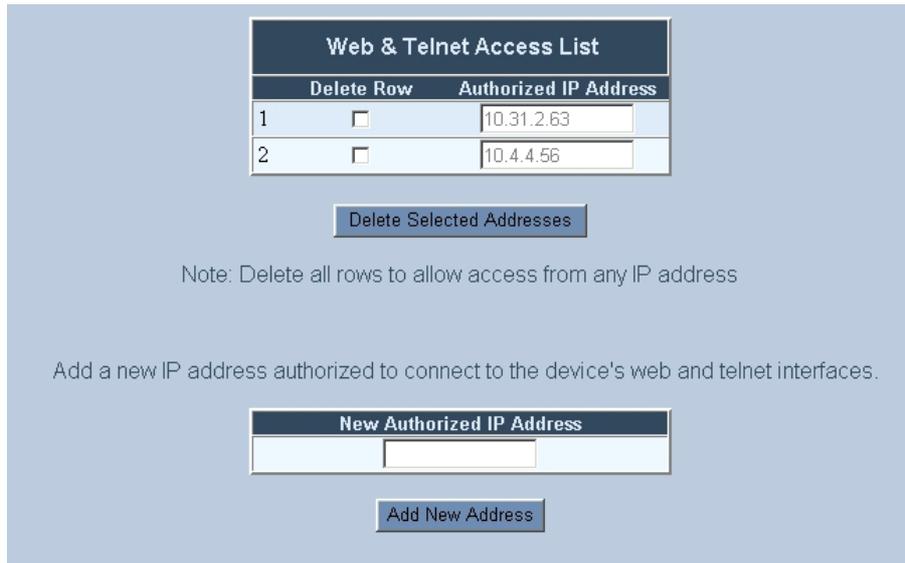
Note: By un-checking a checkbox and clicking submit, the whole table row is deleted. By checking the checkbox and clicking submit, the whole table row is created with the current field inputs in that row.

- Configure the table as desired and click the **SUBMIT** button and then click the **Close Window** button. The lines appear in the Application Settings screen.

7.4.4.3 Web & Telnet Access List

➤ **To configure the Web & Telnet Access List, take these 4 steps:**

- From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
- From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click on the **Web & Telnet Access List** option. The Web & Telnet access List screen appears.

Figure 7-15: Web & Telnet Access List Screen


Web & Telnet Access List	
Delete Row	Authorized IP Address
1 <input type="checkbox"/>	10.31.2.63
2 <input type="checkbox"/>	10.4.4.56

Delete Selected Addresses

Note: Delete all rows to allow access from any IP address

Add a new IP address authorized to connect to the device's web and telnet interfaces.

New Authorized IP Address	
	<input type="text"/>

Add New Address

3. To add a new authorized IP address, in the **New Authorized IP Address** field at the bottom portion of the screen, enter the desired IP address and click the **Add New Address** button.
4. To delete an authorized IP address, in the upper portion of the screen, click a checkmark into the checkbox of the desired IP address row (checkmarks in more than one row is permissible) and click the **Delete Selected Addresses** button.



Note 1: When all authorized IP addresses are deleted this security feature becomes disabled.

Note 2: When adding the first authorized IP address, you should add your own terminal's IP address in order to be able to connect to the web server after adding the first IP address that is not your current terminal's IP address.

7.4.4.4 Security Settings

- **To configure the Security Settings, take these 14 steps:**
 1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
 2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click the **Security Settings** option. The Security Settings screen appears.



Note: IPSec Security Settings availability is in accordance with the 's Software Upgrade Key.

Figure 7-16: Security Settings Screen

Security Settings	
Require Secured Web Connection (HTTPS)	Disable (HTTP and HTTP)
RADIUS Settings	
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	*****
IPSec Settings	
Enable IPSec	Enable
IPSec Table	-->
IKE Table	-->

3. Use the 'Web Interface Parameters table' as a reference when configuring/modifying the **Application Settings** parameter fields in the Application Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

- To access the IPsec table, on the IPsec Table row, click the  arrow button. The IPsec Table screen appears.

Figure 7-17: IPsec Table Screen (Existing Table Row)

IPsec Table

Policy Index 0 State: Exists

[↕ Related key exchange method](#)
[↕ Back to 'Security Settings' page](#)

Remote IP Address	1.1.1.1
Source Port	2000
Destination Port	2000
Protocol	17
Related Key Exchange Method Index	0
SA Life Time [sec]	300
SA Life Time [KB]	25000
First Proposal Encryption Type	DES-CBC
First Proposal Authentication Type	HMAC-SHA-1-96
Second Proposal Encryption Type	Not Defined
Second Proposal Authentication Type	Not Defined
Third Proposal Encryption Type	Not Defined
Third Proposal Authentication Type	Not Defined
Fourth Proposal Encryption Type	Not Defined
Fourth Proposal Authentication Type	Not Defined

Apply
Delete

Figure 7-18: IPSec Table Screen (Non -Existing Table Row)

IPSec Table	
Policy Index	2 State: Does not exist
IPSec table row does not exist	
Back to 'Security Settings' page	
Remote IP Address	
Source Port	0
Destination Port	0
Protocol	0
Related Key Exchange Method Index	0
SA Life Time [sec]	28800
SA Life Time [KB]	0
First Proposal Encryption Type	Not Defined
First Proposal Authentication Type	Not Defined
Second Proposal Encryption Type	Not Defined
Second Proposal Authentication Type	Not Defined
Third Proposal Encryption Type	Not Defined
Third Proposal Authentication Type	Not Defined
Fourth Proposal Encryption Type	Not Defined
Fourth Proposal Authentication Type	Not Defined
<input type="button" value="Create"/>	

6. Each screen represents a single row in the Security Settings table. User can navigate between rows by selecting the desired row index in the **Policy Index** drop-down list at the top of the screen.
7. Table rows may be in 2 states – existent or non-existent – as stated in option showing in the **Policy Index** drop-down list.
8. For an existent row you may delete it by clicking the **Delete** button, or you may re-configure it by configuring the desired parameters and clicking the **Apply** button.
9. For a non existent row you may create it by configuring the parameters and clicking the **Create** button.

- To access the IKE table, click the  arrow button. The IKE Table screen appears.

Figure 7-19: IKE Table Screen (Existing Table Row)

IKE Table

Policy Index: State: Exists ▼

↩ Back to 'Security Settings' page

Shared Key	*****
IKE SA LifeTime [sec]	300
IKE SA LifeTime [KB]	25000
First Proposal Encryption Type	DES-CBC ▼
First Proposal Authentication Type	HMAC-SHA-1-96 ▼
First Proposal DH Group	DH-768-BIT ▼
Second Proposal Encryption Type	Triple DES-CBC ▼
Second Proposal Authentication Type	HMAC-SHA-1-96 ▼
Second Proposal DH Group	DH-1024-BIT ▼
Third Proposal Encryption Type	Triple DES-CBC ▼
Third Proposal Authentication Type	HMAC-SHA-1-96 ▼
Third Proposal DH Group	DH-1024-BIT ▼
Fourth Proposal Encryption Type	DES-CBC ▼
Fourth Proposal Authentication Type	HMAC-MD5-96 ▼
Fourth Proposal DH Group	DH-768-BIT ▼

Figure 7-20: IKE Table Screen (Non -Existing Table Row)

IKE Table	
Policy Index	7 State: Does not exist
'Internet Key Exchange' table row does not exist	
Back to 'Security Settings' page	
Shared Key	*****
IKE SA LifeTime [sec]	28800
IKE SA LifeTime [KB]	0
First Proposal Encryption Type	Not Defined
First Proposal Authentication Type	Not Defined
First Proposal DH Group	Not Defined
Second Proposal Encryption Type	Not Defined
Second Proposal Authentication Type	Not Defined
Second Proposal DH Group	Not Defined
Third Proposal Encryption Type	Not Defined
Third Proposal Authentication Type	Not Defined
Third Proposal DH Group	Not Defined
Fourth Proposal Encryption Type	Not Defined
Fourth Proposal Authentication Type	Not Defined
Fourth Proposal DH Group	Not Defined
<input type="button" value="Create"/>	

11. Each screen represents a single row in the IKE table. User can navigate between rows by selecting the desired row index in the **Policy Index** drop-down list at the top of the screen.
12. Table rows may be in 2 states – existent or non-existent – as stated in the options showing in the **Policy Index** drop-down list.
13. For an existent row you may delete it by clicking the **Delete** button, or you may re-configure it by configuring the desired parameters and clicking the **Apply** button.
14. For a non existent row you may create it by configuring the parameters and clicking the **Create** button.

7.4.4.5 RTP Settings

➤ **To configure the RTP Settings, take these 4 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

- From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click ON the **RTP Settings** option. The RTP Settings screen appears.

Figure 7-21: RTP Settings Screen (Network Settings)

RTP Settings	
RTP Base UDP Port	4000
RTP IP Diff Serv	0
RTP IP TOS	0
RTP IP Precedence	0

- Use the appropriate tables in the Appendix, "Individual 'ini' File Parameters" on page 195 as a reference when configuring/modifying the RTP Settings parameter fields in the RTP Settings screen.
- After configuring/modifying the parameter fields, click the SUBMIT button. The changes are entered into the system and the screen is refreshed.

7.4.4.6 Routing Table

➤ **To configure the Routing Table, take these 4 steps:**

- From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
- From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click ON the **Routing Table** option. The Routing Table screen appears.

Figure 7-22: Routing Table Screen

Routing Table							
Delete Row	Destination IP Address	Destination Mask	Gateway IP Address	TTL	Hop Count	Network Type	
1 <input type="checkbox"/>	0.0.0.0	0.0.0.0	10.31.0.1	Infinite	1	OAM	
2 <input type="checkbox"/>	10.31.0.0	255.255.0.0	10.31.3.96	Infinite	0	OAM	
3 <input type="checkbox"/>	127.0.0.0	255.0.0.0	127.0.0.1	Infinite	1	OAM	
4 <input type="checkbox"/>	127.0.0.1	255.255.255.255	127.0.0.1	Infinite	0	OAM	

Add a new table entry:

Destination IP Address	Destination Mask	Gateway IP Address	Hop Count	Network Type
<input type="text"/>	<input type="text"/>	<input type="text"/>	0	OAM

Note: All fields should have a value

- To add a new routing entry, in the **Add a new table entry** fields at the bottom portion of the screen, enter a the entry data and the click the **Add New Entry** button.

4. To delete an existing entry in the upper portion of the screen, click a checkmark in the checkbox of the desired IP address row (more than one checkmark is permissible) and then click the **Delete Selected Entries** button.

7.4.4.7 Ethernet Port Information

- **To view the Ethernet Port Information, take these 2 steps:**
1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
 2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click the **Ethernet Port Information** option. The Ethernet Port Information screen appears.

Figure 7-23: Ethernet Port Information Screen

Ethernet Port Information	
Active Port	2
Port 1 Duplex Mode	Not Available
Port 1 Speed	Not Available
Port 2 Duplex Mode	Full Duplex
Port 2 Speed	100 mbps

7.4.4.8 VLAN Settings

- **To configure the VLAN Settings, take these 4 steps:**
1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

2. From the sub-menu bar on the top, move the cursor on the **Network Settings** link. A drop-down menu appears. Click the **VLAN Settings** option in the drop-down list. The VLAN Settings screen appears.

Figure 7-24: VLAN Settings Screen

VLAN Settings	
VLAN Mode	Disable
ID Settings	
Native VLAN ID	1
OAM VLAN ID	1
Control VLAN ID	2
Media VLAN ID	3
Priority Settings	
Network Priority	7
Media Premium Priority	6
Control Premium Priority	6
Gold Priority	4
Bronze Priority	2
Differential Services	
Network QoS	48
Media Premium QoS	46
Control Premium QoS	46
Gold QoS	26
Bronze QoS	10

3. Use the "Infrastructure Parameters table" on page 199 as a reference when configuring/modifying the **VLAN Settings** parameter fields in the VLAN Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.4.9 Voice Settings

➤ **To configure the Voice Settings, take these 4 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

2. From the sub-menu bar on the top, move the cursor on the **Channel Settings** link. A drop down menu appears. Click the **Voice Settings** option in the drop down list. The Voice Settings screen appears.

Figure 7-25: Voice Settings Screen

Voice Settings	
Voice Volume (-32 to 31 dB)	0
Input Gain (-32 to 31 dB)	0
Silence Suppression	Disable
Echo Canceler	On
DTMF Transport Type	RFC2833 Relay DTMF
MF Transport Type	RFC2833 Relay MF
DTMF Volume (-31 to 0 dB)	-11
CAS Transport Type	CAS Events Only

3. Use the appropriate tables in the Appendix, "Individual *'ini'* File Parameters" on page 195 as a reference when configuring/modifying the **Voice Settings** parameter fields in the Voice Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.4.10 Fax/Modem/CID Settings

➤ **To configure the Fax/Modem/CID Settings, take these 4 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

2. From the sub-menu bar on the top, move the cursor on the **Channel Settings** link. A drop-down menu appears. Click on the **Fax/Modem/CID Settings** option. The Fax/Modem/CID Settings screen appears.

Figure 7-26: Fax/Modem/CID Settings Screen

Fax/Modem/CID Settings	
Fax Transport Mode	T.38 Relay
Caller ID Transport Type	Mute
Caller ID Type	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 Relay Redundancy Depth	0
Fax Relay Enhanced Redundancy Depth	4
Fax Relay ECM Enable	Enable
Fax Relay Max Rate (bps)	14400
Fax/Modem Bypass Coder Type	G711Alaw
Fax/Modem Bypass Packing Factor	1
CNG Detector Mode	Disable

3. Use the appropriate tables in the Appendix, "Individual *'ini'* File Parameters" on page 195 as a reference when configuring/modifying the Fax/Modem/CID Settings parameter fields in the Fax/Modem/CID Settings screen.
4. After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.4.11 RTP Settings

➤ **To configure the RTP Settings, take these 4 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.

- From the sub-menu bar on the top, move the cursor on the **Channel Settings** link. A drop-down menu appears. Click on the **RTP Settings** option. The RTP Settings screen appears.

Figure 7-27: RTP Settings Screen (Channel Settings)

RTP Settings	
Dynamic Jitter Buffer Minimum Delay	70
Dynamic Jitter Buffer Optimization Factor	7
RTP Redundancy Depth	0
Packing Factor	1
Basic RTP Packet Interval	Default
RTP Directional Control	Transmit-Receive
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	Disable
Analog Signal Transport Type	Ignore analog signals

- Use the appropriate tables in the Appendix, "Individual *ini* File Parameters" on page 195 as a reference when configuring/modifying the RTP Settings parameter fields in the RTP Settings screen.
- After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.4.12 Hook-Flash Settings

➤ **To configure the Hook-Flash Settings, take these 4 steps:**

- From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
- From the sub-menu bar on the top, move cursor on the **Channel Settings** link. A drop-down menu appears. Click the **Hook-Flash Settings** option in the drop-down list. The Hook-Flash Settings screen appears.

Figure 7-28: Hook-Flash Settings Screen

Hook-Flash Settings	
Min. Hook-Flash Detection Period [msec]	300
Max. Hook-Flash Detection Period [msec]	400

- Use the Analog parameters table as a reference when configuring/modifying the Hook-Flash Settings parameter fields in the Hook-Flash Settings screen.
- After configuring/modifying the parameter fields, click the **SUBMIT** button. The changes are entered into the system and the screen is refreshed.

7.4.4.13 Configuration File

The Configuration File screen enables you to restore/change (download a new *ini* file to the Device) or backup the current configuration file that the device is using (make a copy of the VoIP device's *ini* file and store it in a directory on your PC).

1. Restore your configuration - If the VoIP device has been replaced or has lost its programming information, you can restore the VoIP device configuration file from a previous backup or from a newly created *ini* file. To restore the VoIP Device configuration from a previous backup you must have a backup of the VoIP device information stored on your PC. (For information about restoring *ini* file defaults or backup files, refer to 'Restoring and Backing Up the MediaPack Configuration' on page 165'.)
2. Back up your configuration - If you want to protect your VoIP device programming. . The generated backup *ini* file contains values that have been set by the user or are other than the default values.

In the Configuration File screen, you can bring an *ini* file from the device to a directory in your PC, and send the *ini* file from your PC to the device.

Protect the device configuration by bringing the *ini* file from the device to your PC. Later, if another device is replaced or loses its programming data, you'll be able to restore / send the *ini* file backed up on your PC to the device.

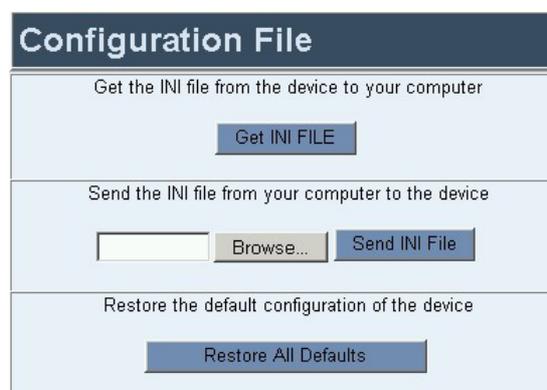
The *ini* file is a proprietary configuration text file containing configuration parameters and data. Sending the *ini* file to the device only provisions parameters that are contained in the *ini* file.

The *ini* file with parameters set at their default values is on the CD accompanying the device. The *ini* file can also be received as an e-mail attachment from AudioCodes' Technical Support. Users can also generate their own *ini* file using AudioCodes' DConvert utility (refer to the Appendix, "Utilities" on page 245).

➤ To save the *ini* file to the PC, take these 3 steps:

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the Advanced Configuration screen, click the **Configuration File** link in the sub-menu bar on the top. The Configuration File screen appears.

Figure 7-29: Configuration File Screen



3. Click the **Get *ini* File** button. You are prompted to select a location in which to save it.



Note: The *ini* file that you save from the device to the PC contains only those parameters whose values you modified following receipt of the device. It does not contain parameters unchanged at their (original) default value.

➤ **To load an ini file from the PC to the device, take these 4 steps:**

1. Click on the **Browse** button next to the **Send the *ini* file from your computer to the device** field and navigate to the location of the predefined *ini* file. Refer to the figure below.
2. Click the **Send File** button. The file loading process is activated. When the loading is complete, a verification message is displayed at the bottom of the screen: **File XXXX was successfully loaded into the device.**
3. From the main menu list on the left, click **Reset**. The Reset screen appears.
4. Select the **Burn** option and click the **Restart** button. Wait for the device to reset. After self-testing, the Ready and LAN LEDs on the device's front panel are lit green. Any malfunction causes the Ready LED to change to red. Users can restore default parameters by clicking the **Restore All Defaults** button.

7.4.4.14 Regional Settings

From the Regional Settings screen users can send a Call Progress Tones *dat* file, a Coefficient *dat* file and/or a Voice Prompts *dat* file to the device from their PC.

➤ **To access the Regional Settings screen, take these 2 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, click the **Regional Settings** link. The Regional Settings screen appears. Used for Sending CPT, Coefficient and/or Voice Prompt File to the Device.

Figure 7-30: Regional Settings Screen

YYYY	MM	DD	Hour	Min	Sec	
2000	1	1	2	51	9	Set Date & Time

The files are available on the CD accompanying your device. They can also be received as an e-mail attachment from AudioCodes' Technical Support. A Call Progress Tones *txt* file can be modified and converted into the binary *dat* file (refer to "Converting a CPT '*ini*' File to a Binary '*dat*' File" on page 247 in the Appendix, 'Utilities'). When modifying the Call Progress Tones File and Distinctive Ringing File, only the *dat* file can be sent from your PC to the device. (Refer to 'Modifying the Call Progress Tones File and Distinctive Ringing File' on page 72 and 'Appendix, 'Utilities' on page 245.)

- The Call Progress Tones *dat* file is a region-specific, telephone exchange-dependent file. It provides call status/call progress to Customers, operators, and connected equipment. Default Tone: U.S.A.
- The Coefficient *dat* file must be sent to the device in order to match subscriber line characteristics.
- The *dat* Voice Prompts file is played by the device during the phone conversation on Call Agent request. Download if you have an application requiring Voice Prompts. The Voice Prompt buffer size in the board is 1 Mbyte.

➤ **To send a Call Progress Tone, Coefficient, or Voice Prompt file to the board, take these 6 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, click the **Regional Settings** link. The Regional Settings screen appears. (Refer to the figure below.)
3. Click the **Browse** button to locate the predefined **Call Progress Tone, Coefficient, or Voice Prompt** file as appropriate. (A new software file package may be issued from AudioCodes or your local supplier.)
4. Click the **Send File** button. The file is sent to the board, overwriting the previous one. The screen is refreshed and a message informs you about the waiting period. When the loading is complete, a verification message is displayed at the bottom of the screen: **File XXX was successfully loaded into the device.**
5. For CPT file downloading only - (The rest of files do not require a device reset.) From the main menu list on the left, click **Reset**. The Reset screen appears.
6. Select the **Burn** option and click the **Restart** button. Wait for the device to reset. After self-testing, the Ready and LAN LEDs on the device's front panel are lit green. Any malfunction causes the Ready LED to change to red.

➤ **To set the date and time, take these 2 steps:**

1. Enter the date and/or time using the **YYYY, MM, and DD** field for Year, Month and Day and **HH, MM, and SS** fields for Hour, Minutes and Seconds.
2. Click the **Set Date and Time** button. The date and time is set on the device, accordingly.



Note: When the NTP feature is enabled (the NTP server is defined in the Network Settings screen), the date and time are in **Read Only** mode as they are set by the NTP server.

7.4.4.14.1 Change Password

➤ **To change the Password, take these 4 steps:**

1. From the main menu list on the left, click on the **Advanced Configuration** link. The Advanced Configuration screen appears.
2. From the sub-menu bar on the top, click the **Change Password** link. The Change Password screen appears.



Note: A user with Administrator privileges may change both Administrator and Monitoring level passwords. A user with Monitoring privileges may change only the Monitoring level password.

Figure 7-31: Change Password Screen - For Users with Administrator Privileges

Change Password	
New User Name	<input type="text"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

For applying changes to the Administrator access level click the 'Change Administrator Password' button otherwise, for applying changes to the Monitoring access level click the 'Change Monitoring Password' button.

After changing the current access level password you will be prompted to re-enter the updated password.

Note: Your current access level password is the default password.
For security reasons, you are recommended to change your password.

Figure 7-32: Change Password Screen - For Users with Monitoring Privileges

Change Password	
New User Name	<input type="text"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

Note: Your current access level password is the default password.
For security reasons, you are recommended to change your password.

3. Enter a User Name and New Password into the fields and confirm the New Password in the **Confirm Password** field.
4. To apply new settings to the Administrator level, click the **Change Administrator Password** button. You are prompted to enter a new username and password. The

new username/password takes effect immediately.

To apply new settings to the Monitoring level, click the Change Monitoring Password button. The new username/password takes effect immediately.

When making a change, note that the Password and Username can be up to 7 characters and that they are case sensitive. The new password takes effect immediately.

➤ **To reset the username and password to their defaults:**

- Set the ini file parameter ResetWebPassword to 1 and use the BootP/TFTP Server to load the ini file to the device (refer to the Appendix, "BootP/TFTP Server" on page 185). After loading, the username and password automatically revert to their default values (Admin).



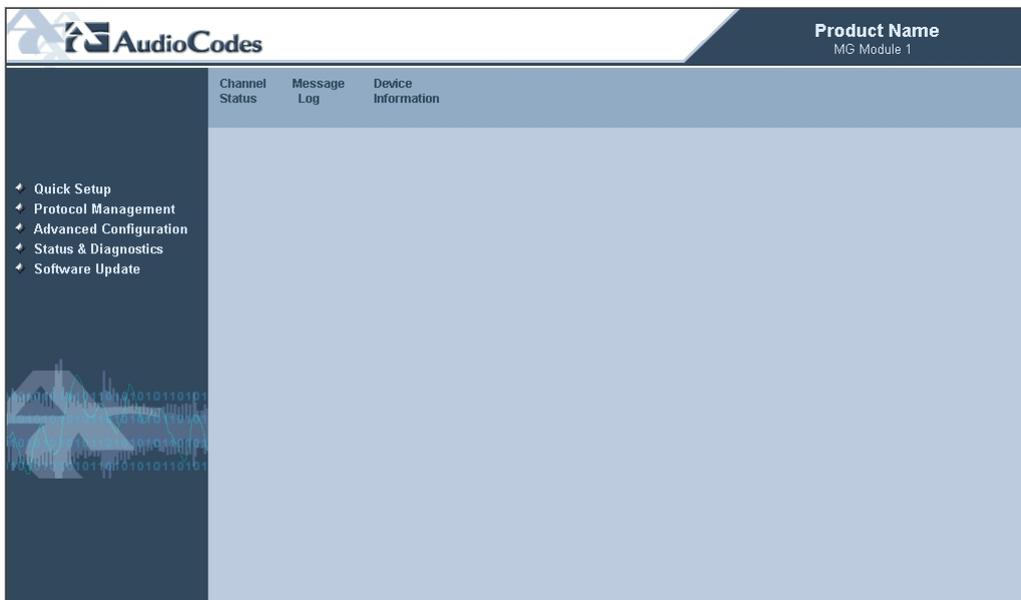
Note: This procedure resets both Administrator and Monitoring level passwords to their defaults.

7.4.5 Status and Diagnostic Menu

➤ **To access the Status and Diagnostics menu, take this step:**

- From the main menu list on the left, click on the Status and Diagnostics link. The Status and Diagnostics screen with the sub-menu bar on the top is displayed.

Figure 7-33: Status and Diagnostic Menu Screen



7.4.5.1 Channel Status

- **To access the Channel Status screen, take these 3 steps:**
1. From the main menu list on the left, click on the **Status and Diagnostics** link. The Status and Diagnostics screen appears.
 2. From the sub-menu bar on the top, click the **Channel Status** link. The Channel Status screen appears. The screen is Read-only.

Figure 7-34: Channel Status Screen - FXO

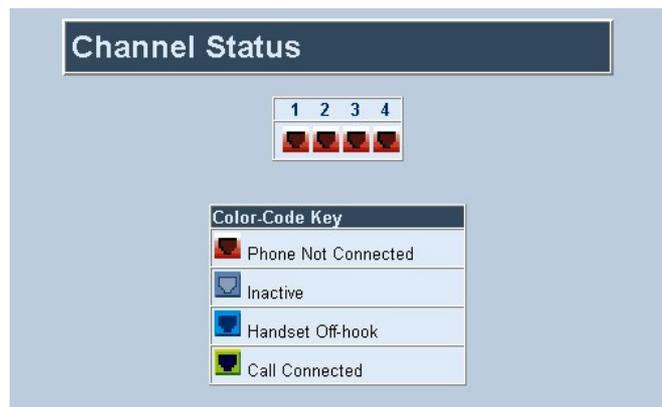


Figure 7-35: Channel Status Screen - FXS



The Channel Status indicators can appear colored. the table below shows the possible indicators and their descriptions.

Table 7-2: Channel Status Color Indicator Key

Channel Status Definition		
Indicator	Color	Description
	Gray	Inactive
	Green	RTP Connection
	Blue	Handset Off
	Red-White	Line not connected (FXO only)

3. To display a screen with a summary of parameter information relevant to a channel, click on the channel.

The following 'per channel' screen information is available when clicking on a specific channel:

Figure 7-36: Channel Status Screen

AudioCodes Product Name: MG Module 1

Channel Status Message Log Versions

- Quick Setup
- Protocol Management
- Advanced Configuration
- Status & Diagnostics**
- Software Update
- Save Configuration
- Reset

Channel Status RTP/RTCP Settings Fax & Modem Settings Transport Settings
Voice Settings IBS Detectors Settings Jitter Buffer Settings

Channel Status	
Channel Identifier:	51
Active :	No
RTP Active :	No
Bypass NIC :	1
Tx Silence Period :	No
Rx Silence Period :	No
Tx Fax Mode :	0
Rx Fax Mode :	0
Tx DTMF Period :	No
Rx DTMF Period :	No
Packets to DSP Counter :	0
Jitter Buffer Underrun Counter :	0
Jitter Buffer Overrun Counter :	0

This page refreshes every 5 seconds

Figure 7-37: RTP/RTCP Settings Screen

RTP/RTCP Settings	
Channel Identifier:	0
RTP Canonical Name :	Ch0
IP Precedence :	0
IP Type of Service :	0
Local RTP Port :	4000
Remote RTP Address :	10.31.3.96
Remote RTP Port :	4000
Remote T.38 Address :	10.31.3.96
Remote T.38 Port :	4002
RTCP Mean Tx Interval :	5000
Rx RTP Payload Type :	4
Tx RTP Payload Type :	4

Figure 7-38: Fax & Modem Settings Screen

Fax & Modem Settings	
Channel Identifier :	51
FAX Transport Type :	Relay Enabled
V.21 Modem Transport Type :	Disabled
V.22 Modem Transport Type :	Bypass Enabled
V.23 Modem Transport Type :	Bypass Enabled
V.32 Modem Transport Type :	Bypass Enabled
V.34 Modem Transport Type :	Bypass Enabled
Fax Relay Max Rate :	14400 bps
Fax Relay ECM Enable :	Enable
Fax Relay Redundancy Depth :	0
Enhanced Fax Relay Redundancy Depth :	4
Fax Modem Relay Volume :	-12
Fax Modem Bypass Coder Type :	G711Alaw_64 (0)
Fax Modem Bypass M :	1

Figure 7-39: Transport Settings Screen

Transport Settings	
Channel Identifier:	51
Use NI or PCI :	NI
Soft IP Loopback :	Disable
Unidirectional RTP :	RTPTxRx

Figure 7-40: Voice Settings Screen

Voice Settings	
Channel Identifier :	51
Coder :	G723High (16)
ECE :	Yes
SCE :	No
PFE :	Yes
HPFE :	Yes
Test Mode :	NoLoopback
VoiceVolume :	0
Input Gain :	0
M :	1
RTP Redundancy Depth :	0
EC Length :	0
EC Hybrid Loss :	0

Figure 7-41: IBS Detector Settings Screen

IBS Detectors Settings	
Channel Identifier :	51
Enable DTMF Detection :	Yes
Enable MFR1 :	No
Enable MFR2 Forward :	No
Enable MFR2 Backward :	No
Enable Line Signaling :	No
Enable Call Progress :	Yes
Enable User Define Tone Detection :	No
DTMF Volume :	-11
DTMF Transport Type :	RFC2833 Relay DTMF
MF Transport Type :	RFC2833 Relay MF

Figure 7-42: Jitter Buffer Settings Screen

Jitter Buffer Settings	
Channel Identifier :	51
Jitter Buffer Minimum Delay :	70
Jitter Buffer Opt. Factor :	7

Figure 7-43: IPmedia Settings Screen

IPmedia Settings	
Channel Identifier:	3
Enable Answer Detector :	No
Answer Detector Activity Delay :	0
Answer Detector Silence Time :	10
Answer Detector Redirection :	0
Answer Detector Sensitivity :	0
Enable Agc :	No
Agc Gain Slope :	0
Agc Redirection :	0
Agc Target Energy :	0
Enable Energy Detector :	No
Energy Detector Quality Factor :	0
Energy Detector Threshold :	0
Enable Pattern Detector :	No

7.4.5.2 Message Log

The Message Log is similar to a Syslog. It provides debug messages useful in pursuing troubleshooting issues.

The Message Log serves the Web Server and is similar to a Syslog server. It displays debug messages. It is not recommend to use the Message Log screen for logging errors and warnings because errors can appear over a prolonged period of time, e.g., a device can display an error after running for a week. Similarly, It is not recommend to keep a Message Log session open for a prolonged period (refer to the Note below). For logging of errors and warnings, refer to 'Syslog'.

➤ **To activate the Message Log, take these 4 steps:**

1. From the main menu list on the left, click on the **Status and Diagnostics** link. The Status and Diagnostics screen appears and Log is activated.

- From the sub-menu bar on the top, click the **Message Log** link. The Message Log screen appears.

Figure 7-44: Message Log Screen


- After receiving messages - Using the scroll bar, select the messages, copy them and paste them into a text editor such as Notepad. Send this *txt* file to Technical Support for diagnosis and troubleshooting as needed.
- To clear the screen of messages, click on the sub-menu Message Log. The screen is cleared. A new session is activated and new messages begin appearing.



Note: Do not keep the Message Log screen activated and minimized for a prolonged period as a long session may cause the PC workstation to overload. While the screen is open (even if minimized), a session is in progress and messages are sent. Closing the window or moving to another link stops the messages and terminates the session.

7.4.5.3 Device Information

The Device Information screen displays hardware, software product information and Device state information. This information can help you to expedite any troubleshooting process. Capture the screen and email it to Technical Support personnel to ensure quick diagnosis and effective corrective action.

The screen also displays any loaded files in the device.

➤ To display the Device Information screen, take these 2 steps:

- From the main menu list on the left, click on the **Status and Diagnostics** link. The Status and Diagnostics screen appears.

- From the sub-menu bar on the top, click the **Device Information** link. The Device Information screen appears.

Figure 7-45: Versions Screen

Device Information		
General		
MAC Address:	00908f045fec	
Serial Number:	286700	
Board Type:	24	
Device Up Time:	0d:0h:49m:39s:93th	
Device Administrative State:	Unlocked	
Device Operational State:	Enabled	
Versions		
Version ID:	4.50.522	
DSP Type:	2	
DSP Software Version:	20724	
DSP Software Name:	624AE3	
Flash Version:	192	
Module FirmWare:	0x31	
Loaded Files		
Call Progress Tones File Name:	normalDialTone.dat	Delete
VXML File Name:	tt_dec17.dat	Delete
Pre Recorded Tones File Name:	prerecordedtones2indexes.dat	Delete

➤ **To delete any loaded files, take these 5 steps:**

- From the main menu list on the left, click on the **Status and Diagnostics** link. The Status and Diagnostics screen appears.
- From the sub-menu bar on the top, click the **Device Information** link. The Device Information screen appears.
- In the Device Information table, click the **Delete** button. The file deletion takes effect only after a device reset is performed.
- In main menu to the left, click the **Reset** link. The Reset screen appears.
- Select the **Burn** option and click the **Reset** button to restart the device with the new settings. (Refer to "Reset Button" on page 164.)

7.4.6 Software Update

The Software Update screen offers two options for downloading current software update files: the Software Upgrade Wizard and Load Auxiliary Files screen.

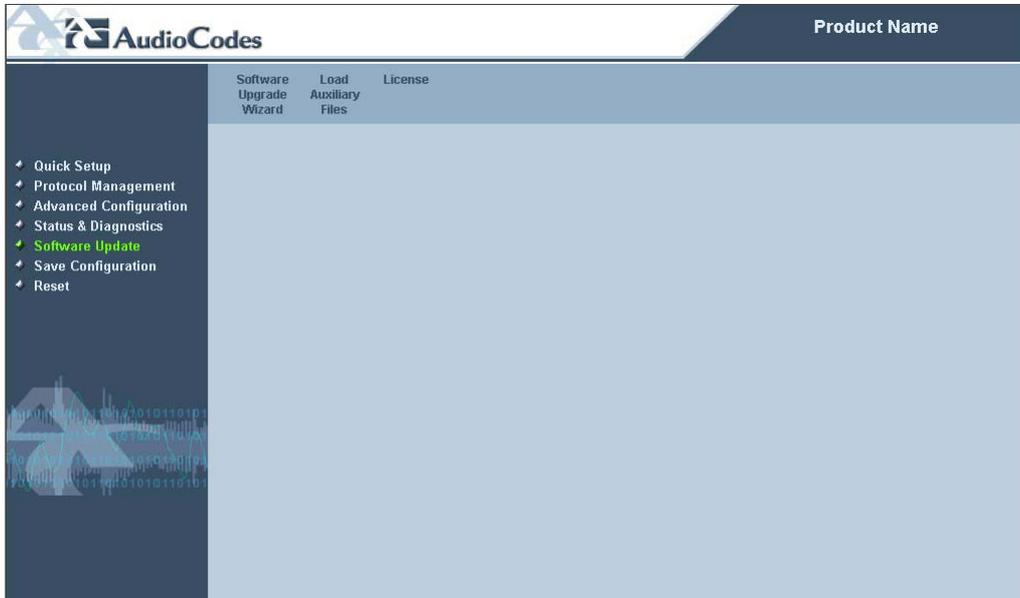
- Software Upgrade Wizard - Refer to 'Software Upgrade Wizard' below
- Load Auxiliary Files - Refer to "Auxiliary Files Download" on page 161

7.4.6.1 Software Upgrade Wizard

The Software Upgrade Wizard allows the user to upgrade the MediaPack's software by loading a new *.cmp file together with a full suite of useful auxiliary files.

Loading a *.cmp file is mandatory in the Software Upgrade Wizard process. During the process, you choose from the auxiliary files provided for loading. For each auxiliary file type, you can choose between reloading an existing file, loading a new file or not loading a file at all.

Figure 7-46: Start Software Upgrade Screen



➤ **To use the Software Upgrade Wizard take these 12 steps:**

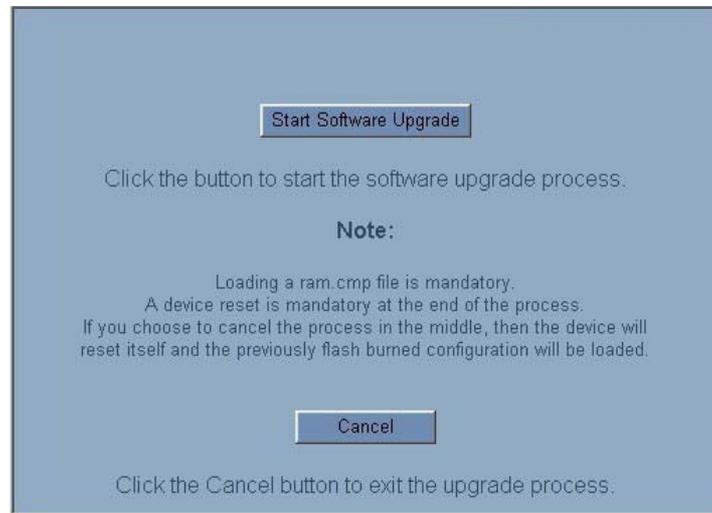


Note: The Software Upgrade Wizard requires the device to be reset at the end of the process, which disrupts any existing traffic on the device. To avoid disrupting traffic, disable all traffic on the device before initiating the Software Upgrade Wizard.

1. Stop all traffic on the device (refer to the note above.)
2. From the main menu list on the left, click on the **Software Update** link. The Software Upgrade screen with the sub-menu bar on the top is displayed.

3. On the sub-menu bar on the top, click the **Software Upgrade Wizard** link. The Start Software Upgrade screen appears.

Figure 7-47: Start Software Upgrade Screen

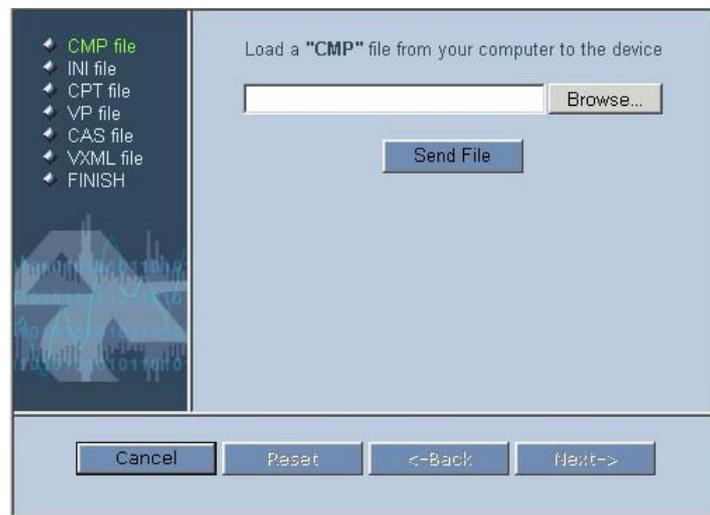




Note: At this point you may cancel the Software Upgrade process with no consequence to the device by using the cancel button. If you continue with the Software Upgrade process by clicking the **Start Software Upgrade** button, the process must be followed through and completed with a device reset at the end of the process. If you use the **Cancel** button, in any of the subsequent screens, the Software Upgrade process causes the device to be reset.

- Click the **Start Software Upgrade** button to initiate the upgrade process. The File Loading screen appears displaying the *cmp* file information. The background Web screen is disabled. During the Software Upgrade process, the rest of the Web application is unavailable. After the Software Upgrade process is complete, access to the full Web application is restored.

Figure 7-48: Load CMP File Dialog Screen



Note the file type list in the left side of the screen. This list contains the relevant file types that can be loaded via the wizard for this device type. The highlighted file type in the file type list indicates which file type is being displayed in the main part of the screen. As you continue through the Software Upgrade process by clicking on the **Next** button, each of the relevant file type screens are presented, going down the list until the Finish screen appears.

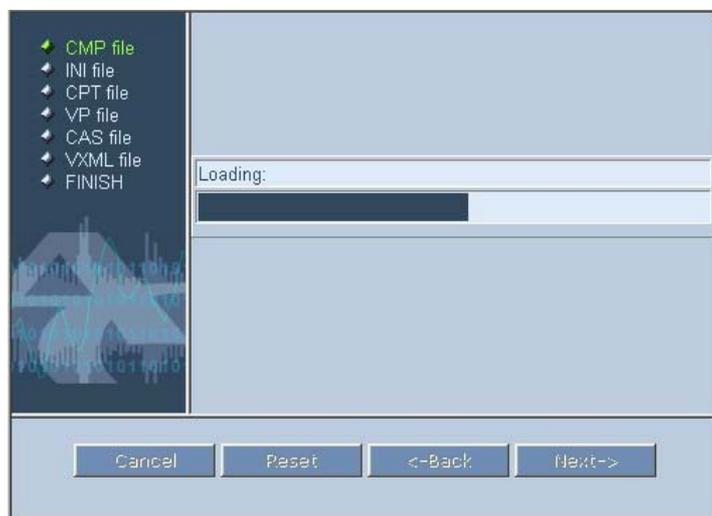


Note: The **Next** button is disabled until you load a **.cmp* file. After a **.cmp* file is selected, the wizard upgrade process continues and the Next button is enabled.

- Click the **Browse** button and navigate to the location of the **.cmp* file to be loaded. The path and file name appears in the field.

6. Click the **Send File** button to send the file to the device. The File Loading screen appears with a progress bar indicating the loading period. When the loading is complete, a message is displayed indicated the file was successfully loaded into the device.

Figure 7-49: File Loading Dialog Screen



All four buttons (**Cancel**, **Reset**, **Back**, and **Next**) in the bottom portion of the screen are activated.

7. You may choose between these options:
 - Loading Additional Auxiliary Files
 - Completing the Software Upgrade Process
 - Cancel Upgrade Process and revert to the Previous Configuration Files
8. **Loading Additional Auxiliary Files**

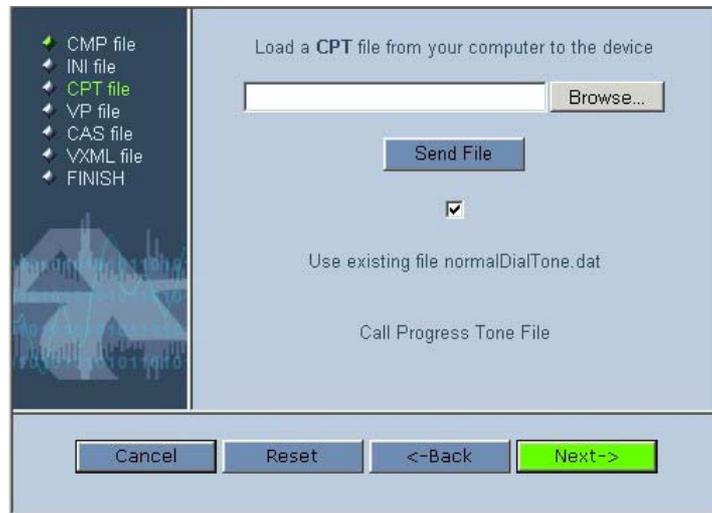
To move to the next file type on the list to the left, click the **Next** button. The File Loading screen appears with the next relevant file type highlighted.

For each file type the user has three options:

- Load a new auxiliary file to the device using the Browse and Send File' button as described above.
- Load the existing auxiliary file - A checkbox (checked by default as shown in the figure below) appears if relevant to the device. If this checkbox is checked, the existing file is used in the upgraded system.
- Avoid loading any file at all - Clear the checkbox (if the checkbox appears).

Continue through each of the file type screens by clicking **Next** and selecting one of the above options. As an example, the figure below displays the File Loading screen with the *CPT* file type selected.

Figure 7-50: File Loading Dialog Screen - CPT Type Displayed



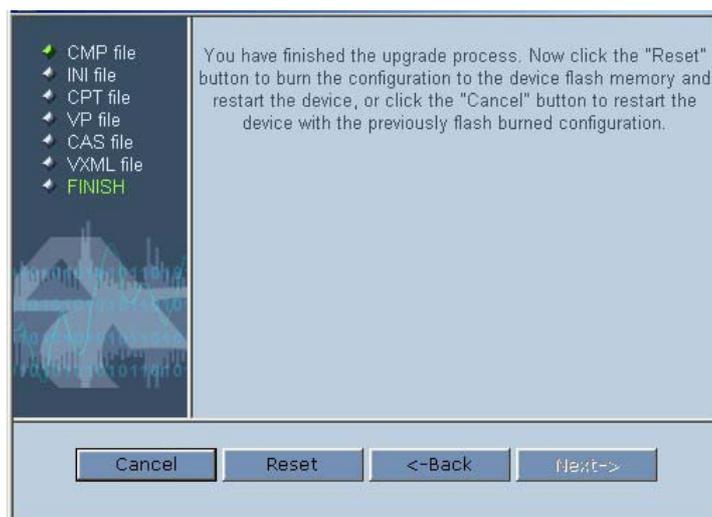
9. Completing the Software Upgrade Process

From any of the file type screens, you can complete the Software Upgrade process by clicking the **Reset** button. The device is reset utilizing the new files you have loaded up to that point, as well as using the existing files according to the checkbox status of each file type.

10. Revert to the Previous Configuration Files

From any of the file type screens, you can revert to the previous configuration by clicking the **Cancel** button. The Software Upgrade process is terminated and the device is reset utilizing the previous configuration files. Similar screens as shown in two figures below are displayed.

- 11. When continuing through the Software Upgrade process, you complete the process from the Finish screen by clicking the **Reset** button (the **Next** button is disabled).



During the Reset process, the device 'burns' the newly loaded configuration to the non-volatile memory. The File Burning screen appears displaying the File Burning to Flash Memory progress bar. When this is completed, the Reset Device screen appears displaying the Reset in progress bar. When this is complete, the End Of Process screen appears displaying the current configuration information.

Figure 7-51: End of Process Dialog Screen



12. Click the **End Process** button. The Quick Setup screen appears and the full Web application is reactivated.

7.4.6.2 Auxiliary Files Download

The Auxiliary Files Download screen facilitates the download of software updates using the HTTP protocol. Types of software file updates include:

- Coefficient - This file contains the analog line electrical characteristics. Several files are available for FXS and FXO and for different metering tone frequencies.
- Voice Prompt - The *.dat* Voice Prompts file is played by the device during the phone conversation on Call Agent request. Download if you have an application requiring Voice Prompts.
- Call Progress Tone - *usa_tones.dat* - This is a region-specific, telephone exchange-dependent file. Call Progress Tones provide call status/call progress to customers, operators, and connected equipment. Default Tones: U.S.A. *usa_tones.ini* - The *.ini* file is the value of the different Call Progress Tones files (frequency, cadence, etc.). To convert the *usa_tones.ini* file, which is a *.txt* file, to a *usa_tones.dat* file that can be downloaded into the MediaPack, use the Call Progress Tones file generator utility *TPDMUtil.exe*.

➤ To download an auxiliary file, take these 5 steps:

1. From the main menu list on the left, click on the **Software Download** link. The Software Download screen is displayed.

- From the sub-menu bar on the top, click the **Auxiliary Files Download** link. The Auxiliary Files Download screen appears.

Figure 7-52: Auxiliary Files Download Screen

Auxiliary Files

Send "INI" file from your computer to the device

Send FXS "Coefficient" file from your computer to the device*

Send "Voice Prompt" file from your computer to the device*

Send "Call Progress Tone" file from your computer to the device

Send "Pre Recorded Tones" file from your computer to the device*

* Loading the file takes effect on-the-fly (no reset is required)

- Use the **Browse** button to locate the appropriate file on your PC.
- Click the **Send File** button. The files are sent to the MediaPack.
- To commit the changes to the non-volatile (flash) memory, in the main menu on the left, click the **Save Configuration** link. In the **Save Configuration** screen that appears, click the **Save Configuration** button. The changes are committed to the non-volatile memory.



Note: A device reset is required to activate a loaded *CPT* file, and may be required for the activation of certain *ini* file parameters. The **Burn** option must be selected. (Refer to "Reset Button" on page 164.)

➤ **To download an auxiliary file, take these 5 steps:**

- From the main menu list on the left, click on the **Software Download** link. The Software Download screen is displayed.
- From the sub-menu bar on the top, click the **Auxiliary Files Download** link. The Auxiliary Files Download screen appears.

Figure 7-53: Auxiliary Files Download Screen

Auxiliary Files

Send ".INI" file from your computer to the device

Browse... Send File

Send FXS ".Coefficient" file from your computer to the device*

Browse... Send File

Send ".Voice Prompt" file from your computer to the device*

Browse... Send File

Send ".Call Progress Tone" file from your computer to the device

Browse... Send File

Send ".Pre Recorded Tones" file from your computer to the device*

Browse... Send file

* Loading the file takes effect on-the-fly (no reset is required)

3. Use the Browse button to locate the appropriate file on your PC.
4. Click the Send File button. The files are sent to the MediaPack.
5. To commit the changes to the non-volatile (flash) memory, in the main menu on the left, click the Save Configuration link. In the Save Configuration screen that appears, click the Save Configuration button. The changes are committed to the non-volatile memory.



Note: A device reset is required to activate a loaded *CPT* file, and may be required for the activation of certain *ini* file parameters. The **Burn** option must be selected. (Refer to "Reset Button" on page 164.)

7.4.7 Save Configuration

The Save Configuration screen allows users to save the current parameter configuration and the loaded files to the MediaPack's non-volatile (flash) memory.



Note: If you perform a reset with the **Burn** option selected *immediately* after making the changes to the configuration, there is no need to use the Save Configuration function prior to the reset.

➤ **To use the Save Configuration screen, take these 2 steps:**

1. From the main menu list on the left, click on the **Save Configuration** link. The Save Configuration screen is displayed.

Figure 7-54: Save Configuration Dialog Screen



2. Click the **Save Configuration** button. The new/modified configuration and any HTTP loaded files are saved to the non-volatile (flash) memory on the device. A message informing you that it has been saved appears.

7.4.8 Reset Button

The **Reset** link in the main menu on the left allows the user to initiate a device reset following which the device utilizes the new configuration stored in the non-volatile (flash) memory.

➤ **To use the Reset Button screen, take these 3 steps:**

1. From the main menu list on the left, click on the **Reset** button. The Reset screen is displayed.

Figure 7-55: Reset Screen



2. Select either of the following Burn options:
 - **Burn** - (Default setting) burns the current configuration to non-volatile (flash) prior to reset
 - **Don't Burn** - Resets the device without first burning the current configuration to non-volatile (discards all modifications to the configuration that were not saved to non-volatile memory)
3. Select either of the following Graceful Shutdown options:
 - **Yes** - a **timer configuration input** field appears - Reset starts only after the timer expires or no more active traffic exists (the earliest thereof)
 - **No** - immediate reset, any existing traffic is terminated at once
4. Click the **Restart** Button. If Graceful shutdown was selected, the reset is delayed and a screen displaying the number of remaining calls and the timer count is displayed. If Graceful shutdown was not selected the reset starts immediately.

When the reset initiates, If the **Burn** option is selected, all of the changes made to the configuration are saved to the non-volatile memory of the device. If the **Don't Burn** option is selected, all of the changes made to the configuration are discarded. The device is shut down and re-activated. A message about the waiting period is displayed. The screen is refreshed.

7.5 Restoring and Backing Up the Device Configuration

The 'Configuration File' screen enables you to restore (load a new *ini* file to the device) or to back up (make a copy of the *ini* file and store it in a directory on your PC) the current configuration the device is using.

Back up your configuration if you want to protect your device's programming. The backup *ini* file includes only those parameters that were modified and contain other than default values.

Restore your configuration if the device has been replaced or has lost its programming information, you can restore the device's configuration from a previous backup or from a newly created *ini* file. To restore the device's configuration from a previous backup you must have a backup of the device's information stored on your PC.

➤ **To restore or back up the *ini* file, take this step:**

- Open the 'Configuration File' screen (Advanced Configuration menu > Configuration File). The 'Configuration File' screen is displayed. (Refer to "Configuration File" on page 144.)

➤ **To back up the *ini* file take these 4 steps:**

1. Click the **Get INI FILE** button; the 'File Download' dialog opens.
2. Click the **Save** button. The 'Save As' dialog opens.
3. Navigate to the folder where you want to save the *ini* file.
4. Click the **Save** button. The VoIP gateway copies the *ini* file into the folder you selected.

➤ **To restore the *ini* file take these 4 steps:**

1. Click the **Browse** button.
2. Navigate to the folder that contains the *ini* file you want to load.
3. Click the file and click the **Open** button. The name and path of the file appear in the field beside the **Browse** button.
4. Click the **Send ini File** button, and click **OK** in the prompt. The gateway is automatically reset (from the *cmp* version stored on the flash memory).

8 Diagnostics & Troubleshooting



Note 1: MP-11x refers collectively to MP-118 8-port, MP-114 4-port and MP-112 2-port Media Gateways having similar functionality except for the number of channels (the MP-112 supports only FXS).

Note 2: MP-1xx refers to MP-124 24-port, MP-108 8-port, MP-104 4-port and MP-102 2-port Media Gateways having similar functionality except for the number of channels (the MP-124 and MP-102 support only FXS).

Note 3: MP-10x refers only to the MP-108, MP-104 and MP-102 gateways.

Note 4: MP-10x/FXS refers only to the MP-108/FXS, MP-104/FXS and MP-102/FXS gateways.

Note 5: MP-10x/FXO refers only to MP-108/FXO and MP-104/FXO gateways

8.1 Diagnostics Overview

A wide range of diagnostic tools are provided to enable the user to easily identify an error condition and to provide a solution or work-around when working with the MediaPack.

- LED Indication of channel activity status, data, control and LAN status.
- MediaPack Self-Testing on hardware initialization.
- Error/Notification Messages via the following interfaces
 - RS-232 terminal
 - Syslog
 - Control protocols:
 - ◆ MGCP
 - SNMP
- Solutions to Common Problems.

They are described in the following pages.

8.2 Troubleshooting MediaPack Devices via the RS-232 Port

To troubleshoot initialization problems and view the status and error messages of the MediaPack, use serial communication software (e.g., HyperTerminal™) to connect to the MediaPack via the RS-232 port. You can also use this connection to change the network settings (IP address, subnet mask and default gateway IP address) of the MediaPack. To connect the MP-11x RS-232 port to your PC, refer to Section 3.2.5.1. To connect the MP-1xx RS-232 port to your PC refer to Section 3.1.3.1.

8.2.1 Viewing the Gateway's Information

After applying power to or resetting the gateway, the information, shown in the example below, appears on the terminal screen. This information is used to determine possible MediaPack initialization problems, such as incorrectly defined (or undefined) Local IP address, subnet mask, default router IP address, TFTP server IP address, BootFile name, ini file name and Full/Half duplex network state.

Example of Status and Error Messages

```
MAC address = 00-90-8F-01-00-9E
Local IP address = 10.1.37.6
Subnet mask = 255.255.0.0
Default gateway IP address = 10.1.1.5
TFTP server IP address = 10.1.1.167
Boot file name = ram35136.cmp
INI file name = mp108.ini
Call agent IP address = 10.1.1.18
Log server IP address = 0.0.0.0
Full/Half Duplex state = HALF DUPLEX
Flash Software Burning state = OFF
Serial Debug Mode = OFF
Lan Debug Mode = OFF

BootLoad Version 1.75
Starting TFTP download... Done.
MP108 Version 3.80.00
```

8.2.2 Changing the Networking Parameters

You can use the serial connection to change the network settings (IP address, subnet mask and default gateway IP address) of the MediaPack.

➤ To change the network settings via RS-232, take these 4 steps:

1. At the prompt type **conf** and press **Enter**. The configuration command shell is activated.
2. To check the current network parameters, at the prompt, type **GCP IP** and press **Enter**. The current network settings are displayed.
3. To change the network settings, type **SCP IP [ip_address] [subnet_mask][{default_gateway}** (e.g., "SCP IP 10.13.77.7 255.255.0.0 10.13.0.1"). The new settings take effect immediately. Connectivity is active at the new IP address.



Note 1: This command requires you to enter all three network parameters.

Note 2: Consult your network administrator before setting these parameters.

4. To save the configuration, at the prompt, type SAR and press Enter. The MediaPack restarts with the new network settings.

8.2.3 Determining MediaPack Initialization Problems

Possible initialization problems encountered with the MediaPack can be determined by viewing the HyperTerminal screen after performing a hot hardware reset. Possible initialization problems are listed in the table below. (LED indicators located on the front panel of the MediaPack provide first indication that the device has an initialization problem. Refer to 'LED Indicators' for a description of the LED visual indicators.)

Table 8-1: Possible Initialization Problems

Parameter	Problem Definition
Local IP address	Undefined/incorrectly defined
Subnet Mask	Undefined/incorrectly defined
Default gateway IP address	Undefined/incorrectly defined
TFTP server IP address	Undefined/incorrectly defined
Boot file name	Undefined/incorrectly defined/missing
<i>ini</i> file name	Undefined/incorrectly defined/missing
Call Agent IP address	Undefined/incorrectly defined
Log server IP address	Undefined/incorrectly defined
Full/Half Duplex state	Undefined/incorrectly defined
Flash Software Burning state	Undefined/incorrectly defined
Serial Debug Mode	Undefined/incorrectly defined
BootLoad version	Incorrect

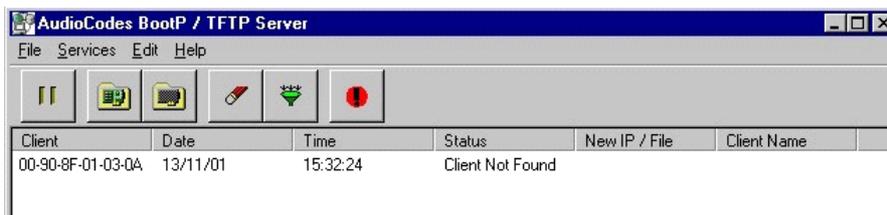
8.2.4 Reinitializing the MediaPack

If an initialization problem is encountered, reinitialize the MediaPack. To reinitialize the MediaPack, a BootP/TFTP Server application must be installed in your management PC. Reinitializing the MediaPack using the BootP/TFTP Server enables you to quickly get started with the MediaPack. For a detailed description of the BootP/TFTP Server Configuration Tool, including installation and configuration, refer to 'BootP Server' on page 185.

➤ **To reinitialize the MediaPack, take the next 13 steps:**

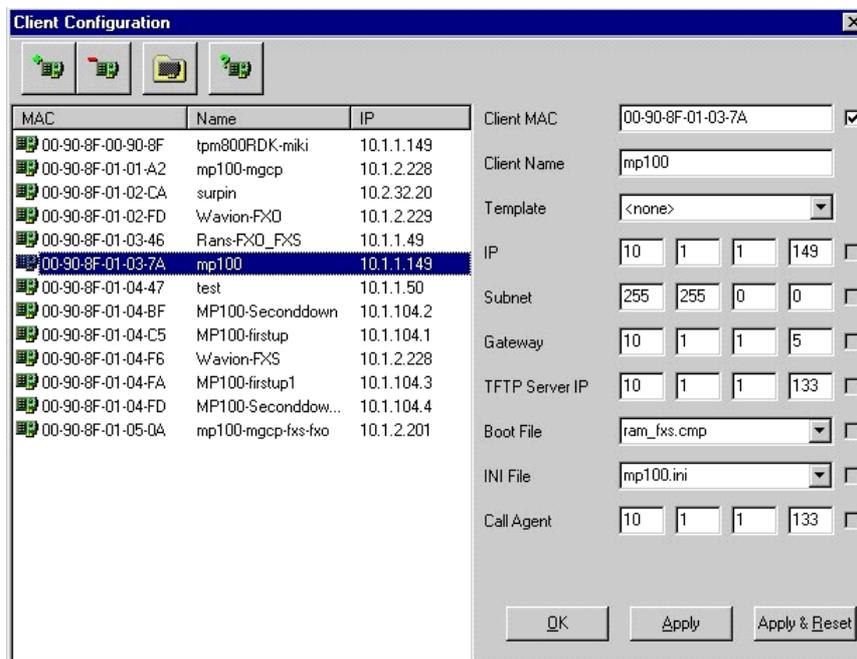
1. Install the BootP/TFTP Server Configuration Tool from the Software CD, Document # LSTC00005 (MediaPack Series), refer to 'BootP Server' on page 185.
2. Open the BootP/TFTP Server from Start>Programs>BootP. The BootP/TFTP Server main screen opens:

Figure 8-1: BootP/TFTP Server Main Screen



3. In the Services menu, choose Edit Clients. Alternately, double-click on the Client Not Found log entry. The Client Configuration screen appears. (Refer to the figure below). The parameter fields displayed on the right side of the screen constitute the MediaPack software profile configuration. For a Client Not Found, the parameter fields are all blank.

Figure 8-2: Client Configuration

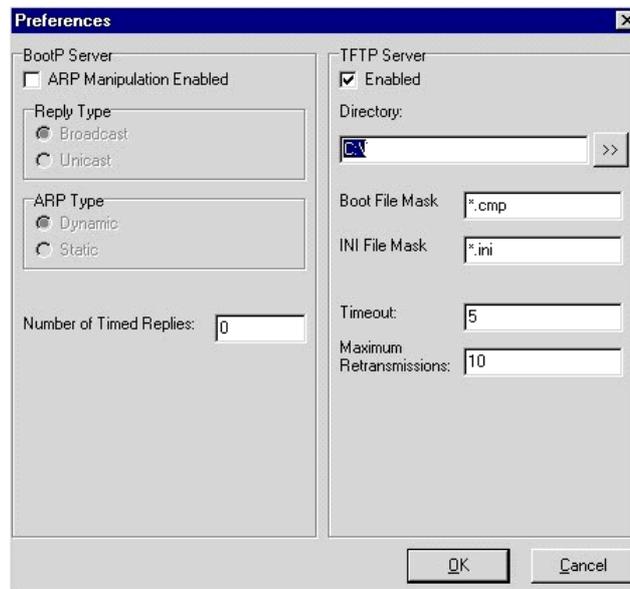


4. Enter the reported MediaPack MAC address (labeled on the underside of the device) in the Client MAC field.
5. Enter the Client Name.
6. Enter the IP address (such as 10.1.1.33).
7. Enter the Subnet (such as 255.255.255.0) and set the Subnet to a valid value in accordance with the IP address. (That is, class C IP addresses can only have

subnet starting with 255.255.255.X, while class B IP addresses can only have subnet starting with 255.255.X.X, and class A IP addresses can only have subnet starting with 255.X.X.X.)

8. Enter the IP address of the default Gateway. It can be any address within the subnet.
9. Enter the Call Agent IP address.
10. Upload the *ram_fxs.cmp* and the *mp_fxs.ini* configuration files by opening the Edit menu and choosing Preferences. The Preferences screen appears.

Figure 8-3: Preferences Screen



11. In the Directory field, click on the >> button and navigate to the directory of the source *cmp* and *ini* files.
If they are not already on your hard disk (C:), copy them to it (under a directory you should create called C:\\AudioCodes\\). If you do not have the MediaPack Software CD from which to copy the *cmp* and *ini* files, contact support@audiocodes.com' mailto:support@audiocodes.com.
12. Click OK. The *cmp* and *ini* files are uploaded.

13. Perform a hot hardware reset or cold reset. The MediaPack initializes and the following status messages should be displayed in the BootP/TFTP Server main screen:

Figure 8-4: BootP/TFTP Server - Client Found

Client	Date	Time	Status	New IP / File	Client Name
10.1.1.134	13/11/01	15:37:59	47%	D:\Backup22-8...	
00-90-8F-01-03-0A	13/11/01	15:37:52	Client Found	10.1.1.134	mp100

8.3 LED Indicators

All LED indicators are described in the tables in 'Front LED Indicators' on page 22 and 'Rear LED Indicators'.

8.3.1 MediaPack Front Panel LED Indicators

The full range of the MediaPack includes a front panel displaying LED Indications of channel activity status, data, control and LAN status.

8.4 MediaPack Self-Testing

The MediaPack features two self-testing modes: **rapid** and **detailed**.

Rapid self-test mode is invoked each time the Media Gateway completes the initialization process. (See 'Reinitializing the MP-11x' on page 169) This is a short test phase in which the only error detected and reported is failure in initializing hardware components. All Status and Error reports in this self-test phase are reported through both the RS-232 and Network Interface ports, as well as indicated by the LED Status Indicators.

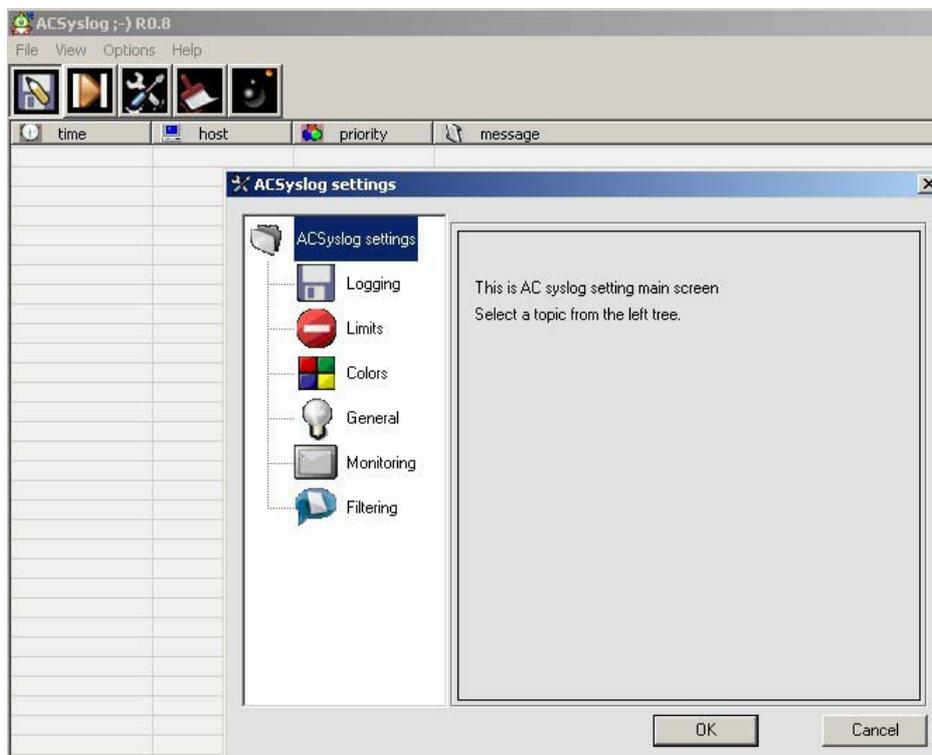
Detailed self-test mode is invoked when initialization of the Media Gateway is completed and if the configuration parameter EnableDiagnostics is set to 1 (this parameter can be configured through the *ini* file mechanism). In this mode, the Media Gateway tests all the hardware components (memory, DSP, etc.), outputs the status of the test results - the board sends EV_END_BIT which contains information on the results of the test of each hardware component. To continue operational running, reset the Media Gateway again but this time configure the EnableDiagnostics parameter to 0.

8.5 Syslog

The Syslog server (refer to the figure below), now available with version 4.4 and above of the VoIPerfect platform, enables filtering of messages according to priority, IP sender address, time, date, etc. Customers can alternatively choose to download and use the following examples of the many Syslog servers available as shareware on the Internet:

- Kiwi Enterprises: http://www.kiwi-enterprises.com/software_downloads.htm
- The US CMS Server: http://uscms.fnal.gov/hanlon/uscms_server/
- TriAction Software: <http://www.triaction.nl/Products/SyslogDaemon.asp>
- Netal SL4NT 2.1 Syslog Daemon: <http://www.netal.com>

Figure 8-5: AC Syslog



Syslog protocol is an event notification protocol that allows a machine to send event notification messages across IP networks to event message collectors- also known as Syslog servers. Syslog protocol is defined in the IETF RFC 3164 standard.

Since each process, application and operating system was written independently, there is little uniformity to Syslog messages. For this reason, no assumption is made on the contents of the messages other than the minimum requirements of its priority.

Syslog uses User Datagram Protocol (UDP) as its underlying transport layer mechanism. The UDP port that has been assigned to Syslog is 514.

The Syslog message is transmitted as an ASCII message. The message starts with a leading "<" ('less-than' character), followed by a number, which is followed by a ">" ('greater-than' character). This is optionally followed by a single ASCII space.

The number described above is known as the Priority and represents both the Facility and Severity as described below. The Priority number consists of one, two, or three decimal integers.

Example:

```
<37> Oct 11 16:00:15 mymachine su: 'su root' failed for lonvick
on /dev/pts/8
```

8.5.1 Operating the Syslog Server

8.5.1.1 Sending the Syslog Messages

The Syslog client, embedded in the firmware of the device, sends error reports/events generated by the device application to a Syslog server, using IP/UDP protocol.

There are presently five error levels reported by the Syslog client:

- Emergency level message:

```
<128>sctp socket setsockopt error 0xf0 [File:sctp.cpp Line:453]
```

- Warning level message

```
<132>Release contains no h.225 Reason neither q.931 Cause
information stateMode:1 [File: Line:-1];
```

- Notice level message:

```
<133>( lgr_flow)(2546 ) | #0:ON_HOOK_EV
```

- Info level message:

```
<134>document http://ab.pisem.net/RadAAIP.txt was not found in
documents table [File:vxml_handleDB.cpp Line:2348]
```

- Debug level message:

```
<135>SCTP port 2905 was initialized [File:csAPI.cpp Line:150]
[CID:0]
```

8.5.1.2 Setting the Syslog Server IP Address

- **To set the address of the Syslog server:**

- Use the Embedded Web Server GUI (Advanced Configuration>Network Settings - screen section Logging Settings). (Refer to 'Embedded Web Server' on page 114 and to the figure below)

Figure 8-6: Setting the Syslog Server IP Address

Logging Settings	
SysLog Server IP address:	10.8.1.19
Enable SysLog:	Enable

- Alternately, use the Embedded Web Server GUI or the BootP/TFTP Server to send the ini configuration file containing the address parameter SyslogServerIP to the device. Before sending the ini file to the device, specify the address parameter. For detailed information on the BootP/TFTP Server, refer to 'BootP Server' on page 185.. For an ini file example showing this parameter, refer to Setting the Syslog Server example below.

8.5.1.3 Activating the Syslog Client

➤ **To activate the Syslog client:**

- Use the Embedded Web Server GUI (Advanced Configuration>Network Settings - screen section Logging Settings). (Refer to 'Advanced Configuration Screen' on page 163 and the Logging Settings figure above.)
- Alternately, use the Embedded Web Server GUI or the BootP/TFTP Server to send the ini configuration file containing the parameter EnableSyslog to the device. For detailed information on the BootP/TFTP Server, refer to 'BootP Server' on page 185. For an ini file example showing this parameter, refer to the Setting the Syslog Server example below.

8.5.1.4 Setting Syslog Server IP Address, Enabling Syslog, in an *ini* File (Example)

The example below shows an *ini* file section with an example configuration for the address parameter SyslogServerIP and an example configuration for the client activation parameter EnableSyslog.

Example of Setting Syslog Server IP Address, Enabling Syslog, in an ini File

```
[Syslog]
SyslogServerIP=10.2.0.136
EnableSyslog =1
```

8.6 The Embedded Web Server's 'Message Log' (Integral Syslog)

The 'Message Log' screen in the Embedded Web Server GUI, similar to a Syslog server only integral to the web server, displays debug messages useful for debugging. For detailed information, refer to 'Message Log' on page 153. The Message Log screen is not recommended for logging of errors and warnings because errors can appear over a prolonged period of time, e.g., a device can display an error after running for a week, and it is not recommended to prolong a 'Message Log' session. For logging of errors and warnings, refer to the section below.

8.7 CommandShell - The Embedded CLI

An embedded Command Line Interface (CLI) is available for basic configuration and diagnostics. The CLI (or CommandShell) can be accessed via VoPLib API, Telnet and the embedded Web server.

To enable Telnet access, set the parameter TelnetServerEnable to 1 or 2.

CLI commands are organized in folders. When first entering the CLI, the user is located at the root folder. The CLI lists the available commands and sub folders. Enter 'h' at the ComamndShell prompt for help on the global commands. 'h <command name>' will provide help on a specific command.

The following CLI commands are available:

/CONFiguration folder:

SaveAndReset	Save all ini-file parameters to non-volatile memory, and reset the board
RestoreFactorySettings	Restore factory settings of all ini-file parameters
SetConfigParam	Set ini file parameters from the shell
GetParameterDescription	Display description of an ini-file parameter
GetConfigParam	Query ini file parameters from the shell
ConfigFile	Retrieve or set current configuration file via Telnet
AutoUPDate	Check for new ini/CMP files, configured in INIFILEURL and CMPFILEURL

/MGmt/FAult folder:

ListActive	List the currently active alarms
ListHistory	Show the alarm history table

/IPNetworking/Ping folder:

Ping	Ping a remote IP address
PingGetStat	Get the status of active ping sessions
PingStop	Stop active ping sessions

/TPApp folder:

BoardInfo	Display general information about the product
LoadVersion	Display the current SW version number
TimeOfDay	Display the system's date and time of day

/BSP/EXCeption folder:

ExceptionInfo	Display information on the last SW exception
PrintHistory	Display the SW exceptions history

8.8 Control Protocol Reports

8.8.1 MGCP Error Conditions

When working with MGCP, the MediaPack reports error conditions via the Call Manager (or via a Call Manager of the Customer's choice), using the standard MGCP facilities, through the Network Interface. For documentation on MGCP error conditions, go to the IETF web site at URL <http://www.ietf.org/rfc/> and open RFC 2705 for MGCP.

8.8.2 SNMP Traps

MediaPack supports Trunk MIB traps according to RFC 2495. For documentation on SNMP event errors, go to the IETF web site at URL <http://www.ietf.org/rfc/> and open RFC 2495.

The Trunk MIB contains objects relevant to E1/T1 Trunk interfaces. In this version, only the dsx1ConfigTable fields and dsx1LineStatusChange NOTIFICATION (Trap) are supported.

8.9 Solutions to Possible Problems

8.9.1 Solutions to Possible Voice Problems

Solutions to possible voice problems are described in the table below:

Table 8-2: Solutions to Possible Voice Problems

Problem	Possible Cause	Solution
G.711 voice quality is bad (clicks)	Silence compression not compatible (when working with different Gateway other than AudioCodes Gateway)	Disable it and check if quality is better.
	Packet size not compatible (with G.711)	Check that packet period in remote side is 20 msec. Check that the correct μ -law or A-law compression is in use
No voice	There is no match in codecs	Check log in HyperTerminal/syslog. Change codec definition.

8.9.2 Solutions to Possible General Problems

Solutions to possible general problems are described in the table below:

Table 8-3: Solutions to Possible General Problems

Problem	Possible Cause	Solution
No communication	Software does not function in MediaPack	Try to "ping" to MediaPack. If ping fails, check for network problems/definitions and try to reset the MediaPack.
	Network problem	Check the cables.
	Network definitions	Check if the default gateway can reach the IP of box. Check if the box got the correct IP (see it in the HyperTerminal screen).

Table 8-3: Solutions to Possible General Problems

Problem	Possible Cause	Solution
		Check the validity of IP address, subnet and default gateway. If the default gateway is not used, enter 0.0.0.0
	BootP did not reply to box	Check if the BootP server replied to the box at restart. See it in the log of BootP server.
		Try to restart the BootP server.
	Check the MAC address of the box in BootP server.	
ini file was not loaded	The TFTP server is down	Check if the TFTP server working.
	The TFTP server did not get the request	Check the log of the TFTP server.
	MediaPack did not request the file from your TFTP	See in HyperTerminal the TFTP server IP address that the MediaPack is trying to use.
	TFTP server bug	Try to restart the TFTP server.
	The BootP sent to MP the wrong TFTP server address	Check in the HyperTerminal screen the address of used TFTP.
	The <i>ini</i> file does not exists in default directory of the TFTP Server	Check the default directory of the TFTP server and check that the <i>ini</i> file exists there.
	Wrong <i>ini</i> file name	Verify in windows explorer that the file extensions are displayed and the <i>ini</i> file is not by mistake " <i>XXX.ini.ini</i> ". Verify that the file extension " <i>ini</i> " is in lowercase letters.
TFTP's timeout is too short	Verify that the TFTP server settings are: Timeout = 2 sec, # of retransmission = 10	
Wrong ini file loaded	The <i>ini</i> file is not in the correct path	An old <i>ini</i> file was probably loaded. Check which <i>ini</i> file was loaded. This can be done using the HyperTerminal screen.
	The <i>ini</i> corrupted	Check the <i>ini</i> file syntax.
BootP reply from wrong BootP server	Other BootP servers contain the MAC address of the MediaPack	Check that only your BootP server contains the MediaPack MAC address.

9 Selected Technical Specifications

9.1 MP-11x Specifications

Table 9-1: MP-11x Functional Specifications (continues on pages 179 to 180)

Channel Capacity	
Available Ports	MP-112R 2 ports* MP-114 4 ports MP-118 8 ports * The MP-112R differs from the MP-114 and MP-118. Its configuration excludes the RS-232 connector, the Lifeline option and outdoor protection.
MP-11x/FXS Functionality	
FXS Capabilities	<p>Short or Long Haul (Automatic Detection): REN2: Up to 10 km (32,800 feet) using 24 AWG line. REN5: Up to 3.5 km (11,400 feet) using 24 AWG line.</p> <p>Note: The lines were tested under the following conditions: ring voltage greater than 30 Vrms, offhook loop current greater than 20 mA (all lines ring simultaneously).</p> <p>MP-11x includes lightning and high voltage protection for outdoor operation. The following standards are supported: EN61000-4-5, EN55024 and UL60950.</p> <p>Caller ID generation: Bellcore GR-30-CORE Type 1 using Bell 202 FSK modulation, ETSI Type 1, NTT, Denmark, India, Brazil, British and DTMF ETSI CID (ETS 300-659-1).</p> <p>Programmable Line Characteristics: Battery feed, line current, hook thresholds, AC impedance matching, hybrid balance, Tx & Rx frequency response, Tx & Rx Gains.</p> <p>Programmable ringing signal. Up to three cadences and frequency 15 to 200 Hz.</p> <p>Drive up to 4 phones per port (total 32 phones) simultaneously in offhook and Ring states. MP-11x Ring Equivalent Number (REN) = 5</p> <p>Over-temperature protection for abnormal situations as shorted lines.</p> <p>Loop-backs for testing and maintenance.</p>
Voice Messaging	
Playback from Local Storage	Prompts and announcements playback (1 MB integral memory for 2 min. of G.711 or 20 min. for G.723 recorded prompts)
Fax/Modem Transport	
Fax Relay and Bypass	<p>Supported on all ports</p> <p>Group 3 real-time Fax Relay to 14.4 kbps with auto fallback</p> <p>Tolerant of delays of up to 9 seconds</p> <p>T.30 (PSTN) and T. 38 (IP) compliant (real-time fax)</p> <p>CNG tone detection & Relay per T.38</p> <p>Automatic Fax ByPass (pass-through) to G.711 or ADPCM</p>
Modem Bypass	Automatic switching (pass-through) to PCM or ADPCM for modem signals (V.34 or V.90 modem detection)
Processor	
Control Processor	Motorola PowerQUICC 870

Table 9-1: MP-11x Functional Specifications (continues on pages 179 to 180)

Control Processor Memory	SDRAM - 32 MB		
Signal Processors	AudioCodes AC482 VoIP DSP		
Interfaces			
FXS Telephony Interface	2, 4 or 8 Analog FXS phone or fax ports, loop start (RJ-11)		
Network Interface	10/100 Base-TX		
RS-232 Interface	RS-232 Terminal Interface for maintenance and diagnostic reports (requires a DB-9 to PS/2 adaptor).		
Lifeline	Lifeline provides a wired analog POTS phone connection to any PSTN or PBX FXS port when there is no power, or the network fails. (Not applicable to MP-112R)		
Connectors & Switches			
Rear Panel			
8 Analog Lines (MP-118)	8 RJ-11 connectors		
4 Analog Lines (MP-114)	4 RJ-11 connectors		
2 Analog Lines (MP-112)	2 RJ-11 connectors		
AC power supply socket	100-240~0.3A max.		
Ethernet	10/100 Base-TX, RJ-45		
RS-232	Console PS/2 port		
Reset Button	Resets the MP-11x		
Physical			
Dimensions (HxWxD)	42 x 172 x 220 mm		
Environmental	Operational:	5° to 40° C	41° to 104° F
	Storage:	-25° to 70° C	-77° to 158° F
	Humidity:	10 to 90% non-condensing	
Mounting	Rack mount, Desktop, Wall mount.		
Electrical	100-240 VAC Nominal 50/60 Hz		
LED Indicators			
LED Indications on Front Panel	Activity (per port), Uplink, Fail, Ready, Power		
Type Approvals			
Safety and EMC	UL 60950, FCC part 15 Class B CE Mark (EN 60950, EN 55022, EN 55024)		
Management			
Configuration	Gateway configuration using Web browser, <i>ini</i> files or local RS-232 console		
Management and Maintenance	SNMP v2c		
	Syslog, per RFC 3164		
	Local RS-232 terminal		
	Web Management (via HTTP or HTTPS)		
	Telnet		

All specifications in this document are subject to change without prior notice.

9.2 MP-1xx Specifications

Table 9-2: MP-1xx Selected Technical Specifications (continues on pages 181 to 183)

MP-1xx/FXS Functionality	
FXS Capabilities	Short or Long Haul: MP-10x/FXS: Up to 7 km (23,000 feet) using 24 AWG line. MP-124/FXS: Up to 6 km (20,000 feet) using 24 AWG line. Note: The lines were tested under the following conditions: ring voltage greater than 30 Vrms, offhook loop current greater than 20 mA.
	Caller ID generation: Bellcore GR-30-CORE Type 1 using Bell 202 FSK modulation, ETSI Type 1, NTT, Denmark, India, Sweden, Brazil, British and DTMF ETSI CID (ETS 300-659-1).
	Programmable Line Characteristics: Battery feed, line current, hook thresholds, AC impedance matching, hybrid balance, Tx & Rx frequency response, Tx & Rx Gains.
	Programmable ringing signal. Up to three cadences and frequency 10 to 200 Hz.
	Drive up to 4 phones per port (total 32 phones) simultaneously in offhook and Ring states. MP-124 REN = 2 MP-10x REN = 5
	Over-temperature protection for abnormal situations as shorted lines. Loop-backs for testing and maintenance.
MP-10x/FXO Functionality	
FXO Capabilities (does not apply to MP-102 and MP-124)	Short or Long Haul.
	Includes lightning and high voltage protection for outdoor operation.
	Programmable Line Characteristics: AC impedance matching, hybrid balance, Tx & Rx frequency response, Tx & Rx Gains, ring detection threshold, DC characteristics.
	Caller ID detection: Bellcore GR-30-CORE Type 1 using Bell 202 FSK modulation, ETSI Type 1, NTT, Denmark, India, Sweden, Brazil and DTMF ETSI CID (ETS 300-659-1).
Voice Messaging	
Playback from Local Storage	Prompts and announcements playback (1 MB integral memory for 2 min. of G.711 or 20 min. for G.723 recorded prompts)
Fax and Modem Transport	
Fax Relay and Bypass	Supported on all ports
	Group 3 real-time Fax Relay to 14.4 kbps with auto fallback
	Tolerant of delays of up to 9 seconds
	T.30 (PSTN) and T. 38 (IP) compliant (real-time fax)
	CNG tone detection & relay per T.38
	Automatic Fax ByPass (pass-through) to G.711 or ADPCM
Modem Bypass	Automatic switching (pass-through) to PCM or ADPCM for modem signals (V.34 or V.90 modem detection)
Control Protocols	
MGCP (RFC 2705)	Call control, Basic announcements package, Conferencing

Table 9-2: MP-1xx Selected Technical Specifications (continues on pages 181 to 183)

Processor	
Control Processor	Motorola PowerQUICC 860
Control Processor Memory	SDRAM – 16 MB
Signal Processors	AudioCodes AC481 VoIP DSP
Interfaces	
FXS Telephony Interface	2, 4, 8 or 24 Analog FXS phone or fax ports, loop start
FXO Telephony Interface	4 or 8 Analog FXO PSTN/PBX loop start ports
Network Interface	RJ-45 shielded connector, 10/100 Base-TX.
RS-232 Interface	RS-232 Terminal Interface for maintenance, diagnostic reports and code tracing. DB-9 connector on rear panel
Lifeline (MP-10x/FXS)	Lifeline provides a wired analog POTS phone connection to any PSTN or PBX FXS port when there is no power, or the network fails.
Connectors & Switches	
Rear Panel	
24 Analog Lines (MP-124)	50-pin Telco shielded connector
8 Analog Lines (MP-108)	8 RJ-11 connectors
4 Analog Lines (MP-104)	4 RJ-11 connectors
2 Analog Lines (MP-102)	2 RJ-11 connectors
Ethernet	10/100 Base-TX, RJ-45 shielded connector
RS-232	Console port - DB-9
Front Panel	
Reset	Resets the MP-1xx
Physical	
MP-10x Enclosure Dimensions	Width: 221 mm 8.7 in Height: 44.5 mm 1.75 in Depth: 240 mm 9.5 in Weight: 1.24 kg 2.5 lb
MP-124 Enclosure Dimensions	1U, 19-inch Rack Width: 445 mm 17.5 in Height: 44.5 mm 1.75 in Depth: 269 mm 10.6 in Weight: 2.24 kg 4.9 lb
Environmental	Operational: -5° to 55° C 23° to 131° F Storage: -40° to 70° C -40° to 158° F Humidity: 10 to 90% non-condensing
Installation	Desk-top, shelf, or 19-inch rack mount with side brackets.
Electrical	Maximum operating voltage range 90-264 VAC Nominal operating voltage range 100-250 VAC, 0.5A, 47-63 Hz
Type Approvals	
Telecommunication	FCC part 68 & CE CTR21, ASIF S003 (FXS)
Safety and EMC	UL 60950-1, FCC part 15 Class B CE Mark (EN 60950-1, EN 55022, EN 55024)
Management	
Configuration	Gateway configuration using Web browser, <i>ini</i> files or local RS-232 console
Management and Maintenance	SNMP v2c Syslog, per RFC 3164

Table 9-2: MP-1xx Selected Technical Specifications (continues on pages 181 to 183)

	Local RS-232 terminal
	Web Management (via HTTP)
	Telnet

Reader's Notes

10 Appendix A - BootP/TFTP Server

10.1 Introduction

The **BootP/TFTP Server** enables easy configuration and provisioning for AudioCodes boards and Media Gateways. The BootP and TFTP servers contain specific adaptations as per manufacturer requirements. The latest version of the BootP/TFTP application is 2.3.0.5.

10.1.1 Key Features

- Internal BootP server supporting hundreds of entities
- Internal TFTP server
- Contains all required data for AudioCodes products in predefined format
- Provides a TFTP server address, enabling network separation of TFTP and BootP servers
- Tools to backup and restore the local database
- Templates
- User-defined names for each entity
- Option for changing MAC address
- Protection against entering faulty information
- Remote reset
- Unicast BootP respond
- User-initiated BootP respond, for remote provisioning over WAN
- Filtered display of BootP requests
- Location of other BootP servers that contain the same MAC entity
- Common log screen for both BootP and TFTP sessions
- Display of manufacturer vendor specific information parameters
- Support for manufacturer's selective BootP feature (The BootP server inserts manufacturer specific vendor information that includes the text, AUDC)
- Compatible with Windows™ 98, Windows™ NT, Windows™ 2000, Windows™ XP

10.1.2 Specifications

- BootP standards: RFC 951 and RFC 1542
- TFTP standards: RFC 1350 and RFC 906
- Operating System: Windows 98, Windows NT and Windows 2000, Windows XP

- Maximum number of MAC entries: 200
- BootP Fields:
 - Hardware address (MAC): 12 hex digits
 - IP address
 - Subnet
 - Default Gateway
 - TFTP server IP (Using the TFTP server IP field enables download of firmware from a different Host)
 - Boot File
 - *ini* File
 - Call Agent IP
 - New MAC (optional)
- Screens:
 - File Upload and Message screen
 - Preferences screen
 - Client Configuration screen
 - Template Definition screen

10.1.3 BootP/TFTP Server Installation

The BootP/TFTP Server can be installed on a PC from the MP-11x Software & Documentation CD.

➤ **To install the BootP/TFTP Server, take these 3 steps:**

1. Unzip the *TPxx.exe* file and navigate to the BootP *zip* file under `.\Utilities\BootP & TFTP server`.
2. Double click on the BootP *zip* file and run *setup.exe*. The installation procedure begins. After completing the procedure, open Start>Programs>BootP. **The BootP/TFTP Server** main screen is displayed.
 - i. At first run, the user is requested to fill in the fields displayed on the Preferences screen.
3. To open the Preferences screen, from the main screen, select **Edit>Preference**. Follow the directions detailed in 'Preferences Screen' on page 190 to configure the screen.

10.1.4 Logging Screen

The BootP/TFTP Server main screen (refer to the figure, 'Main Screen' on page 188) includes the Log line, printed per BootP request with the following parameters:

- Hardware (MAC) address
- Status (found or not found in cache)
- Date and Time

- Assigned IP address (if found)
- Client name
- Client specific Information - contains vendor specific information, which includes: Board type, last IP, bootload version, flash *cmp* version, Analog type (FXS/FXO), and number of analog channels (for MP family). In order to access the board information, add *-be 1* to the *ini* file selection in the BootP application. With this initial setting, even after deleting *-be 1*, the board continues to report its internal data.
- Clicking a Log line displays all BootP reply parameters or enables entry to a new entity.
- Right clicking a Log line opens up a menu.
- Selecting **Reset** causes a soft reset of the board. Reset is available only for client MACs that are configured on the BootP server. The second option on the menu is View Client, which produces the same display as when clicking on the Log line.

10.1.5 Preferences Screen

The Preferences screen (refer to the figure, 'Preferences Screen' on page 190) is used to define BootP and TFTP configuration parameters:

- TFTP directory
- ini File Mask
- Boot File Mask
- TFTP timeout and number of retransmissions
- BootP replay type (Broadcast or Unicast)
- BootP ARP mode (dynamic or static)
- Number of initiated BootP replies (send after remote reset), optionally used when the MP-11x is installed behind the firewall that blocks BootP broadcast requests.

10.1.6 Client Configuration Screen

The Client Configuration screen (refer to the figure, 'Client Configuration Screen' on page 191) shows:

- All client entities
- MAC
- Name
- IP per entity
- With this screen, users can:
 - Add a new entry
 - Delete an existing entry
 - Modify an existing entry
 - Test a selected client for finding all BootP servers that respond to a BootP request with a specific MAC address

If a template is selected, any parameter can be entered manually or copied from the selected template by marking the checkbox to the right of the parameter. Usually, only an IP address is entered manually while other parameters are copied from the template.

10.1.7 Template Screen

The Template screen (refer to the figure, 'Templates screen' on page 192) enables the user to add, modify, or delete templates.

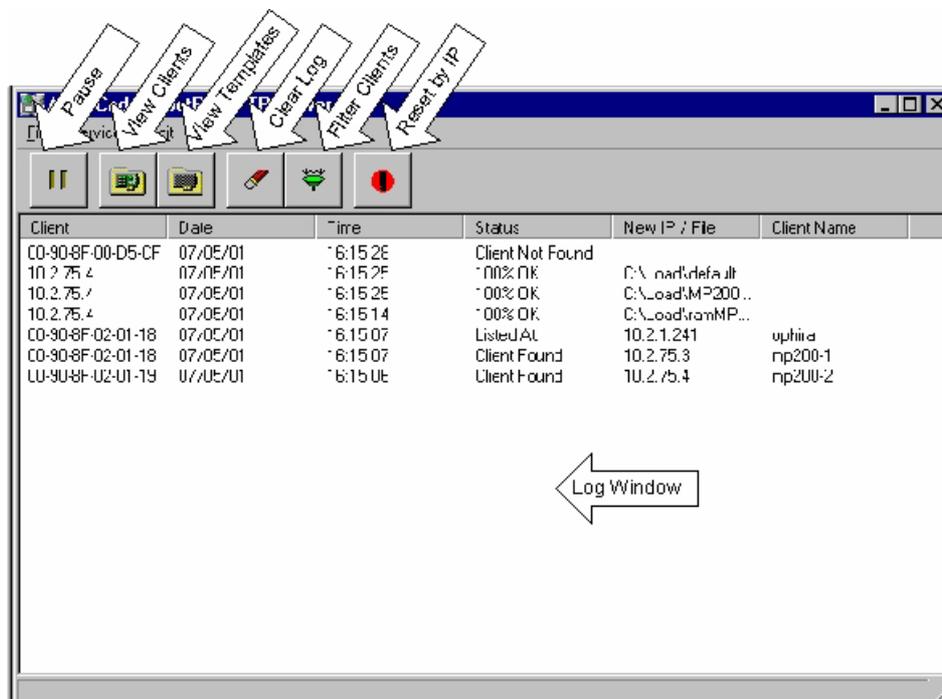
The template includes:

- Subnet
- Gateway, TFTP server
- BootFile
- ini file
- Call Agent fields
- Server IP

10.2 Screen Details

10.2.1 Main Screen

Figure 10-1: Main Screen



The figure above shows the main screen of the **BootP/TFTP Server**, featuring:

- Program State - Pauses the program. When the program is paused, no replies to

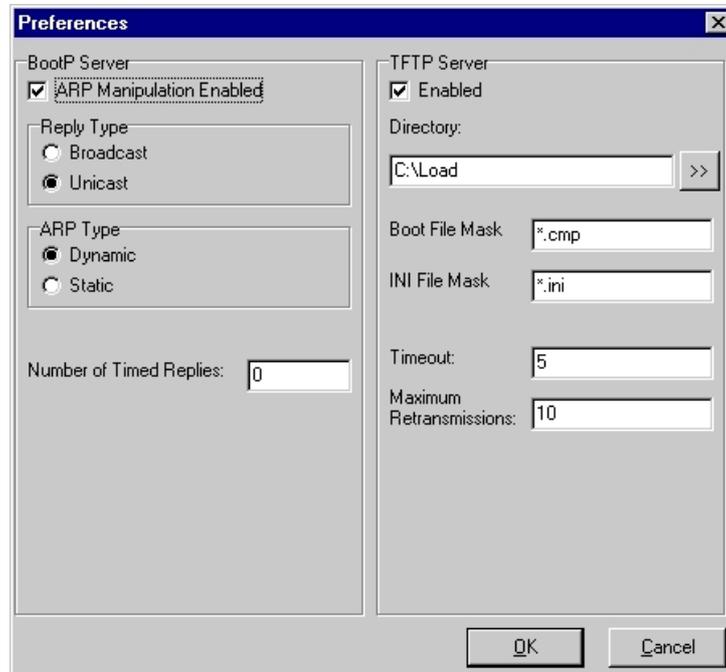
BootP requests are sent.

- View Clients button - Opens up the Clients Configuration screen.
- View Templates button - Opens up the Templates Configuration screen.
- Clear Log button - Clears the log.
- Filter Unknown Clients button - Filters all BootP requests that are not listed in the Client Configuration screen.
- Reset button - Opens a dialog, in which users can enter an IP of a client. The program sends a reset command to that client.
- Edit>Preferences - Opens the Preferences screen for defining BootP and TFTP parameters.
- Log Screen - Displays all BootP requests and TFTP sessions, including the time and date of the request. In addition, the response type is also displayed:
 - Client Not Found
 - Client Found
 - Client's Mac Changed
 - Client Disabled
- Listed at (when using the Test Selected Clients button).
- For a TFTP session, file name and download status are displayed.
- Pop-Up Menu - Right-clicking on a line in the log screen displays the pop-up menu. In this menu there two options:
 - **Reset** - When this option is selected, the program searches the database for the selected MAC. When the client is found, the program adds the client's MAC to the ARP table, and then sends a reset command to the client. Note that by performing the remote reset this way, the user does not have to know the current IP address of the client. To perform this option, the user must have administrator privileges, otherwise an error message appears.
 - **View Client** - This option is the same as double-clicking on a line. When selected, the Clients Screen opens. If the Client's MAC is found in the database, it is focused. If not, a new client is added, with the MAC filled out. The remaining fields require fill in.

10.2.2 Preferences Screen

In the Preferences screen shown below, BootP and TFTP configuration parameters are defined.

Figure 10-2: Preferences Screen



In the BootP section, the user can select ARP mode: Dynamic or Static, and reply type: Broadcast or Unicast. For a typical application, use Dynamic ARP mode and Unicast, as shown above.

This option requires the **user to have administrator privileges** otherwise an error message appears. If you don't have administrator privileges, **uncheck** the ARP Manipulation Enabled checkbox in the Preferences Screen.

The **Number of Timed Replies** (the number of initiated timed BootP replies) can be used when the MP-11x is installed behind a Firewall that blocks BootP broadcast requests. In a typical application, this feature can be disabled by entering **0** in this field. When selected, several BootP replies are sent to the MP-11x immediately after the remote reset command.

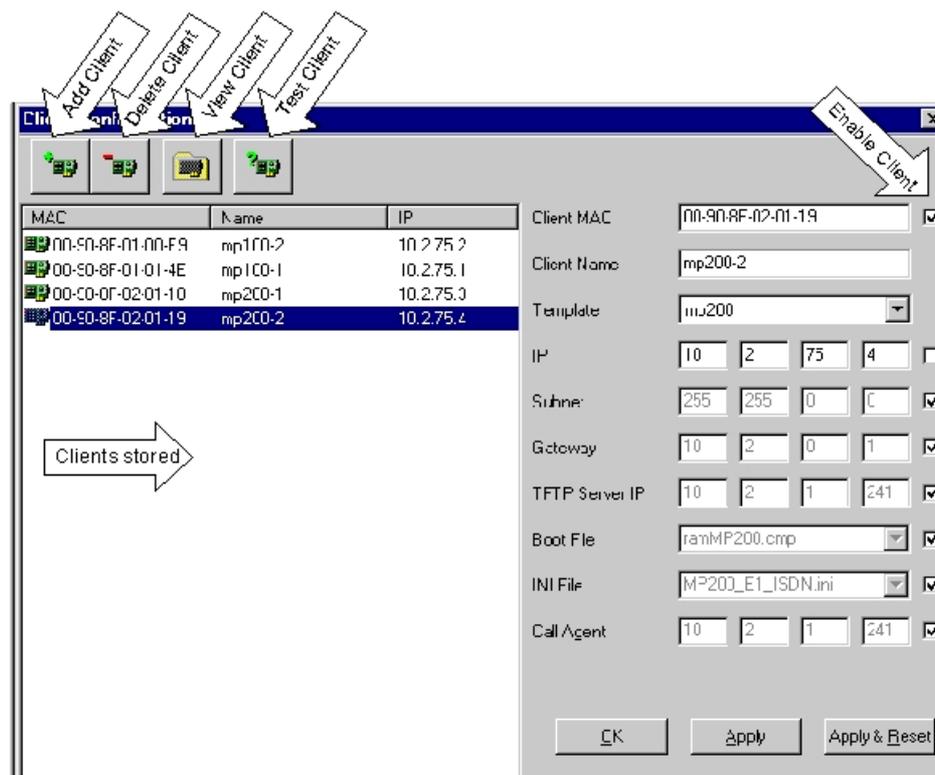
For the TFTP server, the user can configure a TFTP directory and a value for TFTP Timeout and Maximum Retransmissions. Set these values to **2** and **10** as shown above.

The TFTP server can be disabled by clearing the Enable checkbox.

10.2.3 Client Configuration Screen

The figure below is the Client Configuration Screen in which clients are added and defined.

Figure 10-3: Client Configuration Screen



In the left pane of the screen is the client list. By clicking on a client in this list, the following parameters for this client are displayed on the right side of the screen:

- Client MAC - This is the MAC address of the client. When the user edits the MAC, a new client is added, with the same parameters as the previous client. The client can be disabled by un-checking the check box on the right side of the Client MAC. This causes the BootP server not to reply to the BootP request. The client can be enabled by checking the check box. Click on the 'Apply' button each time the client enable check box is checked or unchecked.
- Client Name - A text field for entering the client description.
- Template - The template to be used for this client. When a template is selected, its parameters override all of the previous parameters.
- IP, Subnet, Gateway - Normal IP parameters.
- TFTP Server IP - The IP address of the TFTP Server.
- Boot File, ini File - The files to request from the TFTP server.

Note the seven check boxes to the right of the parameters. These enable the user to assign only the fields from the template, which have adjacent marked checkboxes. The rest can be unique for each client. When the field is assigned a value from the selected template, the field is grayed (and unmodifiable).

To save them after performing changes, click **Apply**. By clicking **Apply & Reset**, the program saves the changes to the database, performs a remote Reset to the client by adding the client's MAC to the ARP table, and then sends out a reset command. This option works **only if "ARP Manipulation Enabled"** checkbox in the "Preferences" screen is **checked** (in the figure, 'Preferences Screen' on page 190) otherwise an error message appears. It requires the user to have **administrator privileges**. The remote reset is supported for software in this version and up.

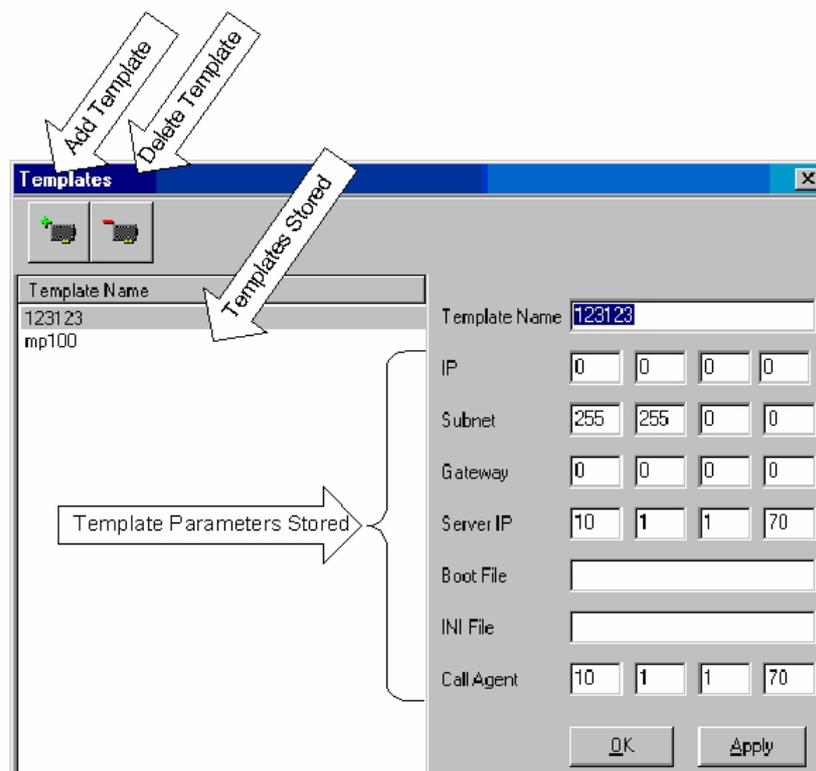
When adding a new client, click **Add Client**. A client dialog box with blank parameters is displayed. After filling out the parameters, click **Apply**. The client is added.

To find out if there is another BootP server on the net that contains a client with the same MAC address, click **Test Selected Clients**. In the log screen, view the IP addresses of all BootP servers that contain the same MAC address in the status 'Listed At'. In normal operation, BootP client MAC address should be listed only on a single BootP server. If the MAC address is listed in multiple BootP servers, it must be removed from other BootP servers.

10.2.4 Templates Screen

The figure below shows the Templates screen, which provides a fast way to configure a number of clients that have the same parameters (except for the IP address). To use the Templates screen, create a template, and then apply the template to the client by selecting it.

Figure 10-4: Templates Screen



Reader's Notes

11 Appendix B - Individual *ini* File Parameters

11.1 Individual ini File Parameters

The individual parameters contained in the *ini* file are provided in the following parameter group tables:

- System Parameters (refer to 'System Parameters')
- Infrastructure Parameters (refer to "Infrastructure Parameters" on page 199)
- Media Processing Parameters (refer to "Media Processing Parameters" on page 205)
- Analog Parameters (refer to 'Analog Parameters')
- Common Control Protocols Parameters (refer to "Common Control Protocols Parameters" on page 218)
- MGCP Specific Parameters (refer to "MGCP Specific Parameters" on page 223)
- Web Interface Parameters (refer to 'Web Interface Parameters')
- SNMP Parameters (refer to "SNMP Parameters" on page 226)
- Names for optional configuration files (Call Progress Tones and Voice Prompts files).

Users do not have to specify all (or any) of the parameters in the *ini* file. If a parameter is left unspecified in an *ini* file and the *ini* file is then loaded to the MP-11x, the MP-11x is configured with that parameter's default value. Leaving all *ini* file parameters unspecified and loading the file to the MP-11x is thus result in the MP-11x being configured with its defaults (contained in the software image *cmp* file).



Note: To restore the MP-11x's default configuration parameters, use an empty *ini* file without any valid parameters or with a semicolon (;) preceding all lines in the file.

Array Parameters

Some parameters have array values. For each of these parameters listed in the parameter tables below, if the *ini* file field name is used as is, the parameter applies to all of its elements. To specify each element individually, add *_xx* (*xx* equals the element number) to the end of the *ini* file field name. Information about the array value's elements is contained in the Description column.

11.1.1 System Parameters

The table below lists and describes the system parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 11-1: System Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
AlarmHistoryTableMaxSize	<p>Determines the maximum number of rows in the Alarm History table.</p> <p>The parameter is controllable via the Config Global Entry Limit MIB (located in the Notification Log MIB).</p> <p>Default = ALARM_HISTORY_DEFAULT_SIZE</p> <p>Range: 50 to 1000 (for MP-1xx media gateways, the range is 50 to 100).</p>	See Descr.	See Descr.
AutoUpdateCmpFile	<p>Updates cmp file automatically.</p> <p>1 = Enable; 0 = Disable</p>	0	0 or 1
AutoUpdateFrequency	<p>Defines the number of minutes to wait in between automatic updates to the configuration files.</p>	0	-
AutoUpdatePredefinedTime	<p>Schedules the update of configuration files to a predefined time of the day (hh:mm).</p> <p>Range = 'HH:MM' (24-hour format)</p>	NULL	See Descr.
CmpFileURL	<p>Links to a software image (cmp file) to be downloaded from a remote server.</p> <p>Range = ftp://server_ip/file, http://server_name/file, https://server_name/file</p>	NULL	See Descr.
CptFileUrl	<p>Links to a Call Progress Tones (CPT) file to be downloaded from a remote server.</p> <p>Range = http://server_name/file, https://server_name/file</p>	NULL	See Descr.
DisableRS232	<p>Enables or disables an RS-232 task.</p> <p>0 = Enable; 1 = Disable</p>	0	0 or 1
DisableWebConfig	<p>Enables or disables Web Configuration</p> <p>0 = Read & Write mode (default)</p> <p>1 = Read Only mode</p>	0	0 or 1
DisableWebtask	<p>Enables or disables Web Server Task</p> <p>0 = Enable (default) 1 = Disable</p>	0	0 or 1
DNSPriServerIP	<p>Defines the DNS primary server's IP address.</p> <p>Range = Legal IP address</p>	0.0.0.0	See Descr.

Table 11-1: System Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
DNSSecServerIP	Defines the DNS secondary server's IP address. Range = Legal IP address	0.0.0.0	See Descr.
EnableParametersMonitoring	Enables monitoring of on-the-fly parameter changes via Syslog messages. 1 = Activate; 0 = Deactivate (default)	0	0 or 1
EnableSTUN	Enables the STUN module, used for NAT traversal of UDP packets.	0	0 or 1
EnableSyslog	Enables the Syslog protocol log. 1 = Activate; 0 = Deactivate	0	0 or 1
FXOCoeffFileUrl	Links to an FXO coefficients file, to be downloaded from a remote server. Range = http://server_name/file, https://server_name/file	NULL	See Descr.
FXSCoeffFileUrl	Links to an FXS coefficients file, to be downloaded from a remote server. Range = http://server_name/file, https://server_name/file	NULL	See Descr.
IniFileTemplateUrl	Links to an ini file to be downloaded from a remote server, in addition to IniFileUrl. Range = http://server_name/file, https://server_name/file	NULL	See Descr.
IniFileURL	Link to an ini file to be downloaded from a remote server. Range = ftp://server_ip/file, http://server_name/file, https://server_name/file	NULL	See Descr.
InitialShellCommand	A Command Shell command to be executed during initialization. Several commands can be entered (separated by a semicolon).	NULL	-
NATBindingDefaultTimeout	Defines the NAT binding lifetime, in seconds. STUN refreshes the binding information after this time expires. Range = 0 to 2592000	30	See Descr.
NTPServerIP	This parameter is used to define the NTP server's IP address. Range = Legal IP address	0.0.0.0	See Descr.

Table 11-1: System Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
NTPServerUTCOffset	This parameter is used to define the NTP time to offset, in seconds. Range = -43200 to + 43200 seconds	0	See Descr.
NTPUpdateInterval	This parameter defines the NTP update interval, in seconds. Do not set it exceeding 1 month (2592000 seconds). Range = 0 to 2592000 seconds Default = 86400 seconds	See Descr.	See Descr.
PrtFileUrl	Links to a prerecorded tones dat file, to be downloaded from a remote server. Range = http://server_name/file, https://server_name/file	NULL	See Descr.
SaveConfiguration	Determines if the device configuration (and the loadable file) is saved in flash. Choose either: 1 = Save configuration file (the Call Progress Tones, PRT and/or coefficient file) in non-volatile memory 0 = Don't save	1	0 or 1
SendKeepAliveTrap	When Enabled, this parameter invokes the keep-alive trap and sends it out every 9/10 of the time defined in the parameter defining NAT Binding Default Timeout.	0	-
STUNServerPrimaryIP	Defines the primary STUN Server IP address. Range = Legal IP address	0.0.0.0	See Descr.
STUNServerSecondaryIP	Defines the secondary STUN server IP address. Range = Legal IP address	0.0.0.0	See Descr.
SyslogServerIP	Defines the IP address in dotted format notation. e.g., 192.10.1.255 Range = Legal IP address	0.0.0.0	See Descr.
TelnetServerEnable	Enables or disables the embedded Telnet server. Telnet is disabled by default for security reasons.	0	0 to 2

Table 11-1: System Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	0 = Disable 1 = Enable 2 = SSL mode (if available - requires an SSL-aware Telnet client software) SSL mode is not available on the MP-108 / MP-124 media gateways		
TelnetServerIdleDisconnect	This parameter is used to set the timeout for disconnection of an idle Telnet session (minutes). When set to zero, idle sessions are not disconnected.	0	Any number
TELNETSERVERPORT	Defines the port number for the embedded Telnet server. Range = Valid port number	23	See Descr.
VpFileUrl	Links to a Voice Prompts file to be downloaded from a remote server. Range = http://server_name/file, https://server_name/file	NULL	See Descr.

11.1.2 Infrastructure Parameters

The table below lists and describes the Infrastructure parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 11-2: Infrastructure Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
AuthorizedTPNCPServers	Sets the IP address of TPNCPC authorized server. Range = IP address in dotted notation xxx.xxx.xxx.xxx	0.0.0.0	See Descr.
BaseUDPPort	Defines the lower boundary of UDP ports to be used by the board. The upper boundary is calculated on the basis of BoardBaseUDPPort + 10 * (Number of Channels). This parameter value must be a multiple of 10.	4000	0 to 55000
BootPDelay	Defines the delay that occurs from the time the board is reset until the first	1	1 to 7 & 15

Table 11-2: Infrastructure Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	<p>BootP request is issued by the board. This parameter takes effect only from the time the board is next reset.</p> <p>1 = 1 BootP retry, 1 sec. 2 = 2 BootP retries, 3 sec. 3 = 3 BootP retries, 6 sec. 4 = 10 BootP retries, 30 sec. 5 = 20 BootP retries, 60 sec. 6 = 40 BootP retries, 120 sec. 7 = 100 BootP retries, 300 sec. 15 = BootP retries indefinitely.</p>		
BootPRetries	<p>Defines the number of BootP retries that the board sends during start-up. The board stops issuing BootP requests when either an AA122BootP reply is received or the Number Of Retries is reached. This parameter takes effect only after the next board reset.</p>	3	1 to 14
BootPSelectiveEnable	<p>Configures the board so that it will only accept BootP replies, from AudioCodes proprietary BootP-TFTP Software.</p> <p>1 = Enable; 0 = Disable</p>	0	0 or 1
DHCPEnable	<p>Enables/disables DHCP support.</p> <p>0 = Disable; 1 = Enable</p> <p>After the gateway is powered up, it attempts to communicate with a BootP server. If a BootP server does not respond and if DHCP is enabled, the gateway attempts to obtain its IP address and other network parameters from the DHCP server.</p> <p>Note: If working with the AudioCodes BootP/TFTP application, throughout the DHCP procedure, the BootP/TFTP application must be deactivated. If it isn't deactivated, the gateway receives a response from the BootP server instead of the DHCP server.</p> <p>For additional information on DHCP, refer to the product documentation.</p>	0	0 or 1

Table 11-2: Infrastructure Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
DHCPspeedFactor	Controls the DHCP renewal speed. 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. 0 = Disable DHCP 1 = Normal 2 to 10 = Fast	1	0 to 10
DisableTPNCPEvent	Disables Events Reporting. For the selected event, refer to enumerator acTEvent. Range = nn = TPNCPEventID to hide. Refer to the VoPLib manual for additional information.	1	See Descr.
EnableDetectRemoteMACChange	Allows for the detection of an incoming RTP stream from a changed remote MAC address. Used for board redundancy purposes. 0 = Disable 1 = Enable (trigger by media) 2 = Enable (trigger by GARP) 3 = Enable (trigger by either media or GARP)	3	0 to 3
EnableDiagnostics	Checks the correct functionality of the different hardware components on the board. On completion of the check, the board sends an EV_END_BIT value, which contains information on the test results of each hardware component. 0 = No diagnostics (default). 1 = Perform diagnostics (full test of DSPs, PCM, Switch, LAN, PHY and Flash). 2 = Perform diagnostics (full test of DSPs, PCM, Switch, LAN, PHY, but partial, test of Flash, a quicker mode).	0	0 to 2
EnableICMPUnreachableReport	Reports receipt of unreachable ICMP packets. 0 = Disabled; 1 = Enabled	1	0 or 1
EnableIPAddrTranslation	Specifies the type of compare operation performed on the first packet that is received on a newly	1	0 or 1

Table 11-2: Infrastructure Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	<p>opened channel for the Network Address Translation (NAT) feature. If set to 1, the board compares the first incoming packet's source IP address, to the remote IP address stated in the opening of the channel. If the two IP addresses do not match, the NAT operation takes place. Consequently, the remote IP address and the UDP port of the outgoing stream are replaced by the source IP address and UDP port of the first incoming packet.</p> <p>0 = Disable; 1 = Enable</p>		
EnableLANWatchdog	<p>Detects LAN failures on the board. A LAN failure can result from a software or hardware malfunction. If a LAN failure is detected, the board performs a self reset (when not in PCI mode).</p> <p>0 = Disable; 1 = Enable</p>	0	0 or 1
EnableTPNCPSecurity	<p>Secures the TrunkPack Network Control Protocol (TPNCP) by accepting only pre-determined servers via the parameter defining authorized TPNCP servers.</p> <p>1 = Enabled; 0 = Disabled</p>	0	0 or 1
EnableUDPPortTranslation	<p>Specifies the type of compare operation performed on the UDP ports. When set, the compare operation is performed on the UDP ports. If this parameter is set, EnableIpAddrTranslation must also be set.</p> <p>0 = Disable; 1 = Enable</p>	0	0 or 1
EthernetPhyConfiguration	<p>Controls the Ethernet connection mode type. Auto-negotiate falls back to Half-Duplex mode (HD) when the opposite port is not in Auto-negotiate mode. The speed (10 Base-T or 100 Base-TX) in this mode is always configured correctly.</p> <p>0 = 10 Base-T half-duplex 1 = 10 Base-T full-duplex 2 = 100 Base-TX half-duplex 3 = 100 Base-TX full-duplex</p>	4	0 to 4

Table 11-2: Infrastructure Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	4 = Auto-negotiate		
ExtBootPReqEnable	Enables extended information to be sent in the BootP request. The device uses the vendor specific information in the BootP request to provide device-related, initial startup parameters such as board type, current IP address, software version, Geographical Address, etc. This is not available in DHCP.	0	0 or 1
ForceExceptionDump	Forces an exception dump that is sent every time the board restarts. 0 = Disable; 1 = Enable	0	0 or 1
HeartbeatDestIP	Sets the destination UDP port to which the heartbeat packets are sent. Range = IP address in dotted notation xxx.xxx.xxx.xxx	0.0.0.0	See Descr.
HeartbeatDestPort	Sets the destination UDP port to which the heartbeat packets are sent.	0	0 to 64000
HeartbeatIntervalmsec	Sets the time delay in msec between consecutive heartbeat packets. Range = 0x0 to 0xFFFFFFFF Default = 0xFFFFFFFF	See Descr.	See Descr.
HeartbeatSecondaryDestIP	Sets the secondary destination IP address to which the heartbeat packets are sent. Range = IP address in dotted notation xxx.xxx.xxx.xxx	0.0.0.0	See Descr.
ICMPUnreachableReportInterval	Determines: (a) The time the board ignores incoming ICMP unreachable packets from the channel activation time (b) The time it takes from the last ICMP unreachable packet until the board reports ICMP Reachable. Range = unsigned long	5000	See Descr.
INIFileVersion	Contains the ini file version number that is reported in the acEV_BOARD_STARTED event. Range = Long integer value.	0	See Descr.

Table 11-2: Infrastructure Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
RoutingTableDestinationMasks Column	Comprises the destination masks column of the static routing rules that users can add to. Range = Legal IP address.	NULL	See Descr.
RoutingTableDestinationsColumn	Comprises the Destination column of the static routing rules that users can add to. Range: Legal IP Address.	NULL	See Descr.
RoutingTableGatewaysColumn	Comprises the gateways column of the static routing rules that users can add. Range = Legal IP Address.	NULL	See Descr.
RoutingTableHopsCountColumn	Comprises the Hops count column of the static routing rules that users can add.	20	0 to 255
RoutingTableInterfacesColumn	Comprises the interfaces column of the static routing rules that users can add.	0	0 to 2
SerialData	Changes the serial data bit for the Simplified Message Desk Interface (SMDI). 7 = 7-bit; 8 = 8-bit	8	7 or 8
SerialFlowControl	Changes the serial flow control for the Simplified Message Desk Interface (SMDI). 0 = None; 1 = Hardware)	0	0 or 1
SerialParity	Changes the serial parity for the Simplified Message Desk Interface (SMDI). 0 = None 1 = Odd 2 = Even	0	0 to 2
SerialStop	Changes the serial stop for the Simplified Message Desk Interface (SMDI). 1 = 1-bit; 2 = 2-bit)	1	1 or 2
SMDI	Enables the Simplified Message Desk Interface (SMDI). SMDI defines a method whereby telephony systems can provide voice-messaging systems with data required by those telephony systems to process incoming calls	0	0 or 1

Table 11-2: Infrastructure Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	intelligently. Whenever the phone system routes a call, it sends an SMDI message through an EIA/TIA-232 connection to the voice-messaging system that tells it the line that it is using, the type of call that it is forwarding, and information about the source and destination of the call. SMDI is supported on a baud rate of 9600. 0 = Normal Serial; 1 = Serial SMDI		

11.1.3 Media Processing Parameters

The table below lists and describes the Media Processing parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 11-3: Media Processing Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
AnalogSignalTransportType	Determines the analog signal transport type. 0 = Ignore 1 = Transfer hookflash via RFC 2833	0	0 to 1
AnswerDetectorRedirection	Determines the AD (Answer Detector) Redirection. 0 (PCM) = Speech from the PCM side is detected 1 (Network) = Speech from the IP side is detected	0	0 or 1
AnswerDetectorSensitivity	Controls the the AD (Answer Detector) sensitivity. 0 = Most Sensitive; 2 = Least Sensitive	0	0 to 2
AnswerDetectorSilenceTime	Controls the silence time period (in 100 msec resolution) from no speech input until the END_OF_SPEECH event is sent. 10 = 1 second; Range = 0 to 0x3FF	10	See Descr.
BasicRTPPacketInterval	Selects the RTP packet rate for	0	0 to 3

Table 11-3: Media Processing Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	<p>sample-based coders (such as G.711, G.726, G.727). Also applicable for G.729, G.729E & G.728.</p> <p>0 = Default (set internally)</p> <p>1 = 5 msec</p> <p>2 = 10 msec</p> <p>3 = 20 msec</p>		
BellModemTransportType	<p>Use this parameter to set the Bell modem transport method.</p> <p>0 = Transparent</p> <p>2 = Bypass (enum ByPassEnable)</p> <p>3 = Transparent with Events (enum EventsOnly)</p>	0	0, 2, 3
BrokenConnectionEventActivationMode	<p>Determines when to enable detection of broken connections. See the VoPLib manual for more information.</p> <p>Default = 0 = Activate when the voice channel is opened for receiving</p> <p>1 = Activate when the first RTP packet is received</p>	0	0 or 1
BrokenConnectionEventTimeout	<p>Determines for how long the RTP connection should be broken before the Broken Connection event is issued. In units of 100 msec.</p> <p>Range = 3 to 21474836 in units of 100 msec (300 to 0x80000000 msec)</p> <p>Default = 3 (= 300 msec)</p>	See Descr.	See Descr.
CallerIDTransportType	<p>Defines the Caller ID transport type.</p> <p>Disable Caller ID (0): Caller ID detectors are not activated. The Caller ID signal flows in the regular RTP audio stream.</p> <p>Relay Caller ID (1): Presently the same as Mute.</p> <p>Mute Caller ID (2): CallerID signals detected and reported but muted from the RTP voice stream.</p>	3	0 to 3
CallerIDType	<p>Defines the supported Caller ID type.</p> <p>0 = Bellcore</p> <p>1 = ETSI</p>	0	0 to 19

Table 11-3: Media Processing Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	2 = NTT 4 = British 16 = ETSI_ETS 17 = Denmark 18 = Indian 19 = Brazilian		
CallProgressDetectorEnable	Enables or disables detection of Call Progress Tones. 0 = Disable; 1 = Enable	1	0 or 1
CNGDetectorMode	Determines the CNG Detector mode. 0 = Disable 1 = Relay 2 = Event Only	0	0 to 2
ConnectionEstablishmentNotificationMode	Determines the notification mode for the RTP connection establishment event acEV_CONNECTION_ESTABLISHED. 0 = Notify only after a broken connection event 1 = Also notify when the first RTP packet is received	0	0 or 1
DisableNAT	Enables or disables the NAT feature. 0 = Don't disable NAT; 1 = Disable NAT	1	0 or 1
DisableRTCPRandomize	Controls whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter defining RTCP Mean Tx Interval (in milliseconds). 0 = Randomize; 1 = Don't Randomize	0	0 or 1
DJBufMinDelay	Defines the Dynamic Jitter Buffer Minimum Delay (in msec).	150	0 to 150
DJBufOptFactor	Defines the Dynamic Jitter Buffer frame error/delay optimization.	7	0 to 12
DSPVersionTemplateNumber	Selects the DSP load number. Each load has a different coder list, a different channel capacity and different features supported.	0	0 to 255

Table 11-3: Media Processing Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
DTMFDetectorEnable	Enables or disables detection of DTMF. 0 = detection disabled; 1 = detection enabled.	1	0 or 1
DTMFTransportType	Defines the type of DTMF transport. 0 = Erase DTMFs from voice transport not relayed to remote 2 = DTMFs not erased are not relayed to remote 3 = DTMFs are muted from the voice stream and relayed according to RFC 2833	3	0 to 3
DTMFVolume	Defines and controls the DTMF generation volume [-dBm].	-11	-31 to 0
ECHybridLoss	Sets the worst case ratio between the signal level transmitted to the hybrid and the echo level returning from hybrid. Set this per worst hybrid in the system in terms of echo return loss. Refer to the enumeration acTECHybridLoss. 0 = 6 dBm 1 = 9 dBm 2 = 0 dBm 3 = 3 dBm	0	0 to 3
EnableAnswerDetector	Enables or disables activation of the AD (Answer Detector). 0 = Disable; 1 = Enable	0	0 or 1
EnableContinuityTones	Enables or disables Continuity Test tone detection and generation according to the ITU-T Q.724 recommendation. 0 = Disable; 1 = Enable	0	0 or 1
EnableEchoCanceller	Enables or disables the Echo Canceller. 0 = Disable; 1 = Enable	1	0 or 1
EnableFaxModemInbandNetworkDetection	Enables or disables inband network detection related to fax/modem.	0	0 to 1
EnablePatternDetector	Enables or disables activation of the PD (Pattern Detector).	0	0 or 1

Table 11-3: Media Processing Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	0 = Disable; 1 = Enable		
EnableRFC2658Interleaving	When enabled, RTP packets include an interleaving byte for VBR coders. 0 = Disable; 1 = Enable	0	0 or 1
EnableSilenceCompression	Enables or disables Silence Suppression Mode. 0 = Disable = SILENCE_COMPRESION_DISABLE 1 = Enable = SILENCE_COMPRESION_ENABLE 2 = Enable without adaptation = SILENCE_COMPRESION_ENABLE_NOISE_ADAPTATION_DISABLE	0	0 to 2
EnableStandardSIDPayloadType	When set to 1 (Enable), SID packets are sent with the RTP SID type (RFC 3389). 0 = Disable; 1 = Enable	0	0 or 1
FaxBypassPayloadType	Modifies the Fax Bypass Mode RTP packet's payload type. If congestion (if the selected payload type is already used for other coders/modes), then a TP_SETUP_PARAMETER_INVALID_ERROR is issued and the payload type is set to the default value (102). It is the user's responsibility to avoid congestion with other payload types.	102	0 to 127
FaxModemBypassDJBufMinDelay	Determines the Jitter Buffer constant delay (in milliseconds) during a Fax & Modem Bypass session. (The minimum Jitter Buffer Size).	40	0 to 150
FaxModemBypassBasicRTPPacketInterval	Sets the basic Fax / Modem Bypass RTP packet rate. 0 = Default (set internally) (PACKET_INTERVAL_DEFAULT) 1 = 5 msec (PACKET_INTERVAL_5_MSEC) 2 = 10 msec (PACKET_INTERVAL_10_MSEC) 3 = 20 msec (PACKET_INTERVAL_20_MSEC)	0	0 to 3

Table 11-3: Media Processing Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
FaxModemBypassCoderType	Sets the fax/modem bypass coder (according to acTCoders). 0 = G.711 A-Law	0	0 to 64
FaxModemBypassM	Defines the number of basic frames to generate one RTP fax/modem bypass packet.	1	1 or 2
FaxModemRelayVolume	Determines the fax gain control. The range -18 to -3 relates to -18.5 dBm to -3.5 dBm in steps of 1 dBm.	-12	-18 to -3
FaxRelayECMEnable	Enables or disables the using of ECM mode during Fax Relay. 0 = Disable; 1 = Enable	1	0 or 1
FaxRelayEnhancedRedundancyDepth	Number of repetitions to be applied to control packets when using the T.38 standard. 4 = Maximum redundancy	4	0 to 4
FaxRelayMaxRate	Limits the maximum rate at which fax messages are transmitted. 0 = 2400 bps 1 = 4800 bps 2 = 7200 bps 3 = 9600 bps 4 = 12000 bps 5 = 14400 bps	5	0 to 5
FaxRelayRedundancyDepth	Determines the depth of redundancy for fax packets. This parameter is applicable only to non-V.21 packets. 0 = No redundancy 1 = Include payload of previous packet 2 = Include payload of previous 2 packets	0	0 to 2
FaxTransportMode	Sets the Fax over IP transport method. 0 = Transparent 1 = Relay 2 = Bypass 3 = Transparent with Events	1	0 to 3
IBSDetectionRedirection	Determines the IBS (In-Band	0	0 or 1

Table 11-3: Media Processing Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	Signaling) Detection Direction. 0 = PCM; 1 = Network		
InputGain	Defines the PCM input gain. The range is -32 dB to +31 dB in 1 dB steps. Default = No Gain	0	-32 to +31
MaxDTMFDigitsInCIDString	Determines the maximum number of DTMF digits in a DTMF-based Caller ID string.	26	0 to 26
MaxEchoCancellerLength	Defines the maximum board EC (Echo Canceller) length capability. 0 = EC length determined internally to reach maximum channel capacity. 1 = 15 milliseconds 2 = 20 milliseconds 3 = 25 milliseconds 4 = 30 milliseconds 5 = 35 milliseconds 6 = 40 milliseconds	0	See Descr.
MFSS5DetectorEnable	Enables or disables detection of MF SS5 line signaling. 0 = Disable; 1 = Enable	0	0 or 1
MinDTMFDigitsInCIDString	Determines the minimum number of DTMF digits in a DTMF-based Caller ID string.	0	0 to 26
ModemBypassPayloadType	Modifies the Modem Bypass Mode RTP packet's payload type. If congestion (if the selected payload type is already used for other coders/modes), then a TP_SETUP_PARAMETER_INVALID_ERROR is issued and the payload type is set to the default value (103). It is the user's responsibility to avoid congestion with other payload types.	103	0 to 127
NSEMode	Enables or disables Cisco's NSE fax / modem automatic pass-through mode. 0 = Disable; 1 = Enable	0	0 or 1
NSEPayloadType	Users can use this parameter to	105	96 to 127

Table 11-3: Media Processing Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	modify the NSE packet's payload type.		
PDPattern	Defines the patterns that can be detected by the Pattern Detector.	-	0 to 0xFF
PDThreshold	Defines the number of consecutive patterns to trigger the pattern detection event.	5	0 to 31
PrerecordedTonesFileName	Defines the name (and path) of the file containing the Prerecorded Tones. Range = String of ASCII characters	-	See Descr.
RFC2198PayloadType	This parameter sets the RFC 2198 (RTP Redundancy) packet's parameter 'RTP Payload Type'.	104	96 to 127
RFC2833RxPayloadType	Controls the RFC 2833 Rx Relay RTP Payload type.	96	96 to 127
RFC2833TxPayloadType	Controls the RFC 2833 Tx Relay RTP Payload type.	96	96 to 127
RTPRedundancyDepth	Enables or disables generation of RFC 2198 redundancy packets. 0 = Disable; 1 = Enable	0	0 or 1
SITDetectorEnable	Enables or disables SIT (Special Information Tone) detection according to the ITU-T recommendation E.180/Q.35. 0 = Disable; 1 = Enable	0	0 or 1
TestMode	Defines the type of testing mode applied: 0 = Coder Loopback performs an encoder/decoder loopback inside the DSP device 1 = PCM Loopback loops back an incoming PCM to the outgoing PCM. 2 = ToneInjection generates a 1000 Hz tone to the outgoing PCM 3 = NoLoopback sets the channel to work in normal mode	3	0 to 3
UserDefinedToneDetectorEnable	Enables or disables detection of User Defined Tones signaling. 0 = Disable; 1 = Enable	0	0 or 1
V22ModemTransportType	Sets the V.22 modem transport method.	2	0 to 3

Table 11-3: Media Processing Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	0 = Transparent 2 = Bypass 3 = Transparent with Events		
V23ModemTransportType	Sets the V.23 modem transport method. 0 = Transparent 2 = Bypass 3 = Transparent with Events	2	0 to 3
V32ModemTransportType	Sets the V.32 modem transport method. 0 = Transparent 2 = Bypass 3 = Transparent with Events	2	0 to 3
V34ModemTransportType	Sets the V.34 modem transport method. 0 = Transparent 2 = Bypass 3 = Transparent with Events	2	0 to 3
VoicePayloadFormat	Sets the voice payload format. Choose either 0 = RTP or 1 = ATM (which enables working with vendors that use G.726 ATM Payload Format over RTP. Uses the enum acTVoicePayloadFormat. 0 = VoicePayloadFormatRTP 1 = VoicePayloadFormatATM 2 = VoicePAYloadFormatIllegal	0	0 to 2
VoicePromptsFileName	Defines the name (and path) of the file containing the Voice Prompts. Range = String of ASCII characters	-	See Descr.
VoiceVolume	Defines the voice output gain control. Range: -32 dB to +31 dB in 1 dB steps -32 = mute Default = 0 = No Gain	0	-32 to +31

11.1.4 Analog Parameters

The table below lists and describes the analog parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 11-4: Analog Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
AnalogCallerIDTimingMode	Defines the Analog CallerID Timing Mode. 0 = CallerID transferred between first and second rings 1 = CallerID transferred on valid Off ring	0	0 or 1
BellcoreCallerIDTypeOneSubStandard	Selects the sub-standard of the Bellcore Caller ID type. 0 = Between_Rings 1 = Not_Ring_Related	0	0 to 1
BellcoreVMWITypeOneStandard	Use this parameter to select the Bellcore VMWI standard. 0 = Between_Rings 1 = Not_Ring_Related	0	0 or 1
CallerIDGeneration	Defines the type of Caller ID. (FXS only) 0 = Bell 202; 1 = V23; 2 = DTMF	0	0 to 2
CallProgressTonesFilename	Defines Call Progress Tone filenames (downloaded by TFTP).	Null	
CurrentDisconnectDefaultThreshold	Sets the voltage threshold for the current disconnect detection. Set the voltage threshold by reading the line voltage. After setting the voltage threshold, compare its value to the CurrentDisconnectDefaultThreshold value. If the measured threshold is smaller than the ini file parameter's value, update the threshold to the same value configured for the ini file parameter (FXO only) .	4	0 to 20
CurrentDisconnectDuration	Defines the current-disconnect duration (in msec). This value is used in generation and detection.	900	200 to 1500
DisconnectToneType	Defines which CPT types are detected as far-end disconnect. CPT type is based on acTCallProgressToneType enum.	0	See Descr.

Table 11-4: Analog Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	Valid when FarEndDisconnectType allows CPT detection. Range = An array of up to 4 tone types		
DistinctiveRingFreq0	Defines Distinctive Ringing Frequency, in units of 10 msec (FXS only).	50	Any number
ETSICallerIDTypeOneSubStandard	Selects number denoting ETSI CallerID Type 1 sub-standard. (FXS only) Either: 0 = ETSI_Between_Rings 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	0	0 to 6
ETSIVMWITypeOneStandard	Selects the number denoting the ETSI VMWI Type 1 Standard. Choose: 0 = ETSI_VMWI_Between_Rings 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	0	0 to 6
FarEndDisconnectSilenceMethod	Defines the FarDisconnect silence detection method.	2	0 to 255

Table 11-4: Analog Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	0 = None 1 = Packets count 2 = Voice/Energy Detectors 255 = All		
FarEndDisconnectSilencePeriod	Defines the Silence period to be detected.	120	10 to 28800
FarEndDisconnectSilenceThreshold	Defines the threshold (in percentages) of the packets to be considered as Silence. This is only applicable if Silence is detected according to the packet count (where FarEndDisconnectSilenceMethod = 1).	8	1 to 100
FarEndDisconnectType	This parameter sets the source for the acEV_FAR_END_DISCONNECTED event (or for the relevant control protocol event). It is a bit-field parameter, hence (for example) if both CPT and current disconnect are required, the parameter should be set to 5. FarDisconnect contributor: 1 = CPT 2 = PolarityReversal 4 = CurrentDisconnect 8 = Silence	15	0 to 15
FlashHookPeriod	Defines the flashhook detection & generation period (in msec).	400	> 0
FXOLoopCharacteristicsFilename	Defines the FXO loop coefficient file name (FXO only).		-
FXSLoopCharacteristicsFilename	Defines the FXS loop coefficient file name (FXS only).		-
GroundKeyDetection	Enables/disables the analog ground key detection. (FXS only) 0 = Disable; 1= Enable	0	0 or 1
LifeLineType	Defines the LifeLine phone type. The LifeLine phone is available (for FXS only) on port 4 in MP-104 and MP-108, on port 2 in MP-102, on ports 1-4 in the MP-118, and on port 2 of each analog module in the Mediant 1000, (FXS only)	0	0 to 2

Table 11-4: Analog Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	<p>0 = activate LifeLine phone on power down</p> <p>1 = activate LifeLine phone on power down or on detection of LAN disconnect</p> <p>2 = activate LifeLine phone on power down, or on detection of LAN disconnect, or on loss of ping</p>		
MeasPersistence	Defines the time (in msec) that passes from the time of detection until the interrupt signal (FXO only).	0	0 to 255
MeteringType	<p>Sets the metering method for charging pulses. (FXS only)</p> <p>0 = 12 kHz sinusoidal bursts</p> <p>1 = 16 kHz sinusoidal bursts</p> <p>2 = Polarity Reversal pulses</p>	0	0 to 2
MinFlashHookTime	Sets the minimal time (in msec) for detection of a flash hook event (for FXS only). Flash hooks that last a shorter period of time are ignored. The detection is guaranteed for periods above 60 msec when setting the minimal time to 25.	300	25 to 300
MWIndicationType	<p>Defines the type of Message Waiting Indicator (MWI); (FXS only).</p> <p>0 = the MWI is generated according to Bellcore (FSK) and ETSI standards</p> <p>1 = a voltage of 100 VDC is applied to the line, lighting a lamp on the TE equipment</p>	0	0 or 1
PolarityReversalType	<p>Sets the type of the polarity reversal signal used for the network far-end answer and disconnect indications. Smooth reversal prevents negative effects as non-required ringing.</p> <p>0 = Soft; 1 = Hard (FXS only)</p>	0	0 or 1
RingDeglitch	Defines the time (in msec) to prevent detection of glitch/noise as a ring. (FXO only)	0	0 to 255
RingOffTime	Defines the Ring Off duration, between two On Rings (FXO only).	0	0 to 255
RingPersistence	Defines the time (in msec) from the	0	0 to 255

Table 11-4: Analog Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	ring detection to signaling the ring interrupt. (FXO only)		
TimeToSampleAnalogLineVoltage	Determines the time to sample the analog line voltage after offhook, for the current disconnect threshold (FXO only) .	1000	100 to 2500

11.1.5 Parameters Common to All Control Protocols

The table below lists and describes the parameters, contained in the *ini* file, that are common to all call control protocols. Use this table as a reference when modifying *ini* file parameter values.

Table 11-5: Common Control Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
CallAgentDomainName	Defines a domain name to be used to connect with the Call Agent. The parameter takes precedence over the Call Agent IP and the provisioned Call Agent parameters. Range = String[63]	NULL	See Descr.
CallWaitingToneDuration	Changes the call waiting tones family duration, in msec.	12000	300 to 30000
ControlDiffServ	Defines the value of the field 'DiffServ' in the IP header for control traffic.	0	0 to 63
CPPlayDigitalVMWI	Selects the method used for VMWI. 0 = Analog (high line voltage) 1 = Digital (play FSK signal as in caller ID)	0	0 or 1
CPTransportType	Defines the transport type for the control protocol: 0 = UDP; 1 = TCP	0	0 or 1
DefaultPacketizationPeriod	Defines the default packetization period (Frame Size). Default = 20 msec (for G.723 30)	20	5 to 80
DialToneDuration	Defines the timeout (in seconds) for the dial tone signal.	16	1 to 65535

Table 11-5: Common Control Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
DigitMapTimeoutTimer	Defines the timeout value (T symbol) in a digit map, in increments of 10. For MEGACO, it's the start timer. For the rest, it's the end timer.	16	1 to 65535
DTMFDigitLength	Defines the time to play DTMF, in msec.	100	0 to 65535
DTMFInterDigitInterval	Defines the time between DTMFs played, in msec.	100	0 to 65535
EnableCallerIDTypeTwo	Enables or disables Caller ID Type 2. If Off (0), Caller ID Type Two is not played (if playing is requested from the Call Agent). 0 = Off; 1 = On	1	0 or 1
EndpointName	MGCP: Gateway's endpoint name. This is a prefix used to identify the endpoint, i.e., 'ACgw' in the following example: 'ACgw5@acl.com'. MEGACO: Prefix of the endpoint part of the termination name Range: String[19] Default: MGCP: 'Acgw' MEGACO: 'line' for analog board and 'c' for trunking boards	See Descr.	See Descr.
GatewayName	Defines the media gateway's identification name. MGCP: Gateway's identification name towards the MGCP Call Agent. If undefined, the gateway name holds the IP address of the board. MEGACO: Prefix of the gateway part of the termination name. Range: String[63] Default: MGCP: AudioCodes.com MEGACO: NULL for analog boards and 'tgw' for trunking boards	See Descr.	See Descr.
IPDiffServ	Defines the value of the 'DiffServ' field in the IP header for media (RTP) traffic.	0	0 to 63
IPPrecedence	Sets the value of the IP precedence	0	0 to 7

Table 11-5: Common Control Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	field in the IP header for all packets generated from the channel.		
IPTOS	Sets the value of the parameter defining IP Type Of Service (TOS) in the IP header for all packets generated from this channel.	0	0 to 15
KeepAliveEnabled	This parameter can be used to enable a KeepAlive message (NOP ServiceChange). 0 = disable; >0 = enable	0	0 or >0
KeepAliveInterval	This parameter is used to define the interval in seconds of a KeepAlive message.	12	1 to 300
MGControlProtocolType	Defines the control protocol type. Choose either: 0 = None 1 = MGCP 2 = MEGACO 4 = H.323 8 = SIP	1	0 to 8
MGCPCommunicationLayerTimeout	This parameter defines the maximal time to wait for a response before declaring a disconnection (in seconds).	30	>0
MGCPCompatibilityProfile	Controls MGCP/MEGACO functioning for vendor-specific compatibility. Refer to the product's User's Manual. Range: Integer > 0 Refer to the product's User's Manual or the enumerator mgTMGCPProfile for possible values.	1	See Descr.
MGCPDefaultCoder	This parameter can be used to set a default coder for channel opening. For the legal coder names, refer to the product's User Manual. Default = cpDPT_G711Mulaw_Coder	G.711	See Descr.
MGCPDefaultPacketizationPeriod	Defines the default packetization period (Frame Size).	20	5 to 120
MGCPDTMFDetectionPoint	Defines if the detection of DTMF events is notified at the start or end of DTMF. 0 = at start of DTMF	1	0 or 1

Table 11-5: Common Control Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	1 = at the end of DTMF		
MGCPRetransmissionTimeout	Controls protocols retransmission timeout. Sets the initial time (in msec) for the first retransmission. The retransmission intervals thereafter increase exponentially.	200	0 to 10000
MGCPRetransmissionTimeout	Sets the initial time for the first retransmission. The Retransmission intervals thereafter increase exponentially.	200	0 to 65535
ProvisionedCallAgents	Use this parameter to define a list of up to 10 (MGCP) or 5 (MEGACO) legal IP addresses separated by ',' or ';' for the ServiceChange command. The gateway starts connecting with the first and in case of failure, attempts the others. Range: Legal IP Address	NULL	See Descr.
ProvisionedCallAgentsPorts	Use this parameter to define a list of up to 10 (MGCP) or 5 (MEGACO) Call Agent UDP ports separated by , or ; for each Call Agent defined by the parameter used to specify the Allowed Call Agent Address.	2944	0 to 65535
RandomizeTransactionID	Defines if the transactions produced by the board start with a fixed or random number. 1 = Randomize On Refer also to the parameters defining Transaction Id Range and Transaction ID Base.	1	0 or 1
RedundantCallAgentDomainName	Defines the redundant MGCP Call Agent domain name. Range = String[63] Default = '' (empty string)	See Descr.	See Descr.
RingOffPeriod	Defines the default ringing OFF period on analog lines.	3000	> 0
RingOffPeriod0	Defines the Distinctive Ringing #0 OFF period (in msec) on analog lines.	1000	> 0
RingOffPeriod1	Defines the Distinctive Ringing #1 OFF period (in msec) on analog lines.	500	> 0
RingOffPeriod2	Defines the Distinctive Ringing #2 OFF	3000	> 0

Table 11-5: Common Control Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	period (in msec) on analog lines.		
RingOffPeriod3	Defines the Distinctive Ringing #3 OFF period (in msec) on analog lines.	500	> 0
RingOffPeriod4	Defines the Distinctive Ringing #4 OFF period (in msec) on analog lines.	4000	> 0
RingOffPeriod5	Defines the Distinctive Ringing #5 OFF period (in msec) on analog lines.	1000	> 0
RingOffPeriod6	Defines the Distinctive Ringing #6 OFF period (in msec) on analog lines.	8000	> 0
RingOffPeriod7	Defines the Distinctive Ringing #7 OFF period (in msec) on analog lines.	8000	> 0
RingOnPeriod	Defines the default ringing ON period on analog lines.	1000	> 0
RingOnPeriod0	Defines the Distinctive Ringing #0 ON period (in msec) on analog lines.	1000	> 0
RingOnPeriod1	Defines the Distinctive Ringing #1 ON period (in msec) on analog lines.	3000	> 0
RingOnPeriod2	Defines the Distinctive Ringing #2 ON period (in msec) on analog lines.	500	> 0
RingOnPeriod3	Defines the Distinctive Ringing #3 ON period (in msec) on analog lines.	500	> 0
RingOnPeriod4	Defines the Distinctive Ringing #4 ON period (in msec) on analog lines.	4000	> 0
RingOnPeriod5	Defines the Distinctive Ringing #5 ON period (in msec) on analog lines.	8000	> 0
RingOnPeriod6	Defines the Distinctive Ringing #6 ON period (in msec) on analog lines.	1000	> 0
RingOnPeriod7	Defines the Distinctive Ringing #7 ON period (in msec) on analog lines.	8000	> 0
RTCPInterval	Defines the time interval between the adjacent RTCP reports, in msec.	5000	0 to 65535
SingleSIDPacketWithSCEG729	<p>When using a G.729 coder connection and SCE (Silence Suppression Enable) is On, a single SID packet is sent.</p> <p>If set to 1 and the channel was opened or modified to operate with the G.729 coder with Silence Suppression when Silence is detected, only a single SID packet is sent.</p> <p>If set to 0, SID packets are sent frequently, according to energy</p>	0	0 or 1

Table 11-5: Common Control Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	changes that require a SID packet for each change.		
TransactionIDBase	Defines the minimum number for the transaction ID.	2000	> 0
TransactionIDRange	Defines the range for the transaction ID. Default = 999999999	See Descr.	> 0
TransparentCoderPayloadType	Alternative payload type to use as transparent coder.	116	0 to 127
USETransparentCoderWithHBR	If this parameter is set to 1 and the connection uses HBR (High Bit Rate) coders, the DTMF transport type is set to Transparent. Coders list: G711Alaw_64, G711Mulaw, G726_16, G726_24, G726_32, G726_40, G727_16, G727_24_16, G727_24, G727_32_16, G727_32_24, G727_32, G727_40_16, G727_40_24, G727_40_32. 0 = Do not use; 1 = Use	0	0 or 1

11.1.6 MGCP-Specific Parameters

The table below lists and describes the MGCP-specific parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 11-6: MGCP Specific Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
CallAgentIP	The Call Agent IP address, in dotted notation, to be used for the initial Restart in Progress (RSIP) message. Set to 0.0.0.0 to avoid sending RSIP. This parameter overrides the BootP server's Call Agent IP address, if provided. Range = Legal IP address	NULL	See Descr.
CallAgentPort	Defines the Call Agent port number. Defaults to the MGCP default port	2427	0 to 65534

Table 11-6: MGCP Specific Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	number of 2427.		
ClearRequestBuffer	<p>If Off (0), only an empty R: clears the event list and only an empty S: clears and stops the current signals list.</p> <p>If On (1) and if an encapsulated identifier (X:) is present in the command, all TO signals and all events are cleared.</p>	1	0 or 1
ConnectionIDBase	Defines the lowest number for the Connection ID values assigned by the media gateway.	20	> 0
ConnectionIDRange	<p>Defines the range for the Connection ID values assigned by the gateway.</p> <p>Default = 999999999</p>	See Descr.	> 0
GatewayMGCPPort	Users can use this parameter to force the media gateway to listen to another UDP port instead of to the original 2427, as defined in RFC 2705.	2427	0 to 65535
LongDurationEventTime	Defines the default time to trigger the long duration event (in seconds).	3600	0 & > 0
MGCPActiveEndpoints	<p>Defines a list of active endpoints, separated by commas. Use a hyphen to define the range of endpoints. For example: '1 3 5-7' means that endpoints 1, 3, 5, 6 and 7 are active. Functions only with Endpoint Naming configuration. With Trunk Naming configuration, the results are unexpected.</p> <p>Default = All endpoints are active</p> <p>Range = String[19]</p>	See Descr.	See Descr.
MGCPEndPointNumberingOffset	Enables users to add an offset to endpoints. This parameter functions only with Endpoint Naming configuration. Using this parameter with Trunk Naming configuration is disallowed.	0	> 0
MGCPNamingPattern	<p>Defines the endpoint naming pattern which represents the naming method used by the gateway. Use of * represents a number or wild card.</p> <p>Default = MGCP 1.0</p> <p>Range = String[39]</p>	See Descr.	See Descr.

Table 11-6: MGCP Specific Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
MGCPPersistentEvents	Lists the events to be used as persistent events. Format is same as the requested event parameter (R:), for example, 'D/ x(N)'. Default: 'L/hd,L/hu,L/hf' Range = String [127]	See Descr.	See Descr.
MGCPSendMACWithRSIP	When this parameter exists in the ini file, the generated RSIPs include the media gateway's / board's MAC address in addition to the regular parameters. This parameter is sent as an MGCP extension parameter. 1 = Include the MAC address of the media gateway / board 0 = Don't include the MAC address of the media gateway / board	0	0 or 1
MGCPVersion	Defines the MGCP protocol version. Range = String[39] Default = MGCP 1.0	See Descr.	See Descr.
MGHistoryBufferTimeLim	Defines the time that a transaction is kept in the history buffer.	30	0 & > 0
QuarantineModeState	Sets the default quarantine handling state. When set, the quarantine handling state is set to LockStep. If not set, it is set to Loop and Discard. 0 = Loop/Discard; 1 = Lockstep	0	0 or 1
RedundantAgentIP	Defines the redundant Call Agent IP address to be used for the initial Restart in Progress message (RSIP). Set to 0.0.0.0 to avoid sending RSIP. Range = IP address in dotted format notation	NULL	See Descr.
RedundantAgentPort	Defines the redundant Call Agent port number. Defaults to the MGCP default port number of 2427.	2427	0 to 65534
RSIPOnNetworkDisconnection	Specifies whether or not to send an RSIP when the LAN is re-connected. Choose either: 0 = Don't send RSIP; 1 = Send RSIP	1	0 or 1
UseBRacketsWithGatewayName	When the Gateway Name is defined as an empty string and this parameter is set to 1, the gateway name takes the	1	0 or 1

Table 11-6: MGCP Specific Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
	board IP address with added brackets. i.e., [10.2.211.11]. 0 = Off; 1 = On		
UseNewFormatCoderNegotiation	Disables the response of all coders (and descriptions) that are returned on execution of the CRCX (Create Connection command) or MDCX (Modify Connection command) without a coder and SDP (Session Description Protocol) included in the command. For detailed information, refer to Coder Negotiation in RFC 3136. 0 = Do not use the new format 1 = Use the new format	1	0 or 1
UseWildcardWithRSIP	When the wildcard is used (1), RSIPs turn in a single message in an EndPoint Naming configuration and a single message for each trunk in a Trunk Naming configuration. If Off (0) and the number of channels is less than 64, an RSIP message is sent for each Endpoint. 0 = Do not use 1 = Use	1	0 or 1

11.1.7 SNMP Parameters

The table below lists and describes the SNMP parameters contained in the *ini* file. Use this table as a reference when modifying *ini* file parameter values.

Table 11-7: SNMP Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
DisableSNMP	Enables or disables SNMP. 0 = Enable; 1 = Disable		0 or 1
PM_EnableThresholdAlarms	Sends SNMP traps and Syslog messages when performance of the device is degraded (according to the configured thresholds).	0	0 or 1

Table 11-7: SNMP Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
SetCommunityString	User-determined community string with access limited to ini file entered values only. This parameter is the singular version of the readWriteCommunityStrings, and corresponds to readWriteCommunityStrings_0. Range = String[19]	NULL	See Descr.
SNMPManagerIP	Defines the IP address of the default SNMP manager, in dotted notation format: xxx.xxx.xxx.xxx. SNMP traps are sent to this manager. Range = string[15]	NULL	See Descr.
SNMPManagerIsUsed	Enables a row in the SNMP Managers table. 0 = row is disabled; 1 = row is enabled.	0	0 or 1
SNMPManagerTableIP	Used to define the SNMP manager server IP address. This is the tabular version of the parameter defining SNMP Manager IP. Range = String[15]	0	See Descr.
SNMPManagerTrapPort	Sets the trap ports to be used by the different managers. This parameter is the tabular version of the parameter defining SNMP Trap Port.	162	100 to 3999
SNMPManagerTrapSendingEnable	Enables the SNMP Manager's IP address for traps to be sent to it. When set to 1, traps are sent to this manager's IP address;. when set to 0, traps are not sent to it.	1	0 or 1
SNMPPort	This parameter specifies the port number for SNMP requests and responses. Generally, it isn't specified and the default is used.	161	100 to 3999
SNMPReadOnlyCommunityString	Used to define a read-only community string. Default = DEFAULT_READONLY_COMMUNITY_STRING Range = String[19]	See Descr.	See Descr.

Table 11-7: SNMP Parameters

<i>ini</i> File Field Name	Description	Host/Manual Default Value	Valid Range
SNMPReadWriteCommunityString	Used to define a read-write community string. Default = DEFAULT_READWRITE_COMMUNITY_STRING Range = String[19]	See Descr.	See Descr.
SNMPTrapCommunityString	Defines the community string used in traps. Default = DEFAULT_TRAP_COMMUNITY_STRING Range = String[19]	See Descr.	See Descr.
SNMPTrapManagerHostName	Defines the Host Name of the SNMP Trap Manager. Example: 'mngr.corp.mycompany.com'. String. 99 characters maximum.	NULL	
SNMPTrustedMGR	Defines the IP address of a trusted SNMP manager. Range = String[15]	0.0.0.0	See Descr.

12 Appendix C - RTP/RTCP Payload Types

Latest RTP Payload Types are defined in RFC 3551. For coders that should have dynamic Payload types, proprietary default values out of the dynamic Payload type range have been defined. These defaults are appropriate when working with AudioCodes products only. However, it is recommended to set a dynamic Payload type for them, which is usually done by higher applications during call setup. Be sure not to overload dynamic Payload types.



Note: Refer to the Release Notes for the supported coders.

12.1 Payload Types Defined in RFC 3551

Table 12-1: Payload Types Defined in RFC 3551

Payload Type	Description	Basic Packet Rate [msec]
0	G.711 μ -law	20
2	G.726-32	20
4	G.723 (6.3/5.3 kbps)	30
8	G.711 A-law	20
18	G.729	20
35	G.726-16	20
36	G.726-24	20
38	G.726-40	20
200	RTCP Sender Report	Randomly, approximately every 5 sec (when packets are sent by channel)
201	RTCP Receiver Report	Randomly, approximately every 5 sec (when channel is only receiving)
202	RTCP SDES packet	
203	RTCP BYE packet	
204	RTCP APP packet	

12.2 Payload Types Not Defined in RFC 3551

Table 12-2: Payload Types Not Defined in RFC 3551

Payload Type	Description	Basic Packet Rate [msec]
39	G.727 16 kbps	20
40	G.727 24-16 kbps	20
41	G.727 24 kbps	20
42	G.727 32-16 kbps	20
43	G.727 32-24 kbps	20
44	G.727-32 kbps	20
45	G.727 40-16 kbps	20
46	G.727 40-24 kbps	20
47	G.727 40-32 kbps	20
56	Transparent PCM	20
72	Vox ADPCM	20
90	Linear PCM	20

12.3 Default Dynamic Payload Types Which are Not Voice Coders

Table 12-3: Payload Types Not Defined in RFC 3551

Payload Type	Description
96	RFC 2833
102	Fax Bypass
103	Modem Bypass
104	RFC 2198
105	NSE

12.4 Default RTP/RTCP/T.38 Port Allocation

The following table shows the default RTP/RTCP/T.38 port allocation.

Table 12-4: Default RTP/RTCP/T.38 Port Allocation

Channel Number	RTP Port	RTCP Port	T.38 Port
1	4000	4001	4002
2	4010	4011	4012
3	4020	4021	4022
4	4030	4031	4032
5	4040	4041	4042
6	4050	4051	4052
7	4060	4061	4062
8	4070	4071	4072
9	4080	4081	4082
10	4090	4091	4092
11	4100	4101	4102
12	4110	4111	4112
13	4120	4121	4122
14	4130	4131	4132
15	4140	4141	4142
16	4150	4151	4152
17	4160	4161	4162
18	4170	4171	4172
19	4180	4181	4182
20	4190	4191	4192
21	4200	4201	4202
22	4210	4211	4112
23	4220	4221	4222
24	4230	4231	4232

Note the changed port allocation from earlier releases, for channel #5 and above.

Reader's Notes

13 Appendix D - DTMF, Fax and Modem Transport Modes

13.1 DTMF/MF Relay Settings

Users can control the way DTMF/MF digits are transported to the remote Endpoint, using the DTMFTransport/MFTransport configuration parameters. The following four modes are supported:

- DTMF/MFTransportType= 0 (MuteDTMF/MF) In this mode, DTMF/MF digits are erased from the audio stream and are not relayed to the remote side. Instead, silence is sent in the RTP stream.
- DTMF/MFTransportType= 2 (TransparentDTMF/MF) In this mode, DTMF/MF digits are left in the audio stream and the DTMF/MF relay is disabled.
- DTMF/MFTransportType= 3 (acRelayDTMFOverRTP/ acRFC2833RelayMF) In this mode, DTMF/MF digits are relayed to the remote side using the RFC 2833 Relay syntax.
- DTMFTransportType = 7 (acRFC2833RelayDecoderMute) In this mode, DTMF digits are relayed to the remote side using the RFC 2833 Relay syntax. RFC 2833 digit packets that are received from the remote side are muted on the audio stream.

13.2 Fax/Modem Settings

Users may choose from one of the following transport methods for Fax and for each modem type (V.22/V.23/Bell/V.32/V.34):

- fax relay - demodulation / remodulation
- bypass - using a high bit rate coder to pass the signal
- transparent - passing the signal in the current voice coder
- transparent with events - transparent + issues fax/modem events

When the fax relay mode is enabled, distinction between fax and modem is not immediately possible at the beginning of a session. Therefore, the channel is in **Answer Tone** mode until a distinction is determined. The packets being sent to the network at this stage are Fax relay T.38 packets.

13.3 Configuring Fax Relay Mode

When FaxTransportType= 1 (relay mode), upon detection of fax, the channel automatically switches from the current voice coder to answer tone mode, and then to Fax T.38 relay mode.

When Fax transmission has ended, the reverse switching from fax relay to voice is performed. This switching automatically mode occurs at both the local and remote Endpoints.

The fax rate can be limited by using the FaxRelayMaxRate parameter and the ECM Fax Mode can be enabled/disabled using the FaxRelayECMEnable parameter settings.

The (proprietary) redundancy mode that was specially designed to improve protection against packet loss through the EnhancedFaxRelayRedundancyDepth parameter. Although this is a proprietary redundancy scheme, it is compatible with other T.38 decoders. The depth of the redundancy (that is, the number of repetitions) is defined by the FaxRelayRedundancyDepth configuration parameter.



Note: T.38 mode currently supports only the T.38 UP syntax.

13.4 Configuring Fax/Modem Bypass Mode

When VxxTransportType= 2 (FaxModemBypass, Vxx can be one of the following: V32/V22/V21/Bell/V34/Fax), then on detection of Fax/Modem, the channel automatically switches from the current voice coder to a high bit-rate coder, as defined by the user in the FaxModemBypassCoderType configuration parameter.

If relay is enabled for one of the modes (Fax/Modem), the Answer Tone mode packets are relayed as Fax relay packets.

When the EnableFaxModemInbandNetworkDetection parameter is enabled under the conditions discussed above, 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

During the bypass period, the coder uses the packing factor (by which a number of basic coder frames are combined together in the outgoing WAN packet) set by the user in the FaxModemBypassM configuration parameter. The user can also configure the basic frame size by through the FaxModemBypassBasicRTPPacketInterval configuration parameter. The network packets generated and received during the bypass period are regular RTP voice packets (as per the selected bypass coder) but with a different RTP Payload type.

When Fax/Modem transmission ends, the reverse switching, from bypass coder to regular voice coder, is performed.



Note: When Fax relay is enabled, V21TransportType must be set to disable (Transparent) mode.

13.5 Configuring Fax/Modem Bypass NSE mode

Setting the NSEMode to 1 configures the answering Fax/Modem channel to send NSE packets to the calling Fax/Modem channel to switch to Bypass. Using the NSEPayloadType parameter, the user can control the NSE RTP packet's Payload type (default = 105). Note that the value of this parameter should be within the RTP Dynamic Payload Type range (96 to 127).

13.6 Supporting V.34 Faxes

Unlike the T.30 fax machines, the V.34 fax machines have no relay standard to transmit the data over IP to the remote side. Therefore AudioCodes provides the following operation modes for transporting the V.34 fax data over the IP.



Note: For all the setups described below, the CNG tone detector is disabled.

13.6.1 Using Bypass Mechanism for V.34 Fax Transmission:

Configuration:

- Fax transport mode - Relay/Bypass
- Vxx modem mode - Bypass

Expected events for V.34 Fax to V.34 Fax - Bypass Mode are shown in the table below.

Table 13-1: V.34 Fax to V.34 Fax - Bypass Mode

Calling	Answering
	EV_DETECT_MODEM (2100 AM + Reversal)
EV_DETECT_MODEM	
	EV_DETECT_FAX
EV_DETECT_FAX (Refer to Note 1 below)	
EV_END_FAX	EV_END_FAX



Note: The board changes its status to bypass mode upon receiving fax bypass packet from the remote side.

Note that if the fax transport type is set to relay, the fax relay benefits for the T.30 fax machines and, in parallel, are a variable when using a V.34 fax with its full rate. Therefore, AudioCodes recommends this setup. Also note that if CNG relay is used, in some cases, such as for manual answering machine, the fax may revert to T.30 fax with a speed of 14400 bps.

13.6.2 Using Events Only Mechanism for V.34 Fax Transmission

Use events only mode to transmit V.34 fax with its maximum capabilities:

Configuration:

3. Fax transport mode - Events only mode
4. Vxx modem mode - Events only mode

Expected events for V.34 Fax to V.34 Fax - Events Only Mode are shown in the table below.

Table 13-2: V.34 Fax to V.34 Fax - Events Only Mode

Calling	Answering
	EV_DETECT_ANSWER_TONE
	EV_DETECT_FAX

13.6.3 Using Relay Mode for Various Fax Machines (T.30 and V.34)

The user can force the V.34 fax machines to revert to T.30 and work at relay mode.

Configuration:

- Fax transport mode - Relay
- Vxx modem mode - Disable
- CNG detectors mode - Disable

In this mode, the fax events are identical to the regular T.30 fax session over T.38 protocol.

Expected events for V.34 Fax to V.34 Fax - Relay Mode are shown in the table below.

Table 13-3: V.34 Fax to V.34 Fax - Relay Mode

Calling	Answering
	EV_DETECT_ANSWER_TONE
	EV_DETECT_FAX
EV_DETECT_FAX	
EV_END_FAX	EV_END_FAX

14 Appendix E - Security

This appendix describes the MP-11x's implementation of security protocols.

The following list specifies the available security protocols and their purposes:

- **SSL/TLS** - Secures Web access (HTTPS) and Telnet access (applicable to MP-118 only)
- **RADIUS** - Is utilized by the Embedded Web Server and Telnet server for authentication.

14.1 SSL/TLS

SSL/TLS IS applicable to MP-118 only.

SSL (the Secure Socket Layer), also known as TLS (Transport Layer Security), is the method used to secure the MP-11x's Embedded Web Server and Telnet server. The SSL protocol provides confidentiality, integrity and authenticity of the Web server.

Specifications for the SSL/TLS implementation:

- Supported transports: SSL 2.0, SSL 3.0, TLS 1.0
- Supported ciphers: DES, RC4 compatible
- Authentication: X.509 certificates; CRLs are not supported

14.1.1 Web Server Configuration

For additional security, you can configure the Web server to accept only secure (HTTPS) connections. This is done by changing the *ini* file parameter, HTTPS Only or via the Embedded Web Server, Network Settings screen (refer to "Network Settings" on page 127). You can also change the port number used for the secure Web server (by default 443) by changing the *ini* file parameter, HTTPSPort.

14.1.2 Using the Secure Web Server

➤ **To use the secure Web server, take these 3 Steps:**

1. Navigate your browser to the following URL:

`https://[hostname] or [ip address]`

Depending on the browser's configuration, a security warning dialog may be displayed. The reason for the warning is that the MP-11x's initial certificate is not trusted by your PC. The browser may allow you to install the certificate, thus skipping the warning dialog the next time you connect to the MP-11x

2. If you are using Internet Explorer, click **View Certificate** and then **Install Certificate**.
3. The browser also warns you if the host name used in the URL is not identical to the one listed in the certificate. To overcome this, add the IP address and host name (ACL_nnnnnn where nnnnnn is the serial number of the MP-11x) to your

hosts file, located at /etc/hosts on UNIX or C:\WINDOWS\SYSTEM32\DRIVERS\ETC\hosts on Windows; then use the host name in the URL, e.g., https://ACL_280152 .Below is an example of a host file:

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
# Location: C:\WINDOWS\SYSTEM32\DRIVERS\ETC\hosts
#
127.0.0.1    localhost
10.31.4.47  ACL_280152
```

14.1.3 Secure Telnet

The MP-11x has an embedded Telnet server allowing easy command-line access to the device configuration and management interface. The Telnet server is disabled by default. To enable it, set the parameter, TELNETServerEnable to 1 (standard mode) or 2 (SSL mode).

No information is transmitted in the clear when using SSL mode.

If the Telnet server is set to SSL mode, a special Telnet client is required on your PC to connect to the Telnet interface over a secure connection; examples include C-Kermit for UNIX, Kermit-95 for Windows, and AudioCodes' acSSLTelnet utility for Windows (which requires prior installation of the free OpenSSL toolkit).

14.1.4 Server Certificate Replacement

The MP-11x is shipped with a working SSL configuration consisting of a unique self-signed server certificate. When a MP-11x is upgraded to firmware version 4.6, a unique self-signed server certificate is created. If an organizational PKI (public key infrastructure) is in place, you may wish to replace this certificate with one provided by your security administrator.

➤ To replace this certificate, take these 9 steps:

1. Your network administrator should allocate a unique DNS name for the MP-11x (e.g., dns_name.corp.customer.com). This name is used to access the device, and should therefore be listed in the server certificate.
2. Navigate your browser to the following URL (case-sensitive):

'https://dns_name.corp.customer.com/SSLCertificateSR'

https://dns_name.corp.customer.com/sslcertificatesr

Note that you should use the DNS name provided by your network administrator. The Certificate Signing Request Web page is displayed.

3. Enter the DNS name as the certificate subject (in the input box), and click **Generate CSR**. The Web page displays a textual certificate signing request, which contains the SSL device identifier
4. Copy this text and send it to your security provider. The security provider (also known as Certification Authority or CA) signs this request and send you a server certificate for the device.
5. Save the certificate in a file (e.g., cert.txt) and make sure it is a plain-text file with the "BEGIN CERTIFICATE" header. Below is an example of a Base64-Encoded X.509 Certificate.

```

-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJG
UjETMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBTZXXJ2
ZXVYMB4XDTE4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMC
RlIxIzEzARBgNVBAAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9zdGUxGzEz
dmVlcjCCASEwDQYJKoZIhvcNAQEBBQADggEoADCCAQkCggEAPqd4MziR4spWldGR
x8bQrhZkonWnNm+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qI
JcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lR
efiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwv
REXfFcUW+w==
-----END CERTIFICATE-----

```

6. Before continuing, set the parameter, HTTPSONly = 0 to make sure you have a method of accessing the device in case the new certificate is not working. Restore the previous setting after testing the configuration.
7. In the SSLCertificateSR Web page, locate the server certificate upload section.
8. Click **Browse** and locate the *cert.txt* file, then click **Send File**.
9. When the operation is complete, save the configuration and restart the device. The Web server now uses the provided certificate.



Note 1: The certificate replacement process may be repeated as necessary, e.g., when the new certificate expires.

Note 2: It is possible to set the subject name to the IP address of the device (e.g., "10.3.3.1") instead of a qualified DNS name. This practice is not recommended, since the IP address is subject to changes and may not uniquely identify the device.

14.1.5 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 in place, two-way authentication may be desired: both client and server should be authenticated using X.509 certificates. This is achieved by installing a client certificate on the management PC, and uploading the same certificate (in base64-encoded X.509 format) to the MP-11x'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 MP-11x must be configured to use NTP (Network Time Protocol) to obtain the current date and time. Without a correct date and time, client certificates cannot work.

➤ To install a client certificate, take these 5 steps:

1. Before continuing, set HTTPSONLY=0 to make sure you have a method of accessing the device in case the client certificate is not working. Restore the previous setting after testing the configuration.
2. To upload the Trusted Root Certificate file, go to the SSLCertificateSR Web page as above and locate the trusted root certificate upload section.

3. Click **Browse** and locate the file, then click **Send File**.
4. When the operation is complete, set the *ini* file parameter, `HTTPSRequireClientCertificates = 1`.
5. Save the configuration and restart the device.

When a user connects to the secure Web server:

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



Note : The process of installing a client certificate on your PC is beyond the scope of this document. For more information, refer to your Web browser or operating system documentation, and/or consult your security administrator.

14.2 RADIUS Support

To connect to the Embedded Web Server or Telnet server, the user must provide a valid name and password. While the device supports only a single system password, it is possible to enhance login security using a RADIUS server. RADIUS (RFC 2865) is a standard protocol for authentication, which defines a method for contacting a predefined server and verifying a given name and password pair against a remote database, in a secure manner.

14.2.1 Setting Up a RADIUS Server

A free RADIUS server implementation can be downloaded from' <http://www.freeradius.org>' <http://www.freeradius.org>. Follow the directions on that site for information on installing and configuring the server. If you use a RADIUS server from a different vendor, refer to the appropriate documentation.

➤ **To set up a RADIUS server, take these 4 steps:**

1. Define the MP-11x as an authorized client of the RADIUS server, with a predefined "shared secret" - a password used to secure communication. Below is an example of a clients.conf file (FreeRADIUS client configuration).

```
#
# clients.conf - client configuration directives
#
client 10.31.4.47 {
    secret          = FutureRADIUS
    shortname       = tp1610_master_tpm
}
```



2. Define the users authorized to use the MP-11x on the server, using one of the password authentication methods supported by the server implementation. The following example shows a user configuration file for FreeRADIUS using a plain-text password.

```
# users - local user configuration database
john  Auth-Type := Local, User-Password == "qwerty"
      Service-Type = Login-User
larry Auth-Type := Local, User-Password == "123456"
      Service-Type = Login-User
```

3. Make sure you have the IP address and port number used by the RADIUS server, and the configured "shared secret".
4. Go to "Configuring RADIUS Support" on page 241.

14.2.2 Configuring RADIUS Support

- **To configure RADIUS support on the MP-11x via the Embedded Web Server, take these 7 steps:**

1. In the Embedded Web Server, from the Advanced Configuration screen, select the **Network Settings** from the sub-menu bar on the top (Refer to "Network Settings" on page 127).
2. Locate the **RADIUS settings** section.
3. Fill in the RADIUS server IP address, port number and shared secret.
4. Set **Enable RADIUS access control** to **Enable**.
5. Set **Use RADIUS for Web/Telnet login** to **Enable**.
6. Set **Require secure Web connection (HTTPS)** to **Enable (HTTPS Only)**.

It is important that you use HTTPS (secure Web server) if connecting to the device over an open network, since the password must be transmitted in clear text over the network. Similarly, if using Telnet, make sure you use SSL mode (TELNETSERVERENABLE=2).

7. Save the configuration and restart the device. When you connect to the Web server or Telnet interface, use the name and password configured in the RADIUS database. The old system password is still active, and may be used if the RADIUS server is down.

- **To configure RADIUS support on the MP-11x using the ini file, take these 3 steps:**
1. Open the *ini* file in any text editor.
 2. Add the following lines to the *ini* file:
 - ENABLERADIUS = 1
 - WEBRADIUSLOGIN = 1
 - RADIUSAuthServerIP = IP address of RADIUS server
 - RADIUSAuthPort = port number of RADIUS server, usually 1812
 - SHAREDSECRET = 'your shared secret'
 - HTTPSONLY = 1
 3. Save the configuration and restart the device. When you connect to the Telnet interface, use the name and password configured in the RADIUS database. The old system password is still active, and may be used if the RADIUS server is down.

14.3 Network Port Usage

The following table lists the default TCP/UDP network port numbers used by the MP-11x. Where relevant, the table lists the *ini* file parameters that control the port usage and provide source IP address filtering capabilities.

Table 14-1: Default TCP/UDP Network Port Numbers

Port number	Peer port	Application	Notes
2	2	Debugging interface	Always ignored
4	4	EtherDiscover	Open only on unconfigured devices
23	-	Telnet	Disabled by default (TELNETSERVERENABLE). Configurable (TELNETSERVERPORT), access controlled by TELNETSERVERAUTHORIZEDADDRESS
68	67	DHCP	Active only if DHCPENABLE=1
80	-	Web server (HTTP)	Configurable (HTTPPORT), may be disabled (DISABLEWEBTASK or HTTPSONLY). Access controlled by WEBACCESSLIST
161	-	SNMP GET/SET	Configurable (SNMPPORT), may be disabled (DISABLESNMP). Access controlled by SNMPTRUSTEDMGR
443	-	Web server (HTTPS)	Configurable (HTTPSSPORT), may be disabled (DISABLEWEBTASK). Access controlled by WEBACCESSLIST

Table 14-1: Default TCP/UDP Network Port Numbers

Port number	Peer port	Application	Notes
500	-	IPSec IKE	May be disabled (ENABLEIPSEC)
2422	2422	TPM LinkLayer	Used for internal synchronization between the two TPMs on a board (Applicable to 1610 and 2810 boards only)
2423-2424	2423 and up	TPNCP	Proprietary control protocol. Access controlled by ENABLETPNCPSECURITY and AUTHORIZEDTPNCPSERVERS
2427	2427	MGCP / Megaco	Configurable (GATEWAYMGCPPORT), Access controlled by PROVISIONEDCALLAGENTS and MEGACOCHECKLEGALITYOFMGC
4000, 4010 and up	-	RTP traffic	Base port number configurable (BASEUDPPORT), fixed increments of 10. The number of ports used depends on the channel capacity of the device.
4001, 4011 and up	-	RTCP traffic	Always adjacent to the RTP port number
4002, 4012 and up	-	T.38 traffic	Always adjacent to the RTCP port number
32767	-	SCTP	If SCTP/IUA is available on the device
(random) > 32767	514	Syslog	May be disabled (ENABLESYSLOG).
(random) > 32767	-	Syslog ICMP	May be disabled (ENABLESYSLOG).
(random) > 32767	-	ARP listener	
(random) > 32767	162	SNMP Traps	May be disabled (DISABLESNMP)
(random) > 32767	-	DNS client	

14.4 Recommended Practices

To improve network security, the following guidelines are recommended when configuring the MP-11x:

- Set the management password to a unique, hard-to-guess string. Do not use the same password for several devices, as a compromise of one may lead to the compromise of others. Keep this password safe at all times, and change it frequently.
- If possible, use a RADIUS server for authentication. RADIUS allows you to set different passwords for different users of the MP-11x, with centralized management of the password database. Both Web and Telnet interfaces support RADIUS authentication.

- Use IPSec to secure traffic to all management and control hosts. Since IPSec encrypts all traffic, hackers cannot capture sensitive data transmitted on the network, and malicious intrusions are severely limited.
- Use HTTPS when accessing the Web interface. Set HTTPSONLY=1 to allow only HTTPS traffic (and block port 80). If you don't need the Web interface, disable the Web server.
- If you use Telnet, do not use the default port (23). Use SSL mode to protect Telnet traffic from network sniffing.
- If you use SNMP, do not leave the community strings at their default values, as they can be easily discovered by hackers. See the SNMP configuration chapter for further details.
- Use a firewall to protect your VoIP network from external attacks. Robustness of the network may be compromised if the network is exposed to "denial of service" (DoS) attacks; such attacks are mitigated by stateful firewalls. Do not allow unauthorized traffic to reach the MP-11x.

14.5 Legal Notice

By default, the MP-11x supports export-grade (40-bit and 56-bit) encryption, due to U.S. government restrictions on the export of security technologies. To enable 128-bit and 256-bit encryption on your device, contact your AudioCodes representative.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/> <http://www.openssl.org/>)

This product includes cryptographic software written by Eric Young' (eay@cryptsoft.co'm mail to: eay@cryptsoft.com).

15 Appendix F - Utilities

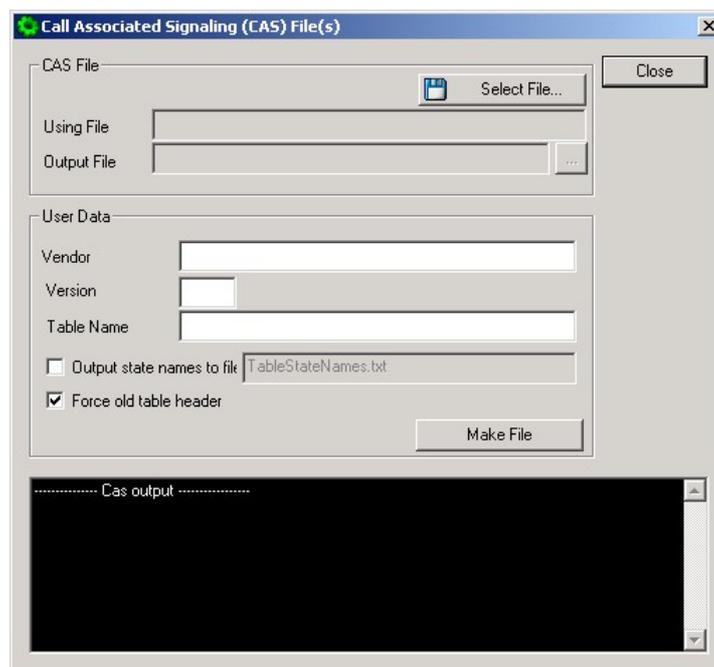
This section describes the functionality and operation of a list of utilities supplied with the TrunkPack software package:

15.1 TrunkPack Downloadable Conversion Utility

LOCATION:

```
.\Utilities\ Downloadables Construction  
Utility\DConvert240.exe
```

Figure 15-1: Downloadable Conversion Utility Opening Screen



This utility is used to generate the following:

- Call Progress Tones configuration files
- Voice Prompts files
- CAS protocol configuration files (Even though this utility is listed in the main menu, it is NOT applicable to IPmedia 2000, IPmedia 3000, MP products, TPM-1100)
- VXML files (Even though this utility is listed in the main menu, it is applicable to IPmedia 2000 and IPmedia 3000 only)
- Prerecorded Tones files

- Encoded *ini* files The above files can be used when:
- Using an ini file during BootP/DHCP session
- Using the Web Interface.

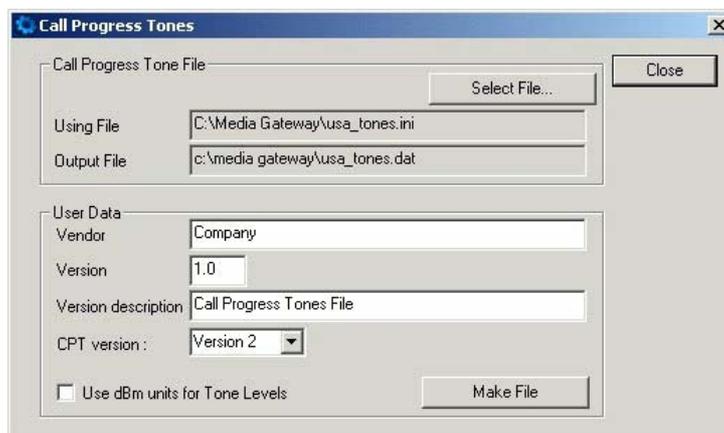
Some files may have usage restrictions as described under their usage information.

15.1.1 Converting a CPT ini File to a Binary dat File

➤ To convert a CPT ini file to a binary dat file, take these 8 steps:

1. Create a CPT *ini* file using the direction in "Modifying the Call Progress Tones File & Distinctive Ringing File" on page 72 or by editing a CPT *ini* file provided by AudioCodes.
2. Execute *DConvert240.exe* and click the **Process Call Progress Tones file(s)** button. The Call Progress Tones dialog appears.

Figure 15-2: Call Progress Tones Screen



3. Click the **Select File . . .** button and navigate to the location of the CPT *ini* file that you want to convert.
4. Select the desired file and click **Open**. The name and path of both the CPT *ini* file and the *dat* file appear in the **Using File** field and **Output File** field respectively. (The file names and paths are identical except for the file extension.)
5. Fill in the **Vendor**, **Version** and **Version Description** fields.
 - **Vendor** field - 256 characters maximum
 - **Version** field - must be made up an integer, followed by a period ".", then followed by another integer (e.g., 1.2, 23.4, 5.22)
 - **Description** field - 256 characters maximum
6. The default value of the CPT version drop-down list is **Version 3**. Do one of the following:
 - If the software version release you are using is 4.4, in the **CPT Version** drop-down list, select **Version 2**.
 - If the software device version release is prior to version 4.4, in the **CPT Version** drop-down list, select **Version 1** (to maintain backward compatibility).

- The **Use dBm units for tone levels** checkbox is not checked as the default. To use -dBm units for setting the Call Progress Tone and User Defined Tone Levels, click a checkmark into the **Use dBm units for tone levels** checkbox. This checkbox should be checked to maintain backward compatibility.



Note: The default value of the **dBm units for tone levels** checkbox is left unchecked for backward compatibility with versions prior to version 4.4.

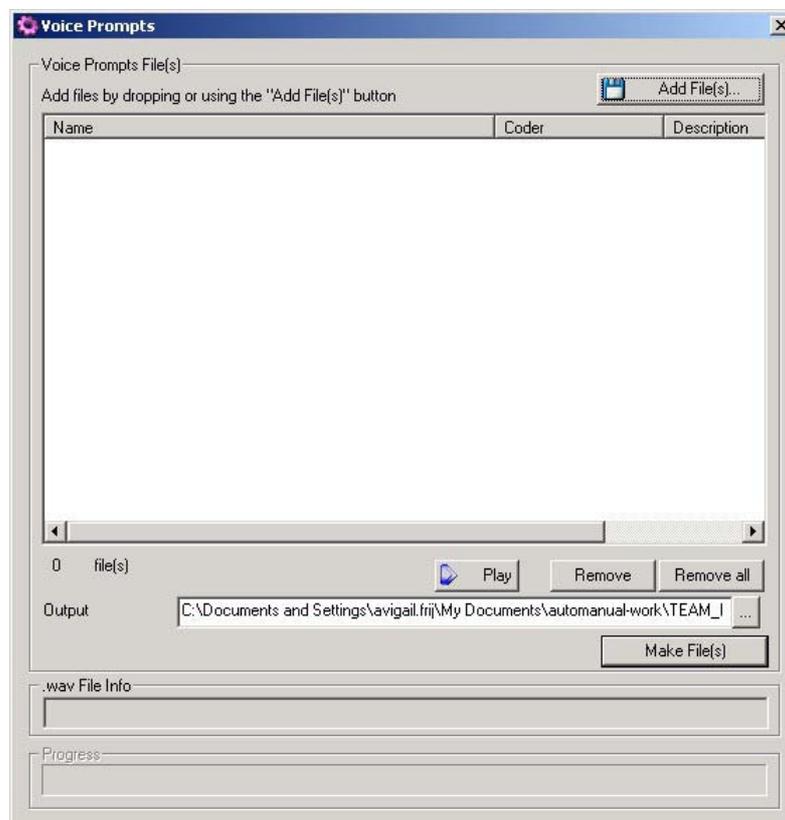
- Click the **Make File** button. The *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

15.1.2 Generating Voice Prompts Files

➤ To generate a Voice Prompts file, take these 12 steps:

- Create raw Voice Prompt files according to the instructions in the section on “Relaying DTMF/MF Digits” in AudioCodes’ “VoPLib User’s Manual”, Document #: LTRT-844xx). From version 4.2, **DConvert** supports *wav* files as well.
- Execute *DConvert240.exe* and click the **Process Voice Prompts file(s)** button. The Voice Prompts window appears.

Figure 15-3: Voice Prompts Screen

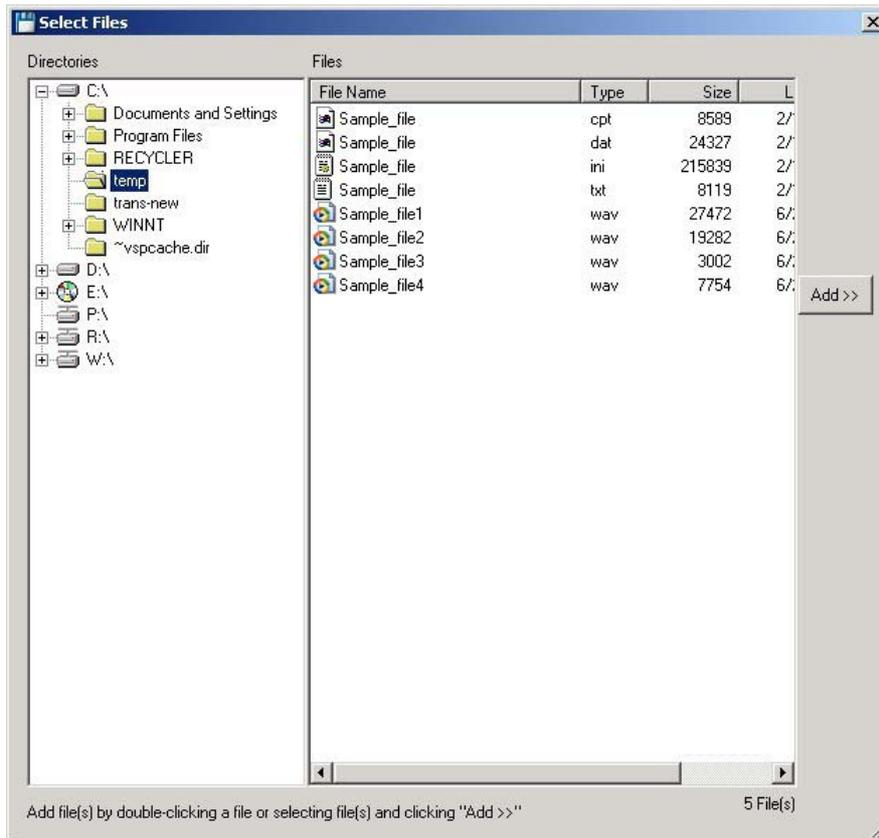


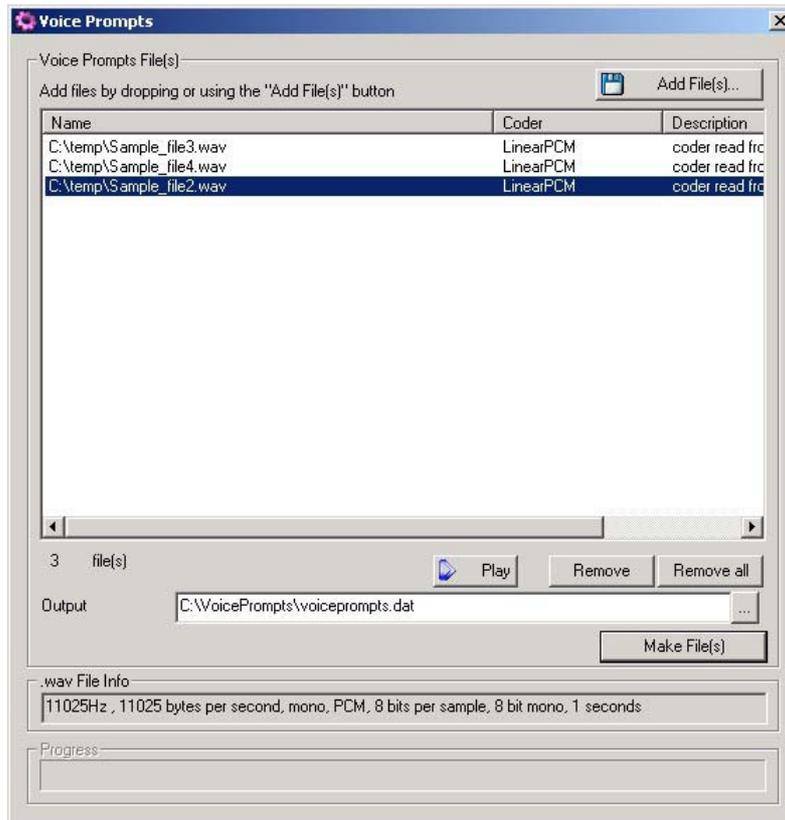
3. Select the raw Voice Prompt files (created in Step 1) step either by one of these actions:
 - a. Click the **Add Files** button in the upper right corner. The Add Files window appears. (Refer to the figure, "Select Files Window" below.)

Navigate to the appropriate file.

Select it and click the **Add>>** button. To close the Add Files window, click the  Exit button. (Press the **Esc** key to cancel changes.)

Figure 15-4: Select Files Window





- b. From any location on the PC, select the appropriate files and drag-drop them into the Voice Prompts window.
4. Arrange the files as desired by dragging and dropping them from one location in the list to another location.



Note: The sequence of files in the “Add Files...” window defines the Voice Prompt ID.

5. Use the **Play** button to preview the sound of the wav file. Use the **Remove** and **Remove all** buttons to remove files in the list as needed.
6. Select a coder for each file by first selecting the file (or files) and then double-clicking or right-clicking on it. The File Data window appears.

Figure 15-5: File Data Window



7. From the **Coder** drop-down list, select a coder type (to be used by the `acPlayVoicePrompt()` function).
8. In the **Description** field, enter a description (optional).



Note: For *wav* files, a coder is automatically selected from the *wav* file header.

9. Close the File Data dialog by clicking on the  Exit button. (Press the **Esc** key to cancel changes.). You are returned to the Voice Prompts window.
10. The default **Output** file name is *voiceprompts.dat*. You can modify it. Or, Use the  Browse button to select a different Output file. Navigate to the desired file and select it. The selected file name and its path appear in the **Output** field.
11. Click the **Make File(s)** button to generate the Voice Prompts file. The Progress bar at the bottom of the window is activated. The *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.
12. The generated file can be used only for downloading using the *ini* file facility or using `acOpenRemoteBoard()` in full configuration operation mode. When using the `acAddVoicePrompt()`, use the single raw voice prompt files.

15.1.3 Generating CAS Protocol Configuration Files

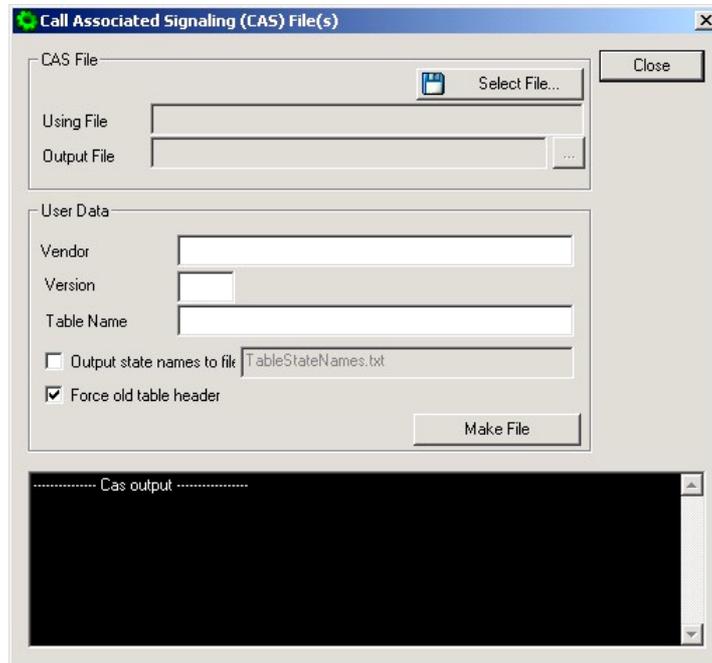


Note: The CAS utility is not applicable to MP-1xx products and TPM-1100.

- **To produce a CAS Protocol configuration file, take these 10 steps:**
1. Construct the CAS protocol *xxx.txt* and *xxx.h* files according to the instructions in the sections on “Caller ID Support” and “CAS Protocol Table” in AudioCodes’ “VoPLib User’s Manual”, Document #: LTRT-844xx.
 2. Copy the files generated in the previous step (or at least the *xxx.h* file) to the same directory in which *DConvert240.exe* is located and make sure that the two following files, *CASSetup.h* and *CPP.exe*, are also located in this same directory.

- Execute *DConvert240.exe* and click the **Process CAS Tables** button. The Call Associated Signaling (CAS) Window appears.

Figure 15-6: Call Associated Signaling (CAS) Screen



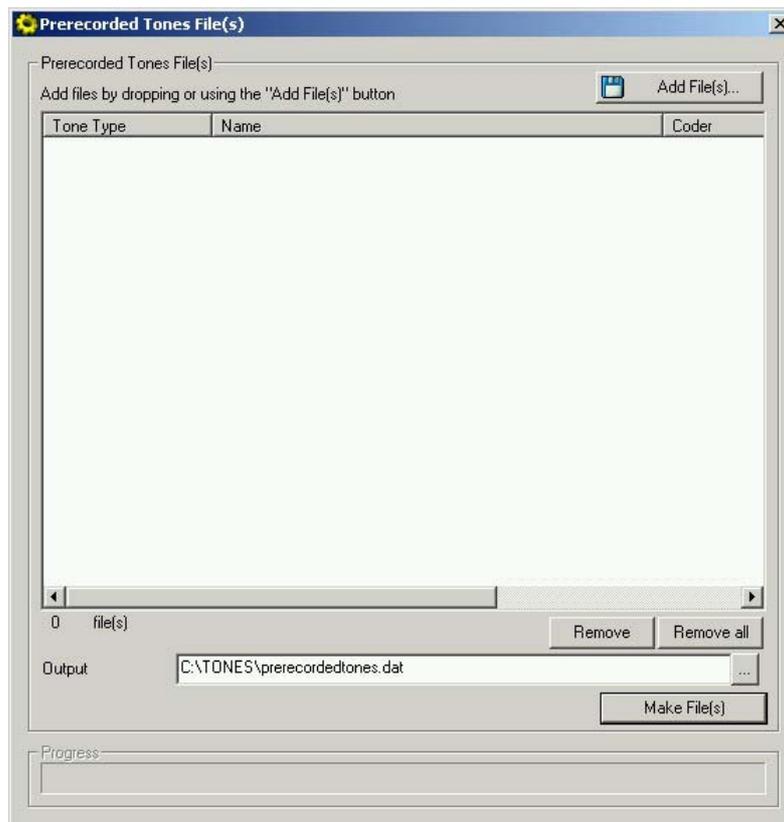
- Click the **Select File** button. A Browse window appears.
- Navigate to the desired location and select the file to be converted. (This automatically designates the output file as the same name and path, but with the *dat* extension. The Table Name is also automatically designated.)
- Fill in the **Vendor** and **Version** fields.
 - Vendor** Field - 32 characters maximum
 - Version** Field - must be made up an integer, followed by a period ".", then followed by another integer (e.g., 1.2, 23.4, 5.22)
- Modify the **Table Name** if desired.
- For troubleshooting purposes, you can click a check into the **Output state names to file** checkbox. This activates the file name field in which the default file name, **TableState Names.txt** appears. You can modify the file name if desired. The file is located in the same directory as the **Using file** and **Output file** designated above.
- If the file to be converted uses the **new table header**, un-check the **Force old table header** checkbox.
- Click the **Make File** button. The *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

On the bottom of the Call Assisted Signaling (CAS) Files(s) window, the Cas output log box displays the log generated by the process. It can be copied as needed. The information in it is **NOT** retained after the window is closed.

15.1.4 Generating Prerecorded Tones Files

- To generate a Prerecorded Tones file, take these 11 steps:
1. Prior to the conversion process, the user should prepare the appropriate prerecorded tones file(s).
 2. Execute *DConvert240.exe* and press the **Process Prerecorded Tones file(s)** button. The Prerecorded Tones file(s) window appears.

Figure 15-7: Prerecorded Tones File(s) Screen



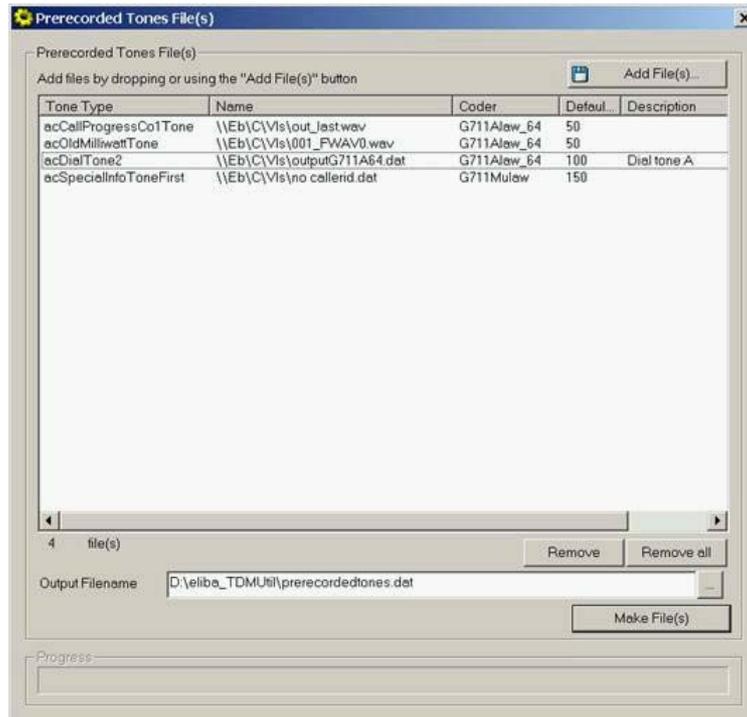
3. Select the raw Prerecorded Tones files (created in Step 1) utilizing one of these actions:

4. Click the **Add Files** button in the upper right corner. The Add Files window appears. (Refer to the figure, Select Files Window.)

Navigate to the appropriate file.

Select it and click the **Add>>** button. (To close the Add Files window, click the  Exit button. Press the **Esc** key to cancel changes.) You are returned to the Prerecorded Tones file(s) window.

Figure 15-8: Prerecorded Tones File(s) Screen with wav Files



- c. From any location on the PC, select the appropriate files and drag-drop them into the Voice Prompts window.
5. To define a tone type, coder and default duration for each file, select the file (or group of files to be set the same) and double click or right click on it. The File Data window appears.

Figure 15-9: File Data Dialog Box



6. From the **Type** drop-down list, select a Ring parameter type.
7. From the **Coder** drop-down list, select a coder type (G.711 A-law_64, G.711 μ -law, or Linear PCM).
8. In the **Description** field, enter a description (optional).
9. In the **Default** field, enter the duration in msec.

10. Click the  Exit button. (Press the **Esc** key to cancel changes.) You are returned to the Prerecorded Tones file(s) window.
11. The default **Output** file name is *prerecordedtones.dat*. You can modify it. Or, Use the  Browse button to select a different Output file. Navigate to the desired file and select it. The selected file name and its path appear in the **Output** field.
12. Click **Make File(s)** button. The Progress bar at the bottom of the window is activated. The *dat* file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

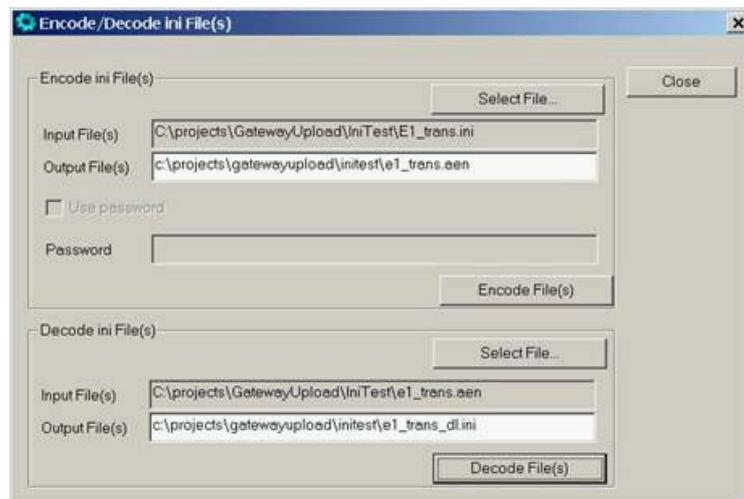
The *ini* file can be both encoded and decoded using **DConvert**. Encoding usually takes place before downloading an *ini* file to the board while decoding usually takes place after uploading an *ini* file from the board.

➤ **To Encode an *ini* file, take these 4 steps:**

1. Prior to the encoding process, the user should prepare the appropriate *ini* file either by uploading from the board or by constructing one (refer to "Initialization (ini) Files" on page 51).

Execute *DConvert240.exe* and click the **Process Encoded *ini* file(s)** button. The Encoded *ini* file(s) window appears.

Figure 15-10: Encoded ini File(s) Screen



2. In the **Encode Ini File(s)** area, click the **Select File...** Button. A Browse window appears.
3. Navigate to the desired location and select the *ini* file to be encoded. (This automatically designates the output file as the same name and path, but with the *aen* extension.



Note: The Password field is to be implemented in a future version.

4. Click the **Encode File(s)** button. The encoded file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.

The encoded *ini* file can be loaded using the regular *ini* file procedure. To upload a file from a device, use the Web Interface (refer to "Software Update" on page 155).

➤ **To Decode an *ini* file follow these 4 steps:**

1. Prior to the decoding process the user should prepare the appropriate encoded *ini* file either by uploading from the board or by using the encoding process on an exiting *ini* file.
2. Execute *DConvert240.exe* and click the **Process Encoded *ini* file(s)** button.
3. In the **Decode Ini File(s)** area, click **Select File(s)** and select the *aen* file to be decoded. (This automatically designates the output file as the same name and path, but with the extension, *_dl.ini*.)
4. Click the **Decode File(s)** button. The decoded file is generated and placed in the same directory as shown in the **Output File** field. A message box informing you that the operation was successful indicates that the process is completed.



Note: The decoding process verifies the input file for validity. Any change made to the encoded file causes an error and the decoding process is aborted.

15.2 MGCP Tester Utility

LOCATION:

```
.\Utilities\MGCPTester
```

DESCRIPTION:

This utility serves as a simulation for the MGCP Call Agent. It can send any MGCP command, as well as run complicated scripts. This utility can be used to exercise the MGCP clients embedded in TrunkPack series boards and modules.

OPERATION:

The MGCP tester demo application operation is self-explanatory.

Reader's Notes

16 Appendix G - MGCP Compliance

The MGCP Compliance Matrix Table below summarizes the supported MGCP features respectively. The Reference column in the table refers to IETF RFC 3435 from January 2003 (which replaced RFC 2705).

16.1 MGCP Compliance Matrix

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
6.	Case Sensitivity			Page 62
7.	Command Verb	Yes		
8.	Parameters	Yes		
9.	EndPoint identifier			2.1.2 Page 15
10.	"" Wild-carding	Yes		
11.	"\$" Wild-carding	Yes		
12.	Domain name for Call Agent	No	IP address is used to identify Call Agent	Pages 23, 96
13.	Digit Maps	Yes	12 Digit Maps Such as: R: [0 -9](D) R: D/X(D) D: xxxx 88# 7xx xxxT 5x.T	2.1.5 Page 24
14.	Timer indication - T	Yes	Interdigit timer Fixed Timer of 4 sec is used	6.1.2 Pages 27, 112
15.	Digits and Letters			Page 27
16.	#	Yes		
17.	X	Yes		
18.	X.	Yes	X. - Arbitrary number of X Occurrences	Page 26
19.	*	Yes		
20.	[1-7]	Yes	For digit maps	Page 25
21.	A,B,C,D	Yes		

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
22.	Event names	Yes		Pages 26, 2.1.6 page 37, 3.2.2.7 page 73
23.	Wildcard notations (X, \$, *,all)	Yes		Page 27
24.	Optional connection ID (G/rt@A3F58)	No		Page 28
25.	Signals on/off			Page 29
26.	On/Off (OO)	Yes		
27.	Time out (TO)	Yes		
28.	Brief (BR)	Yes		
29.	Using "+", "-" to turn on/off the "OO" Signal	Yes	for DTMF digits	
30.	Connection modes			Pages 31, 3.2.2.6 page 73
31.	Inactive	Yes		Page 31
32.	Send only	Yes		Pages 21,31
33.	Receive only	Yes		Page 31
34.	Send/receive	Yes		
35.	Conference	Yes		
36.	Data	No	3 participants only	
37.	Loopback	Yes		
38.	Continuity test	Yes		
39.	Network loop back	No		
40.	Network continuity (netwtest)	No		
41.	Endpoint Configuration command	No		2.3.1 page 32, 44
42.	Notification Request command			2.3.2 page 33
43.	Endpoint ID	Yes		2.1.2 page 15
44.	Notified Entity	Yes		Pages 24, 38

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
45.	RequestedEvents (with associate actions)	Yes	If not specified, notifications is send to command originator	Pages 34, 3.2.2.8 74
46.	RequestIdentifier	Yes		2.3.2 page 33
47.	DigitMap	Yes	Limited to 8 digits	2.1.5 page 24
48.	Defined explicitly or through a previous command	Yes		Page 35
49.	SignalRequests	Yes		3.2.2.9 page 76
50.	Quarantine Handling			36, 3.2.2.12 page 77
51.	Discard	No		
52.	Process loop	No	Events are always processed	
53.	Process	Yes	Events are always processed	
54.	Loop	No		
55.	Process step by step			
56.	Requested events	Yes	Empty buffer	
57.	Digit map	Yes	Empty buffer	
58.	DetectEvents	Yes	Empty buffer	37, 3.2.2.13 page 77
59.	Encapsulated Endpoint Configuration	Yes		37
60.	Event associated actions			Pages 34, 76
61.	Notify event immediately with all accumulated events	Yes		35
62.	Swap audio	No		34
63.	Accumulate event in buffer, but do not notify yet	Yes		

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
64.	Accumulate according to digit map	Yes		33
65.	Keep signal active	No		34
66.	Process Embedded Notification Request	Yes		Pages 34, 36, 75
67.	Ignore the event	Yes		34
68.	Supporting two or more actions, hf(S,N)	Yes	Combining actions	Pages 35, 75
69.	Persisted events	Yes	Notify off-hook / on-hook	Page 34, 53
70.	Number of active connection on an endpoint	1 or 2		
71.	Synchronization of Signalrequest action with detected event	Yes	TO (Timeout) signals stop when one of the requested events is detected Example 1: Ringing stops if off-hook event was detected Example 2: Dial tone stops if DTMF was detected	Page 36
72.	Notification request with empty signal list for stopping tone generation	Yes		Page 36
73.	Detection of events on Connections	No		Page 37
74.	Notifications			Page 37
75.	EndpointID	Yes		
76.	NotifiedEntity	Yes		
77.	RequestIdentifier	Yes		
78.	ObservedEvents	Yes		3.2.2.10 page 73, 37, 52, 65
79.	Create Connection command			3.2.2.2 Page 87
80.	CallID	Yes		Page 39
81.	Endpoint	Yes		Page 39

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
82.	NotifiedEntity	Yes		Page 39
83.	Multiple connections per endpoint	Yes	- Only two connections - Only one of them can be in send/send receive mode	Page 39
84.	LocalConnection Options			Pages 39, 40
85.	Encoding method	Yes	One value List of values not supported	Page 41
86.	Packetization period	Yes	SDP "ptime" parameter Supports only 20 msec	Pages 40, 41
87.	Bandwidth	No	Single value or range	Page 40
88.	Type of Service (TOS)	Yes	2 Hex digits	
89.	Echo cancelation	Yes		
90.	Silence suppression	Yes	-32 to +31 value	
91.	Gain control	Yes	32..31 value	Page 41
92.	Reservation service	No		Page 38
93.	RTP security	No	Providing Key as per RFC 2327	Page 39
94.	Type of network (IN, Local, ATM)	Yes		
95.	Vendor specific extensions	No		Page 40
96.	Mode	Yes		Pages 41, 42
97.	RemoteConnection Descriptor	Yes		Page 42
98.	SecondEndpointID	Yes		Page 42
99.	Encapsulated Notification Request			Page 77
100.	R:	Yes		
101.	S:	Yes		
102.	Encapsulated Endpoint Configuration	Yes		

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
103.	Create Connection return parameters			
104.	ConnectionID	Yes		
105.	SpecificEndpointID ("Z")	Yes		Page 40
106.	LocalConnection Descriptor	Yes		
107.	SecondEndpointID	Yes		Pages 39, 42
108.	Secondconnection ID	Yes		
109.				
110.	ModifyConnection			2.3.4 page 46
111.	CallID	Yes		
112.	Endpoint	Yes		
113.	Connection ID	Yes		
114.	NotifiedEntity	Yes		
115.	LocalConnection Options	Yes	CreateConnectionCmnd refers	
116.	Mode	Yes		Page 42
117.	RemoteConnection Descriptor	Yes		Pages 42, 43
118.	Encapsulated Notification Request			Pages 43, 45, 46, 77
119.	R:	Yes		
120.	S:	Yes		
121.	Encapsulated Endpoint Configuration	No		
122.	Modify Connection return parameters			
123.	LocalConnection Descriptor	Yes	Returns if local connection parameters were modified	Page 44
124.	Delete Connection (from Call Agent)			2.3.5 page 46
125.	CallID	Yes		

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
126.	EndpointID	Yes		
127.	ConnectionID	Yes		
128.	Encapsulated Notification Request			
129.	R:	Yes		
130.	S:	Yes		
131.	Encapsulated Endpoint Configuration	No		
132.	Delete Connection return Parameters			
133.	Connection Parameters			Page 50
134.	Number of packets send	Yes		Pages 47, 49
135.	Number of octets send	Yes	Such as on hook or off hook state per endpoint	Pages 47, 49
136.	Number of packets received	Yes		Pages 47, 49
137.	Number of octets received	Yes		Pages 47, 49
138.	Number of packets lost	Yes		Pages 48, 49
139.	Inter-packet arrival jitter	Yes		Pages 48 - 50
140.	Average transmission delay - latency	Yes		Pages 48 - 50
141.	Delete Connection (from gateway)	No		2.3.6 page 51, 30
142.	CallID			
143.	EndPointID			
144.	ConnectionID			
145.	ReasonCode			

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
146.	Connection Parameters			
147.	DeleteConnection (multiple connections)	Yes		2.3.7 page 51
148.	CallID	Yes		
149.	EndpointID	Yes		
150.	Audit Endpoint	Partially		2.3.8 page 52
151.	EndpointID			
152.	RequestedInfo	Yes		3.2.2.11 pages 76, 53
153.	Wildcard convention * ("all of")	Yes		Pages 27, 52
154.	AuditEndpoint Return parameters			
155.	Endpoint ID list, "Z="	Yes	If nothing was requested, return positive ack if connection exists	
156.	RequestedEvents	Yes		Page 53
157.	Including actions associated with the events	Yes		
158.	DigitMap	Yes		Page 53
159.	SignalRequests TO signals currently active On/Off signals currently ON Pending Brief signals	Yes		Page 53
160.	RequestIdentifier	Yes		Page 53
161.	NotifiedEntity	Yes		Page 53
162.	Connection Identifiers	Yes		Page 53
163.	DetectEvents	Yes	See connection parameters under delete connection	Pages 53,77
164.	ObservedEvents	Yes	Call agent IP is defined in BootP server or <i>ini</i> file	Page 53

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
165.	EventStates	Yes		Page 54
166.	Bearer Information	No	“*” Is reported only in MP-200 for all its endpoints	Page 54
167.	RestartReason	Yes		Page 54
168.	RestartDelay	Yes		Page 54
169.	ReasonCode	No		Page 54
170.	Capabilities			3.2.2.3 pages 70,71,72, 54
171.	List of supported codecs	Yes		Page 54
172.	Packetization Period	No		Page 54
173.	Bandwidth	No		Page 54
174.	Echo Cancelation	No		Page 54
175.	Silence Suppression	No		Page 54
176.	Gain Control	No		
177.	Type of Service	No		Page 54
178.	Resource reservation	No	OK response	
179.	Encryption key	No	Connection was Deleted	
180.	Type of network	Yes	Transient error in transactions	
181.	Supported Event Packages	Yes	Phone is already off hook	
182.	Connection Modes	Yes	Phone is already on hook	Page 55
183.	Audit Connection	Yes	Unknown endpoint	2.3.9 page 55
184.	ConnectionID	Yes	Endpoint not ready	Page 55
185.	RequestedInfo	Yes	Insufficient resource	Page 57
186.	Audit Connection Return Parameters		Protocol error	
187.	CallID	Yes	Unrecognized extension	4.1 Page 119
188.	Notified Entity	Yes	Cannot detect event	Page 56
189.	Local Connection	Yes	Cannot generate signal	Pages 40, 41, 56

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
	Options			
190.	Mode	Yes	Cannot send announcement	Page 56
191.	Remote Connection Descriptor	No	Incorrect transaction id	Page 56
192.	LocalConnection Descriptor	No	Unknown call id	Page 56
193.	Connection Parameters	Yes		2.3.5 pages 48, 56
194.	Restart in Progress (RSIP)		Internal inconsistency	2.3.10 page 56
195.	EndpointID			Page 56
196.	"All of" wildcard (*)	Yes		Page 57
197.	Restart Method	Partially		Page 57
198.	Graceful	No		Page 57
199.	Forced	Yes		Page 57
200.	Restart	Yes		Page 57
201.	Disconnected	Yes	Not supporting Domain name ID, instead use IP address	Page 57
202.	Cancel-graceful	No	Not supporting Domain name ID, instead use IP address	Page 57
203.	Restart Delay	No	UDP port definition is not supported	Page 57
204.	ReasonCode	No	K: 6257 K: 6234-6255	Page 57
205.	Restart in progress return parameters (notified entity & return code)	No		Page 58
206.	Return Codes and Error Codes	Partially		2.4 page 58
207.	100	No	The transaction is currently being executed An actual completion message will follow later	Page 59

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
208.	200	Yes	The requested transaction was executed normally	Page 59
209.	250	Yes	The connection was deleted	Page 59
210.	400	Yes	The transaction couldn't be executed due to a transient error	Page 59
211.	401	Yes	The phone is already off hook	Page 59
212.	402	Yes	The phone is already on hook	Page 59
213.	405	Yes	The transaction could not be executed, because the endpoint is "restarting".	
214.	500	Yes	The transaction could not be executed because the endpoint is unknown	Page 59
215.	501	Yes	The transaction could not be executed because the endpoint is not ready	Page 59
216.	502	Yes	The transaction could not be executed because the endpoint does not have sufficient resources	Page 59
217.	503	No	"All of" wildcard not fully supported The transaction contained an "all of" wildcard, however NotificationRequests non-empty	
218.	504	Yes	Unknown or unsupported command.	
219.	505	Yes	Unsupported RemotedConnectionDescriptor	
220.	506	No	Unable to satisfy both LocalConnectionOptions and RemoteConnection Descriptor	
221.	507	Yes	Unsupported functionality	Page 71

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
222.	510	Yes	The transaction could not be executed because a protocol error was detected	Page 59
223.	511	No	The transaction could not be executed because of the command contained an unrecognized extension	Page 59
224.	512	No	The transaction could not be executed because the gateway is not equipped to detect one of the requested events	Page 59
225.	513	Yes	The transaction could not be executed because the gateway is not equipped to generate one of the requested signals	Page 60
226.	514	No	The transaction could not be executed because the gateway cannot send the specified announcement	Page 60
227.	515	Yes	The transaction refers to an incorrect connection ID	Page 60
228.	516	Yes	The Transaction refers to an unknown call ID	Page 60
229.	517	Yes	Unsupported or invalid mode	
230.	518	No	Unsupported or unknown package	
231.	519	Yes	Gateway does not have a digit map	
232.	520	Yes	The transaction could not be executed because the GateWay is restarting	
233.	521	Yes	Endpoint redirected to another Call Agent endpoint is restarting	
234.	522	Yes	No such event or signal	
235.	523	Yes	Unknown action or illegal combination of actions	
236.	524	Yes	Internal inconsistency in localConnectionOptions	

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
237.	525-531	No		
238.	532	Yes	Unsupported value in LocalConnectionOptions	
239.	533	Yes	Response too big	
240.	534	Yes	Codec negotiation failure	
241.	535	Yes	Packetization period not supported	
242.	536	No	Unknown or unsupported RestartMethod	
243.	537	No	Unknown or unsupported digit map extension	
244.	538	Yes	Event or Signal error	
245.	Reason Codes (900, 901, 902)	No		2.5 page 61
246.	900			
247.	901			
248.	902			
249.	MGCP Command Header		The transaction could not be executed because the GateWay is restarting	3.2 page 62
250.	Endpoint identifier	Yes		3.2.1.3 page 64
251.	Notified entity	Yes		Page 64
252.	In notified entity, If port # is omitted, using default MGCP port (2427)	Yes		Page 65
253.	Response Acknowledgement	Yes (receive side only)		3.2.2.1 Page 68
254.	Encoding of Session Description - SDP			3.5 page 86
255.	SDP parameters: v,c,m,a	Yes		

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
256.	Using RTPMAP attribute to define encoding of dynamic audio formats	No		Page 87
257.	Optional Ptime attribute to define packet duration	No		Page 87
258.	IP address of remote/local gateways	Yes		Page 87
259.	Transmission over UDP			3.6 page 91
260.	Transaction identifiers	Yes		Page 92
261.	Receiving Duplicated transaction IDs	Yes		Page 63, 92
262.	Retransmission timers	Yes		3.6.3 page 93
263.	Piggy backing	Yes		3.6.4 Page 94
264.	Provisional responses	No		3.6.5 Page 94
265.	MultipleCall Agents and Call Agent Redundancy	Yes		
266.	States, failover and race conditions	Partially		3.2 Page 79
267.	Basic Assumptions			3.2.1.3 Page 81
268.	Failover Assumptions and Highlights			4.1 Page 119
269.	Call Agents DNS	No		4.1 Page 119
270.	Notified Entity for endpoint	Yes		4.1 Page 119
271.	Responses send to source address	Yes		
272.	Backup Call Agent	Yes		

Table 16-1: MGCP Compliance Matrix

#	Feature	Support	AudioCodes Comments	References (to IETF RFC 3435)
273.	Security, Retransmission, Detection			4.2 page 96
274.	Commands retransmission	Yes		
275.	Checking presence of new CA	No		Page 99
276.	Disconnecting endpoint/gateway	No		Page 99
277.	Race Conditions			4.3 Page 99
278.	Quarantine list	Yes		4.3.1 page 99
279.	Explicit detection	Yes		4.3.2 page 103
280.	Ordering of commands	Yes		Page 104
281.	Restart avalanche	Yes		Page 105
282.	Disconnected endpoints	No		Page 107
283.	Security requirements			5. Page 108
284.	MGCP IP security (RFC 1825)	No		Page 108

Reader's Notes

17 Appendix H - SNMP Traps

This section provides information regarding proprietary traps currently supported in the MP-11x. Note that traps whose purposes are alarms are different from traps whose purposes are not alarms, e.g., logs.

Currently, all traps have the same structure, which is made up of the same 11 varbinds. An example is: 1.3.6.1.4.1.5003.9.10.1.21.1

The source varbind is made up of a string that details the component from which the trap is being sent, forwarded by the hierarchy in which it resides. For example, an alarm from an SS7 link has the following string in its source varbind:

```
acBoard#1/SS7#0/SS7Link#6
```

In this example, the SS7 link number is specified as 6 and is part of the only SS7 module in the device that is placed in slot number 1 (in a chassis) and is the module to which this trap is related. For devices where there are no chassis options the slot number of the board is always 1.

17.1 Alarm Traps

The following provides information relating to those alarms that are raised as the result of a generated SNMP trap. The component name described within each of the following section headings refers to the string that is provided in the acBoardTrapGlobalsSource trap varbind. In all the following discussions, to clear a generated alarm the same notification type is sent but with the severity set to 'cleared'.

17.1.1 Component: Board#<n>

<n> is the slot number when the BOARDNAME resides in a chassis and is 1 when the device is stand alone.

Table 17-1: acBoardFatalError Alarm Trap

Alarm:	acBoardFatalError
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.1
Default Severity	Critical
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable (56)
Alarm Text:	Board Fatal Error: <text>
Status Changes:	
Condition:	Any fatal error
Alarm status:	Critical
<text> value:	A run-time specific string describing the fatal error

Table 17-1: acBoardFatalError Alarm Trap

Alarm:	acBoardFatalError
Condition:	After fatal error
Alarm status:	Status stays critical until reboot. A clear trap is not sent.
Corrective Action:	Capture the alarm information and the syslog close, if active. Contact your first-level support group. The support group will likely want to collect additional data from the device and then perform a reset.

Table 17-2: acBoardEvResettingBoard Alarm Trap

Alarm:	acBoardEvResettingBoard
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.5
Default Severity	critical
Event Type:	equipmentAlarm
Probable Cause:	outOfService (71)
Alarm Text:	User resetting board
Status Changes:	
Condition:	When a soft reset is triggered via either web interface or SNMP.
Alarm status:	critical
Condition:	After raise
Alarm status:	Status stays critical until reboot. A clear trap is not sent.
Corrective Action:	A network administrator has taken action to reset the device. No corrective action is needed.

17.1.2 Component: AlarmManager#0

Table 17-3: acActiveAlarmTableOverflow Alarm Trap

Alarm:	acActiveAlarmTableOverflow
OID:	1.3.6.1.4.15003.9.10.1.21.2.0.12
Default Severity	Major
Event Type:	processingErrorAlarm

Table 17-3: acActiveAlarmTableOverflow Alarm Trap

Alarm:	acActiveAlarmTableOverflow
Probable Cause:	resourceAtOrNearingCapacity (43)
Alarm Text:	Active alarm table overflow
Status Changes:	
Condition:	Too many alarms to fit in the active alarm table
Alarm status:	Major
Condition:	After raise
Alarm status:	Status stays major until reboot. A clear trap is not sent.
Note:	The status stays major until reboot as it denotes a possible loss of information until the next reboot. If an alarm was raised when the table was full, it is possible that the alarm is active, but does not appear in the active alarm table.
Corrective Action:	Some alarm information may have been lost, but the ability of the device to perform its basic operations has not been impacted. A reboot is the only way to completely clear a problem with the active alarm table. Contact your first-level group.

17.1.3 Component: EthernetLink#0

This trap is related to the Ethernet Link Module (the #0 numbering does not apply on the physical Ethernet link).

Table 17-4: acBoardEthernetLinkAlarm Alarm Trap

Alarm:	acBoardEthernetLinkAlarm
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.10
Default Severity	Critical
Event Type:	equipmentAlarm
Probable Cause:	underlyingResourceUnavailable (56)
Alarm Text:	Ethernet link alarm: <text>
Status Changes:	
Condition:	Fault on single interface

Table 17-4: acBoardEthernetLinkAlarm Alarm Trap

Alarm:	acBoardEthernetLinkAlarm
Alarm status:	Major
<text> value:	Redundant link is down
Condition:	Fault on both interfaces
Alarm status:	critical
<text> value:	No Ethernet link
Condition:	Both interfaces are operational
Alarm status:	cleared
Corrective Action:	Ensure that both Ethernet cables are plugged into the back of the system. Inspect the system's Ethernet link lights to determine which interface is failing. Reconnect the cable or fix the network problem

17.2 Log Traps (Notifications)

This section details traps that are not alarms. These traps are sent out with the severity varbind value of "indeterminate". These traps do not clear, they do not appear in the alarm history or active tables. One log trap that does send out clear is acPerformanceMonitoringThresholdCrossing.

Table 17-5: acKeepAlive Log Trap

Alarm:	acKeepAlive
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.16
Default Severity	Indeterminate
Event Type:	other (0)
Probable Cause:	other (0)
Alarm Text:	Keep alive trap
Status Changes:	
Condition:	The STUN client in the board is enabled and has either identified a NAT or is not finding the STUN server The <i>ini</i> file contains the following line: 'SendKeepAliveTrap=1'
Trap status:	Trap is sent
Note:	Keep-alive is sent out every 9/10 of the time defined in the NatBindingDefaultTimeout parameter

Table 17-6: acPerformanceMonitoringThresholdCrossing Log Trap

Alarm:	acPerformanceMonitoringThresholdCrossing
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.27
Default Severity	Indeterminate
Event Type:	other (0)
Probable Cause:	other (0)
Alarm Text:	"Performance: Threshold alarm was set ", with source = name of performance counter which caused the trap
Status Changes:	
Condition:	A performance counter has crossed the high threshold
Trap status:	Indeterminate
Condition:	A performance counter has crossed the low threshold
Trap status:	cleared

17.3 Other Traps

The following are provided as SNMP traps and are not alarms.

Table 17-7: coldStart Trap

Trap Name:	coldStart
OID:	1.3.6.1.6.3.1.1.5.1
MIB	SNMPv2-MIB
Note:	This is a trap from the standard SNMP MIB.

Table 17-8: authenticationFailure Trap

Trap Name:	authenticationFailure
OID:	1.3.6.1.6.3.1.1.5.5
MIB	SNMPv2-MIB

Table 17-9: acBoardEvBoardStarted Trap

Trap Name:	acBoardEvBoardStarted
OID:	1.3.6.1.4.1.5003.9.10.1.21.2.0.4
MIB	AcBoard
Severity	cleared
Event Type:	equipmentAlarm
Probable Cause:	Other(0)
Alarm Text:	Initialization Ended
Note:	This is the AudioCodes Enterprise application cold start trap.

17.4 Trap Varbinds

Every AudioCodes Enterprise trap described above provides the following fields (known as 'varbinds'). Refer to the AcBoard MIB for additional details on these varbinds.

- acBoardTrapGlobalsName
- acBoardTrapGlobalsTextualDescription
- acBoardTrapGlobalsSource
- acBoardTrapGlobalsSeverity
- acBoardTrapGlobalsUniqID
- acBoardTrapGlobalsType
- acBoardTrapGlobalsProbableCause
- acBoardTrapGlobalsAdditionalInfo1
- acBoardTrapGlobalsAdditionalInfo2
- acBoardTrapGlobalsAdditionalInfo3

Note that acBoardTrapGlobalsName is actually a number. The value of this varbind is 'X' minus 1, where 'X' is the last number in the trap OID. For example, the 'name' of acBoardEthernetLinkAlarm is '9'. The OID for acBoardEthernetLinkAlarm is 1.3.6.1.4.1.5003.9.10.1.21.2.0.10.

18 Appendix I - Customizing the Web Interface

OEM customers incorporating AudioCodes' devices into their portfolios can customize the device's Web interface to suit their specific corporate logo and product naming conventions.

OEM customers can customize the Web interface's title bar (AudioCodes' title bar is shown in the figure, "Web Interface Title Bar", below and an example of a customized title bar is shown in the figure, "Customized Web Interface Title Bar" below.)



Note: The product name appears according to the AudioCodes product utilized together with the AudioCodes Web Interface.

Equation 1: Web Interface Title Bar

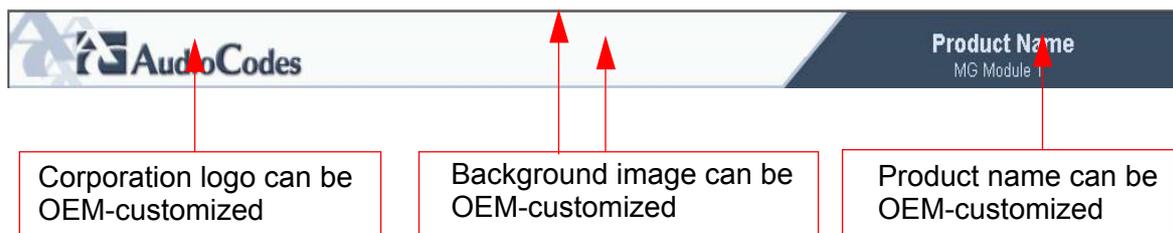


Figure 18-1: Customized Web Interface Title Bar



18.1 Company & Product Bar Components

The Title bar is composed of 3 components:

- Replacing the main corporation logo - refer to "Replacing the Main Corporate Logo" on page 280
- Replacing the title bar's background image file - refer to "Replacing the Title Bar's Background Image File" on page 282
- Customizing the product's name - Refer to "Customizing the Product's Name" on page 283

18.2 Replacing the Main Corporate Logo

The main corporate logo can be replaced either with a different logo image file (refer to 'Replacing the Main Corporate Logo with an Image File' About the Web Interface Screen' on page 119e' below) or with a text string (refer to 'Replacing the Main Corporate Logo with a Text String')



Note: When the main corporate logo is replaced, the AudioCodes logo in the main menu bar on the left (refer to "About the Web Interface Screen" on page 119) and the AudioCodes logo in the Software Upgrade Wizard (refer to "Software Upgrade Wizard" on page 155) disappear.

18.2.1 Replacing the Main Corporate Logo with an Image File

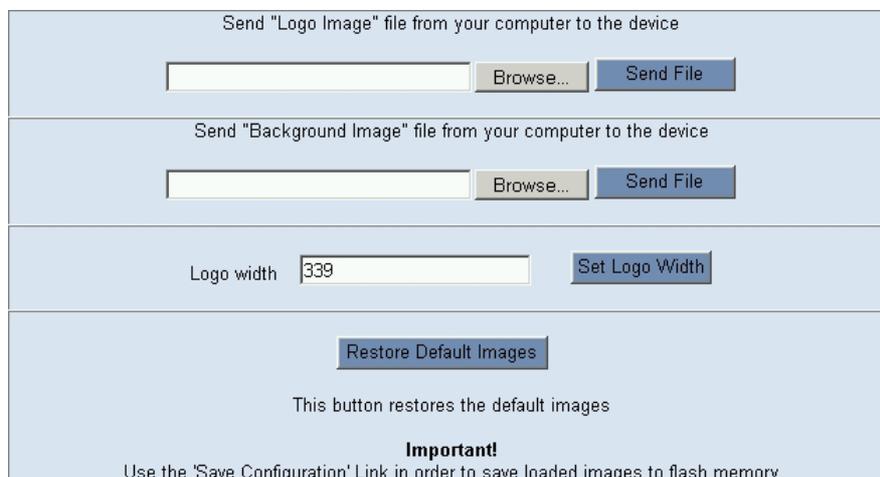


Note: Use a gif, jpg or jpeg file for the logo image. It is important that the image file has a fixed height of 59 pixels (the width can be configured). The total size limit for the image files is 128 k bytes if both files are loaded. Each file type (Logo file or BKG file) should not exceed 64 k bytes).

➤ **To replace AudioCodes' default logo with your own corporate logo via the Web interface, take these 8 steps:**

1. Access the Embedded Web Server (refer to "Accessing the Embedded Web Server" on page 118).
2. In the browser's **URL** field, enter the IP address of the location of the AudioCodes' Web Interface Application, followed by **/AdminPage**.
3. If you have not accessed this page for a while, you are prompted for your user name and Password. Enter them and press **OK**.
4. On the Main-menu bar to the left, click the **Logo Image Download** option. The Image Download screen appears.

Figure 18-2: Logo Image Download Screen



Send "Logo Image" file from your computer to the device

Send "Background Image" file from your computer to the device

Logo width

This button restores the default images

Important!
Use the 'Save Configuration' Link in order to save loaded images to flash memory

5. Click the **Browse** button in the **Send Logo Image File from your computer to the device** box. Navigate to the folder that contains the logo image file you want to download.
6. Click the **Send File** button. The file is sent to the device. When the download is complete, the screen is automatically refreshed and the new logo image is displayed.
7. Check the appearance of the logo to verify that it appears as desired. If you want to modify the width of the logo (the default width is 339 pixels), in the **Logo Width** field, enter the new width (in pixels) and press the **Set Logo Width** button.
8. Save the image to flash memory by clicking the Save Configuration button on the Save Configuration screen. The new logo appears on all Web interface screens.



Note: If you encounter any problem during the loading of the files, or you want to restore the default images, click the **Restore Default Images** button.

➤ **To replace AudioCodes' default logo with your own corporate logo image via the ini file, take these 2 steps:**

1. Place your corporate logo image file in the same folder in which the device's ini file is located (i.e., the same location defined in the BootP/TFTP server). For detailed information on the BootP/TFTP server, refer to the Appendix, "BootP/TFTP Server" on page 185 .
2. Add/modify the two ini file parameters in the table below according to the procedure described in "Software Upgrade Wizard" on page 155.



Note: Loading the device's ini file via the 'Configuration File' screen in the Web interface does not load the corporate logo image file as well.

Table 18-1: Customizable Logo ini File Parameters for the Image File

Parameter	Description
LogoFileName	The name of the image file containing your corporate logo. Use a gif, jpg or jpeg image file. The default is AudioCodes' logo file. Note: The length of the name of the image file is limited to 47 characters.
LogoWidth	Width (in pixels) of the logo image. Note: The optimal setting depends on the resolution settings. The default value is 339, which is the width of AudioCodes' displayed logo.

18.2.2 Replacing the Main Corporate Logo with a Text String

The main corporate logo can be replaced with a text string. To replace AudioCodes' default logo with a text string via the Web interface, modify the two *ini* file parameters in the table below according to the procedure described in "Modifying '*ini*' File Parameters via the Web Interface's AdminPage" on page 284.

Table 18-2: Customizable Logo ini File Parameters for the String Text

Parameter	Description
UseWebLogo	0 = Logo image is used (default value). 1 = Text string is used instead of a logo image.
WebLogoText	Text string that replaces the logo image. The string can be up to 15 characters.

18.3 Replacing the Background Image File

The background image file is repeated across the width of the screen. The number of times the image is repeated depends on the width of the background image and screen resolution. When choosing your background image, keep this in mind.



Note: Use a gif, jpg or jpeg file for the background image. It is important that the image file has a fixed height of 59 pixels. The total size limit for the image files is 128 k bytes if both files are loaded. Each file type (Logo file or BKG file) should not exceed 64 k bytes)

- **To replace the background image via the Web interface, take these 7 steps:**
 1. Access the Embedded Web Server (refer to "Accessing the Embedded Web Server" on page 118).
 2. In the browser's **URL** field, enter the IP address of the location of the Web Interface Application, followed by **/AdminPage**.
 3. If you have not accessed this page for a while, you are prompted for your user name and Password. Enter them and press **OK**.
 4. On the Main-menu bar to the left, click the **Image Download** option. The Image Download screen appears.(shown in the figure, 'Image Download Screen' above).
 5. Click the **Browse** button in the **Send Background Image File from your computer to gateway** box. Navigate to the folder that contains the background image file you want to download.
 6. Click the **Send File** button. The file is sent to the device. When the download is complete, the screen is automatically refreshed and the new background image is displayed.

7. Save the image to the flash memory by clicking the **Save Configuration** button on the Save Configuration screen. The new background appears on all Web interface screens.



Note: If you encounter any problem during the loading of the files, or you want to restore the default images, click the **Restore Default Images** button.

➤ **To replace the background image via the ini file, take these 2 steps:**

1. Place your background image file in the same folder in which the device's ini file is located (i.e., the same location defined in the BootP/TFTP server). For detailed information on the BootP/TFTP server, refer to the Appendix, 'BootP/TFTP Server' on page 185.
2. Add/modify the ini file parameters in the table below according to the procedure described "Software Upgrade Wizard" on page 155.



Note: Loading the device's ini file via the Configuration File screen in the Web interface does not load the background image file as well.

Table 18-3: Customizable Background ini File Parameters

Parameter	Description
BkgImageFileName	<p>The name of the file containing the new background. Use a gif, jpg or jpeg image file. The default is AudioCodes background file.</p> <p>Note: The length of the name of the image file is limited to 47 characters.</p>

18.4 Customizing the Product Name

The Product Name text string can be modified according to OEMs specific requirements.

- To replace the default product name with a text string via the Web interface, modify the two ini file parameters in the table below according to the procedure described in 'Modifying 'ini' File Parameters via the Web Interface's AdminPage' on page 284.
- To replace the default product name with a text string via the ini file, add/modify the two ini file parameters in the table below according to the procedure described in 'Software Upgrade Wizard' on page 155.

Table 18-4: Customizable Product Name ini File Parameters

Parameter	Description
UseProductName	0 = Don't change the product name (default). 1 = Enable product name change.
UserProductName	Text string that replaces the product name. The default is "MP-11x". The string can be up to 29 characters.

18.4.1 Customizing the Web Browser Title Bar

Figure 18-3: Default Web Browser Title Bar

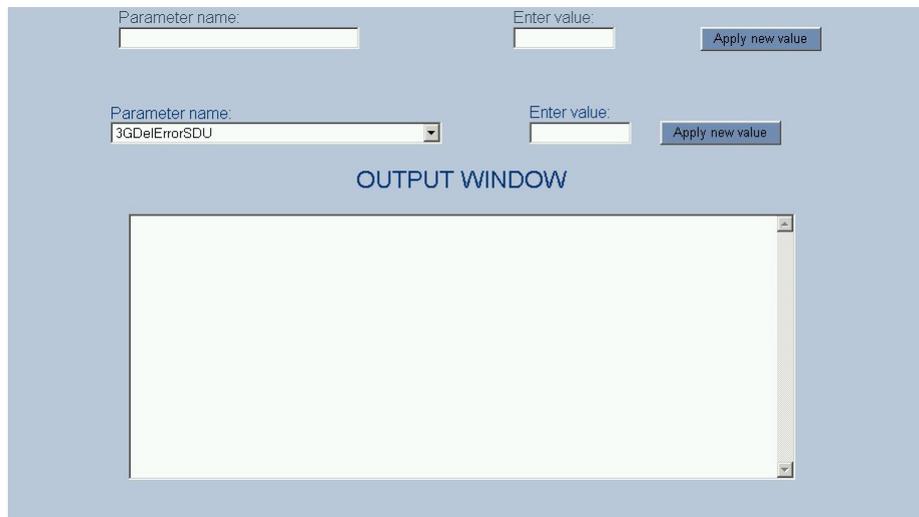

Upon customizing the logo section of the screen as described in "Replacing the Main Corporate Logo" on page 280, the AudioCodes string on the Web browser's title bar changes to the text string held in the WebLogoText parameter. If this parameter holds an empty string, the browser's title bar contains only its own name.

18.5 Modifying ini File Parameters via the Web Interface's AdminPage

- **To modify ini file parameters via the AdminPage, take these 7 steps:**
 1. Open AudioCodes' Web Interface Application, using the directions in the Device Management section of the accompanying AudioCodes product user's manual.
 2. In the browser's **URL** field, enter the IP address of the location of the AudioCodes' Web Interface Application, followed by **/AdminPage**.
 3. If you have not accessed this page for a while, you are prompted for your user name and Password. Enter them and press **OK**.

4. Click the **INI Parameters** option, the ini Parameters screen is displayed.

Figure 18-4: ini Parameters Screen



5. In the **Parameter Name** dropdown list, select the required ini file parameter.
6. In the **Enter Value** text box to the right, enter the parameter's new value.
7. Click the **Apply new value** button to the right. The ini Parameters screen is refreshed, the parameter name with the new value appears in the fields at the top of the screen and the Output Window displays a log displaying information on the operation.



Note: You cannot load the image files (e.g., logo/background image files) to the device by choosing a file name parameter in this screen.

Reader's Notes

19 Appendix J - Call Progress Tones Wizard

This Appendix describes the Call Progress Tones Wizard (CPTWizard), an application designed to help the provisioning of an MP-11x FXO gateway, by recording and analyzing Call Progress Tones generated by any PBX or telephone network.

19.1 About this Software

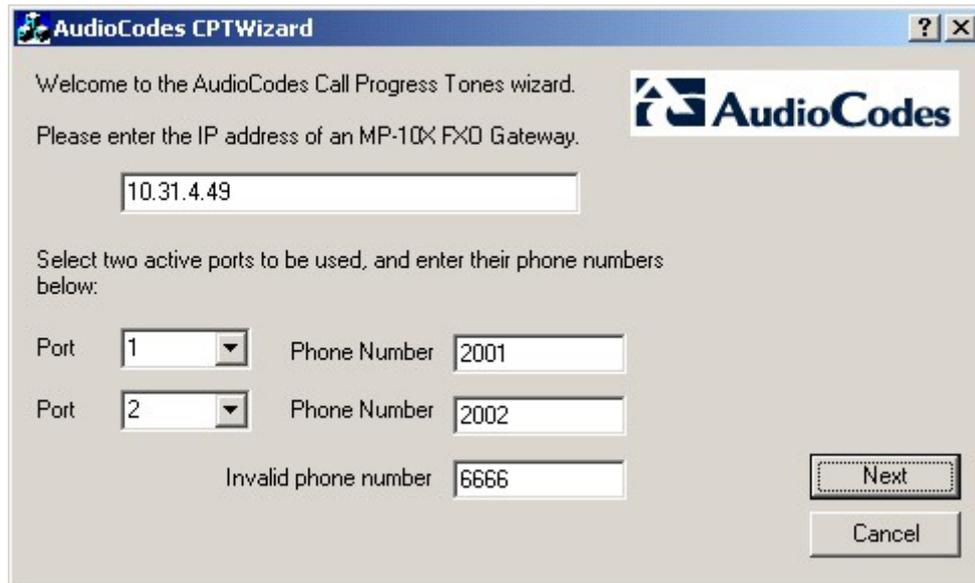
- This wizard helps detect the call progress tones generated by your PBX (or telephone exchange), and creates a basic call progress tone ini file, providing a good starting point when configuring an MP-11x FXO gateway (an ini file containing definitions for all relevant call progress tones can be converted to a dat suitable for downloading to the gateway, using the DConvert utility).
- To use this wizard, you need an MP-11x FXO gateway connected to your PBX with 2 physical phone lines. This gateway should be configured with the factory-default settings, and should not be used for phone calls during operation of the wizard.
- Firmware version 4.2 and above is required on the gateway.

19.2 Installation

- CPTWizard can be installed on any Windows 2000 or Windows XP based PC. Windows-compliant networking and audio peripherals are required for full functionality.
- To install CPTWizard, copy the files from the installation media to any folder on the PC's hard disk. No further setup is required.
- Approximately 5 MB of hard disk space are required.

19.3 Initial Settings

- **To start CPTWizard take these 4 steps:**
 2. Double-click on your copy of the CPTWizard.exe program file. The initial settings dialog is displayed:

Figure 19-1: Initial Settings Dialog


3. In the appropriate fields, fill in the gateway's IP address, select which of the gateway's ports are connected to your PBX, and specify the phone number for each extension.
4. In the "Invalid phone number" box, enter a number which generates a "fast busy" tone when dialed. Usually, any incorrect phone number should cause a "fast busy" tone.
5. When the parameters are entered correctly, press NEXT.

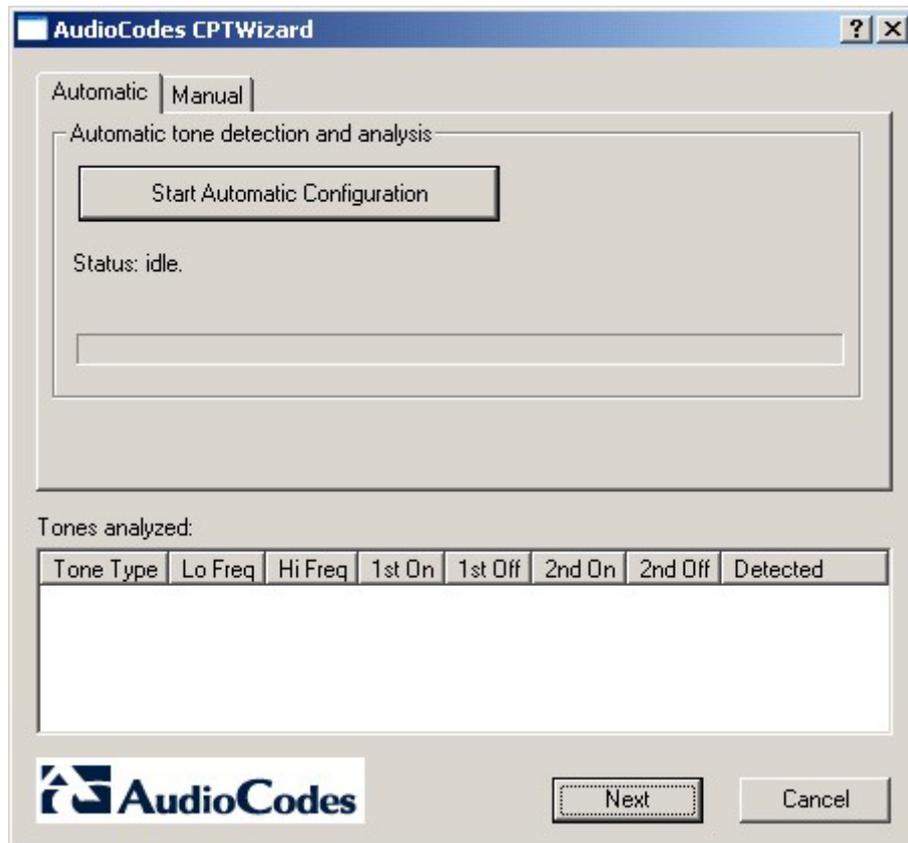


Note: CPTWizard connects to the gateway using the TPNCP protocol. If this protocol has been disabled in the gateway configuration, CPTWizard does not display the next dialog and an error is reported.

19.4 Recording Dialog – Automatic Mode

Once the connection to the MP-11x FXO gateway is established, the recording dialog is displayed:

Figure 19-2: Recording Dialog

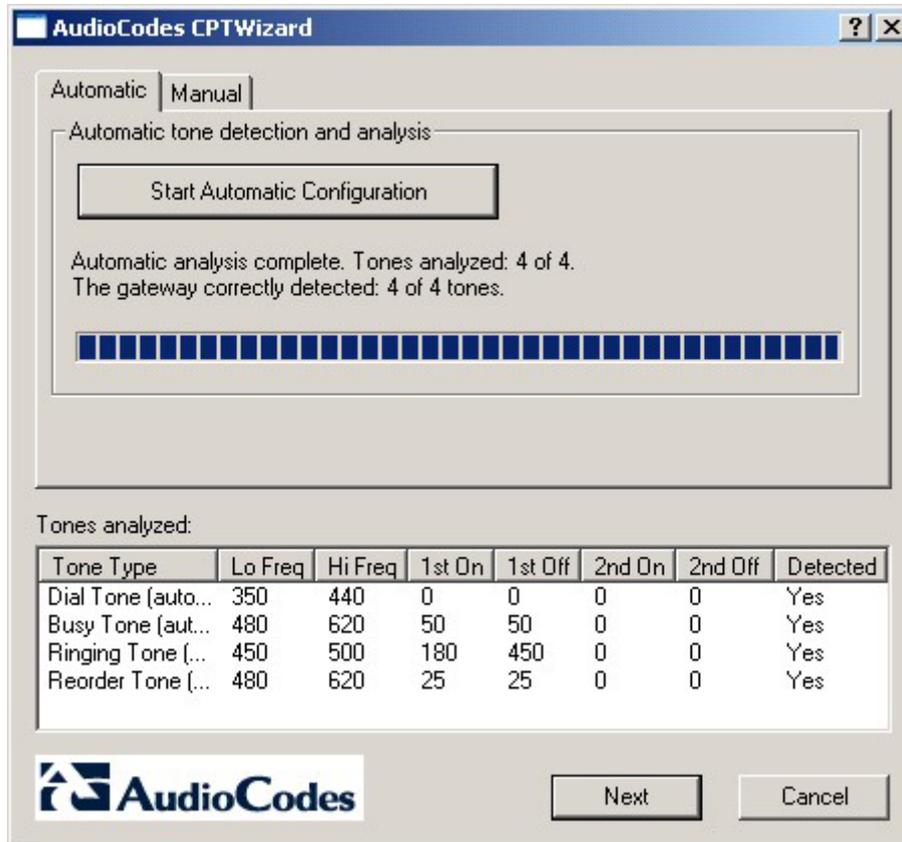


➤ **To start Recording Dialog in Automatic Mode take these 5 steps:**

1. To start the detection process, press the “Start Automatic Configuration” button. The wizard will start a call progress tone detection sequence (the operation should be about 60 seconds long), as follows:
 - Set port 1 off-hook, listen to the dial tone
 - Set port 1 and port 2 off-hook, dial port 2’s number, listen to the busy tone
 - Set port 1 off-hook, dial port 2’s number, listen to the ringback tone
 - Set port 1 off-hook, dial an invalid number, listen to the reorder tone

2. The wizard will then analyze the recorded call progress tones, and display a message specifying which tones were detected (by the gateway) and analyzed (by the wizard) correctly. At the end of a successful detection operation, the dialog displays the results shown in the figure below:

Figure 19-3: Recording Dialog after Automatic Detection



3. All four call progress tones are saved in the same directory as the CPTWizard.exe file, with the following names:
 - ◆ cpt_recorded_dialtone.pcm
 - ◆ cpt_recorded_busytone.pcm
 - ◆ cpt_recorded_rington.pcm
 - ◆ cpt_recorded_invalidtone.pcm
4. All files are saved as standard A-law PCM at 8000 bits per sample.



Note 1: If the gateway is configured correctly (with a call progress tones *dat* file downloaded to the gateway), all four call progress tones shall be **detected** by the gateway. By noting whether the gateway detects the tones or not, you can determine how well the call progress tones *dat* file matches your PBX. During the first run of CPTWizard, it is probable that the gateway might not detect any tones.

Note 2: Some tones cannot be detected by the MP-11x gateway hardware (such as 3-frequency tones and complex cadences). CPTWizard is therefore limited to detecting only those tones which can be detected on the MP-11x gateway.

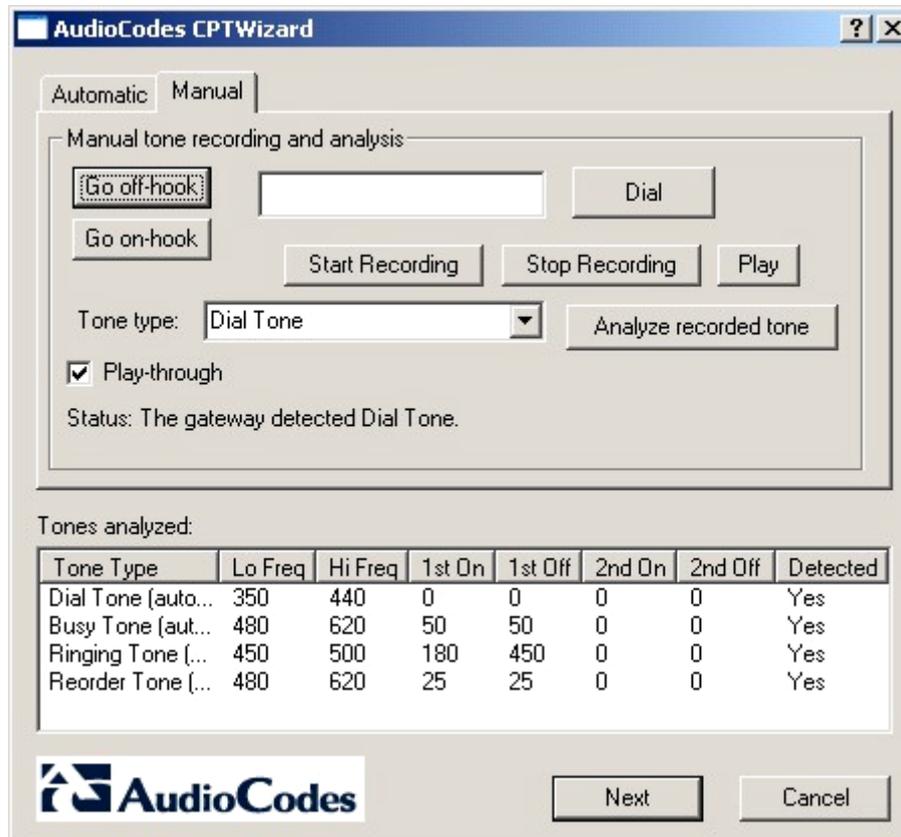
5. At this stage, you can either press NEXT to generate a call progress tone *ini* file and end the wizard, or continue to manual recording mode.

19.5 Recording Dialog – Manual Mode

➤ To start Recording Dialog in Manual Mode take these 6 steps:

1. Choose the “Manual” tab at the top of the recording dialog, it is then possible to record and analyze more tones, which are included in the call progress tone *ini* file.

Figure 19-4: Recording Dialog in Manual Mode



2. For easy operation, use the play-through check box to hear the tones through your PC speakers.
3. Press the “Set off-hook” button, enter a number to dial in the Dial box, and press the Dial button. When you’re ready to record, press the “Start Recording” button; when the desired tone is complete press “Stop Recording”. (The recorded tone will be saved as “cpt_manual_tone.pcm”.)



Note: Due to some PC audio hardware limitations, you may hear “clicks” in play-through mode. It is safe to ignore these clicks.

4. Select the tone type from the drop-down list, and press “Analyze”. The analyzed tone is added to the list at the bottom of the dialog. It is possible to record and analyze several different tones for the same tone type (e.g., different types of “busy” signal).
5. Repeat the process for more tones, as necessary.
6. When you’re done adding tones to the list, click **Next** to generate a call progress tone *ini* file and end the wizard.

19.6 The Call Progress Tone ini File

Once the wizard completes the call progress tone detection, a text file named *call_progress_tones.ini* is created in the same directory as CPTWizard.exe. This file contains:

1. Information about each tone recorded and analyzed by the wizard. This includes frequencies and cadence (on/off) times, and is required for using this file with the DConvert utility.

Figure 19-5: Call Progress Tone Properties

```
[CALL PROGRESS TONE #1]
Tone Type=2
Low Freq [Hz]=440
High Freq [Hz]=480
Low Freq Level [-dBm]=0
High Freq Level [-dBm]=0
First Signal On Time [10msec]=200
First Signal Off Time [10msec]=390
Second Signal On Time [10msec]=0
Second Signal Off Time [10msec]=0
```

- Information related to possible matches of each tone with the CPTWizard internal database of well-known tones. This information is specified as comments in the file, and is ignored by Dconvert utility.

Figure 19-6: Call Progress Tone Database Matches

```
# Recorded tone: Ringing Tone
## Matches: PBX name=ITU Anguilla, Tone name=Ringing tone
## Matches: PBX name=ITU Antigua and Barbuda, Tone name=Ringing t
## Matches: PBX name=ITU Barbados, Tone name=Ringing tone
## Matches: PBX name=ITU Bermuda, Tone name=Ringing tone
## Matches: PBX name=ITU British Virgin Islan, Tone name=Ringing
## Matches: PBX name=ITU Canada, Tone name=Ringing tone
## Matches: PBX name=ITU Dominica (Commonweal, Tone name=Ringing
## Matches: PBX name=ITU Grenada, Tone name=Ringing tone
## Matches: PBX name=ITU Jamaica, Tone name=Ringing tone
## Matches: PBX name=ITU Montserrat, Tone name=Ringing tone
## Matches: PBX name=ITU Saint Kitts and Nevi, Tone name=Ringing
## Matches: PBX name=ITU Trinidad and Tobago, Tone name=Ringing t
## Matches: PBX name=ITU Turks and Caicos Isl, Tone name=Ringing
## Matches: PBX name=*, Tone name=Bell ring
## Matches: PBX name=TADIRAN CORAL 2, Tone name=Coral II Ring
## Matches: PBX name=TADIRAN CORAL 2I, Tone name=Coral III Ring
```

- Information related to matches of all tones recorded with the CPTWizard internal database. The database is scanned to find one or more PBX definitions which match all recorded tones (i.e. both dial tone, busy tone, ringing tone, reorder tone and any other manually-recorded tone – all match the definitions of the PBX). If a match is found, the entire PBX definition is reported in the *ini* file using the same format.

Figure 19-7: Full PBX/Country Database Match

```
## Some tones matched PBX/country ITU Bermuda
## Additional database tones guessed below (remove #'s to use)
#
# # ITU Bermuda, Busy tone
# [CALL PROGRESS TONE #16]
# Tone Type=3
# Low Freq [Hz]=480
# High Freq [Hz]=620
# Low Freq Level [_dBm]=0_
```

- If a match is found with the database, consider using the database definitions instead of the recorded definitions, as they might be more accurate.
- For full operability of the MP-1xx FXO gateway, it may be necessary to edit this file and add more call progress tone definitions. Sample call progress tone *ini* files are available in the release package.
- When the call progress tones *ini* file is complete, use the DConvert utility to create a downloadable call progress tone *dat* file. After loading this file to the gateway, repeat the automatic detection phase discussed above, and verify that the gateway detects all four call progress tones correctly.

Reader's Notes

20 Appendix K - Regulatory Information

20.1 Appendix - Regulatory Information - MP-11x/FXS

<i>Declaration of Conformity</i>	
Application of Council Directives:	73/23/EEC (including amendments), 89/336/EEC (including amendments),
Standards to which Conformity is Declared:	EN55022: 1998, Class B EN55024:1998 EN61000-3-2: 1995 (including amendments A1: 1998, A2: 1998, A14: 2000) EN61000-3-3: 1995 EN60950-1: 2001
Manufacturer's Name:	AudioCodes Ltd.
Manufacturer's Address:	1 Hayarden Street, Airport City, Lod 70151, Israel.
Type of Equipment:	Analog VoIP System.
Model Numbers:	MP-11x/FXS (x- may represent 2, 4, 8)
I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards.	
	11 th February 2005 Airport City, Lod, Israel
<i>Signature</i> I. Zusmanovich, Compliance Engineering Manager	<i>Date (Day/Month/Year)</i> <i>Location</i>

Czech	[AudioCodes Ltd] tímto prohlašuje, že tento [MP-11x/FXS series] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 89/336/EEC, 73/23/EEC.
Danish	Undertegnede [AudioCodes Ltd] erklærer herved, at følgende udstyr [MP-11x/FXS Series] overholder de væsentlige krav og øvrige relevante krav i direktiv 89/336/EEC, 73/23/EEC.
Dutch	Hierbij verklaart [AudioCodes Ltd] dat het toestel [MP-11x/FXS Series] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 89/336/EEC, 73/23/EEC
English	Hereby, [AudioCodes Ltd], declares that this [MP-11x/FXS Series] is in compliance with the essential requirements and other relevant provisions of Directive 89/336/EEC, 73/23/EEC.
Estonian	Käesolevaga kinnitab [AudioCodes Ltd] seadme [MP-11x/FXS Series] vastavust direktiivi 89/336/EEC, 73/23/EEC põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish	[AudioCodes Ltd] vakuuttaa täten että [MP-11x/FXS Series] tyypinen laite on direktiivin 89/336/EEC, 73/23/EEC oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French	Par la présente [AudioCodes Ltd] déclare que l'appareil [MP-11x/FXS Series] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 89/336/EEC, 73/23/EEC
German	Hiermit erkläre [AudioCodes Ltd], dass sich dieser/diese/dieses [MP-11x/FXS Series] in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 89/336/EEC, 73/23/EEC befindet". (BMW)
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [AudioCodes Ltd] ΔΗΛΩΝΕΙ ΟΤΙ [MP-11x/FXS Series] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 89/336/EEC, 73/23/EEC
Hungarian	Alulírott, [AudioCodes Ltd] nyilatkozom, hogy a [MP-11x/FXS Series] megfelel a vonatkozó alapvető követelményeknek és az 89/336/EEC, 73/23/EEC irányelv egyéb előírásainak
Icelandic	æki þetta er í samræmi við tilskipun Evrópusambandsins 89/336/EEC, 73/23/EEC

Italian	Con la presente [AudioCodes Ltd] dichiara che questo [MP-11x/FXS Series] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 89/336/EEC, 73/23/EEC.
Latvian	Ar šo [AudioCodes Ltd] deklarē, ka [MP-11x/FXS Series] atbilst Direktīvas 89/336/EEC, 73/23/EEC būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian	[AudioCodes Ltd] deklaruoja, kad irenginys [MP-11x/FXS Series] tenkina 89/336/EEC, 73/23/EEC Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas
Maltese	Hawnhekk, [AudioCodes Ltd], jiddikjara li dan [MP-11x/FXS Series] jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Direttiva 89/336/EEC, 73/23/EEC
Norwegian	Dette produktet er i samhørighet med det Europeiske Direktiv 89/336/EEC, 73/23/EEC
Polish	[AudioCodes Ltd], deklaruje z pełna odpowiedzialnością, że wyrób [MP-11x/FXS Series] spełnia podstawowe wymagania i odpowiada warunkom zawartym w dyrektywie 89/336/EEC, 73/23/EEC
Portuguese	[AudioCodes Ltd] declara que este [MP-11x/FXS Series] está conforme com os requisitos essenciais e outras disposições da Directiva 89/336/EEC, 73/23/EEC.
Slovak	[AudioCodes Ltd] týmto vyhlasuje, že [MP-11x/FXS Series] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 89/336/EEC, 73/23/EEC.
Slovene	Šiuo [AudioCodes Ltd] deklaruoja, kad šis [MP-11x/FXS Series] atitinka esminius reikalavimus ir kitas 89/336/EEC, 73/23/EEC Direktyvos nuostatas.
Spanish	Por medio de la presente [AudioCodes Ltd] declara que el [MP-11x/FXS Series] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 89/336/EEC, 73/23/EEC
Swedish	Härmed intygar [AudioCodes Ltd] att denna [MP-11x/FXS Series] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 89/336/EEC, 73/23/EEC.

Telecommunication Safety

The safety status of each port is declared and detailed in the table below:

Ports	Safety Status
Ethernet (100 Base-T)	SELV
FXS (ODP P/N's)	TNV-3
FXS	TNV-2

TNV-3: Circuit whose normal operating voltages exceeds the limits for an SELV circuit under normal operating conditions and on which over voltages from Telecommunication Networks are possible.

TNV-2: Circuit whose normal operating voltages exceeds the limits for an SELV circuit under normal operating conditions and is not subjected to over voltages from Telecommunication Networks.

SELV: Safety extra low voltage circuit.

Safety Notice

Installation and service of this unit must only be performed by authorized, qualified service personnel.

The protective earth terminal on the back of the MP-1xx must be permanently connected to protective earth.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

20.2 Appendix - Regulatory Information - MP-1xx/FXO

<i>Declaration of Conformity</i>	
Application of Council Directives:	73/23/EEC (including amendments), 89/336/EEC (including amendments), 1999/5/EC Annex-II of the Directive
Standards to which Conformity is Declared:	EN55022: 1998, Class B EN55024:1998 EN61000-3-2: 1995 (including amendments A1: 1998, A2: 1998, A14: 2000) EN61000-3-3: 1995 EN60950: 2000 TBR-21: 1998
Manufacturer's Name:	AudioCodes Ltd.
Manufacturer's Address:	1 Hayarden Street, Airport City, Lod 70151, Israel.
Type of Equipment:	Analog VoIP System.
Model Numbers:	MP-1xx/FXO (xx- may represent 02, 04, 08)
I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards.	
 _____ <i>Signature</i>	11 th February 2005 _____ <i>Date (Day/Month/Year)</i>
	Airport City, Lod, Israel _____ <i>Location</i>
I. Zusmanovich, Compliance Engineering Manager	

Czech	[AudioCodes Ltd] tímto prohlašuje, že tento [MP-1xx/FXO] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES."
Danish	Undertegnede [AudioCodes Ltd] erklærer herved, at følgende udstyr [MP-1xx/FXO] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
Dutch	Hierbij verklaart [AudioCodes Ltd] dat het toestel [MP-1xx/FXO] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG
English	Hereby, [AudioCodes Ltd], declares that this [MP-1xx/FXO] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Estonian	Käesolevaga kinnitab [AudioCodes Ltd] seadme [MP-1xx/FXO] vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish	[AudioCodes Ltd] vakuuttaa täten että [MP-1xx/FXO] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French	Par la présente [AudioCodes Ltd] déclare que l'appareil [MP-1xx/FXO] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE
German	Hiermit erkläre [AudioCodes Ltd], dass sich dieser/diese/dieses [MP-1xx/FXO] in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW)
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [AudioCodes Ltd] ΔΗΛΩΝΕΙ ΟΤΙ [MP-1xx/FXO] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ
Hungarian	Alulírott, [AudioCodes Ltd] nyilatkozom, hogy a [MP-1xx/FXO] megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak
Icelandic	æki þetta er í samræmi við tilskipun Evrópusambandsins 1999/5
Italian	Con la presente [AudioCodes Ltd] dichiara che questo [MP-1xx/FXO] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latvian	Ar šo [AudioCodes Ltd] deklarē, ka [MP-1xx/FXO] atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.

Lithuanian	[AudioCodes Ltd] deklaruoja, kad irenginys [MP-1xx/FXO] tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas sios direktyvos nuostatas
Maltese	Hawnhekk, [AudioCodes Ltd], jiddikjara li dan [MP-1xx/FXO] jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
Norwegian	Dette produktet er i samhørighet med det Europeiske Direktiv 1999/5
Polish	[AudioCodes Ltd], deklarujemy z pełna odpowiedzialnością, że wyrób [MP-1xx/FXO] spełnia podstawowe wymagania i odpowiada warunkom zawartym w dyrektywie 1999/5/EC
Portuguese	[AudioCodes Ltd] declara que este [MP-1xx/FXO] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovak	[AudioCodes Ltd] týmto vyhlasuje, že [MP-1xx/FXO] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Slovene	Šiuo [AudioCodes Ltd] deklaruoja, kad šis [MP-1xx/FXO] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Spanish	Por medio de la presente [AudioCodes Ltd] declara que el [MP-1xx/FXO] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Swedish	Härmed intygar [AudioCodes Ltd] att denna [MP-1xx/FXO] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Safety Notice

Installation and service of this unit must only be performed by authorized, qualified service personnel.

The protective earth terminal on the back of the MP-1xx must be permanently connected to protective earth.

Network Compatibility

The products support the Telecom networks in EU that comply with TBR21.

Industry Canada Notice

This equipment meets the applicable Industry Canada Terminal Equipment technical specifications. This is confirmed by the registration numbers. The abbreviation, IC, before the registration number signifies that registration was performed based on a declaration of conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

FXO Only: The Ringer Equivalence Number (REN) for this terminal is 0.5. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of Ringer Equivalence Number of all devices do not exceed five.

Telecommunication Safety

The safety status of each port is declared and detailed in the table below:

Ports	Safety Status
Ethernet (100 Base-T)	SELV
FXO	TNV-3

TNV-3: Circuit whose normal operating voltages exceeds the limits for an SELV circuit under normal operating conditions and on which over voltages from Telecommunication Networks are possible.

SELV: Safety extra low voltage circuit.

MP-1xx FXO Notice

The MP-1xx FXO Output Tones and DTMF level should not exceed -9 dBm (AudioCodes setting #23) in order to comply with FCC 68, TIA/EIA/IS-968 and TBR-21.

The maximum allowed gain between any 2 ports connected to the PSTN should be set to 0 dB in order to comply with FCC 68, TIA/EIA/IS-968 Signal power limitation

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

20.3 Appendix - Regulatory Information - MP-1xx/FXS

<i>Declaration of Conformity</i>	
Application of Council Directives:	73/23/EEC (including amendments), 89/336/EEC (including amendments),
Standards to which Conformity is Declared:	EN55022: 1998, Class B EN55024:1998 EN61000-3-2: 1995 EN60950: 2000 (including amendments A1: 1998, A2: 1998, A14: 2000) EN61000-3-3: 1995
Manufacturer's Name:	AudioCodes Ltd.
Manufacturer's Address:	1 Hayarden Street, Airport City, Lod 70151, Israel.
Type of Equipment:	Analog VoIP System.
Model Numbers:	MP-1xx/FXS (xx- may represent 02,04,08)
I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards.	
	11 th February, 2005 Airport City, Lod, Israel
<i>Signature</i> I. Zusmanovich, Compliance Engineering Manager	<i>Date (Day/Month/Year)</i> <i>Location</i>

Czech	[AudioCodes Ltd] tímto prohlašuje, že tento [MP-1xx/FXS series] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 89/336/EEC, 73/23/EEC.
Danish	Undertegnede [AudioCodes Ltd] erklærer herved, at følgende udstyr [MP-1xx/FXS Series] overholder de væsentlige krav og øvrige relevante krav i direktiv 89/336/EEC, 73/23/EEC.
Dutch	Hierbij verklaart [AudioCodes Ltd] dat het toestel [MP-1xx/FXS Series] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 89/336/EEC, 73/23/EEC
English	Hereby, [AudioCodes Ltd], declares that this [MP-1xx/FXS Series] is in compliance with the essential requirements and other relevant provisions of Directive 89/336/EEC, 73/23/EEC.
Estonian	Käesolevaga kinnitab [AudioCodes Ltd] seadme [MP-1xx/FXS Series] vastavust direktiivi 89/336/EEC, 73/23/EEC põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish	[AudioCodes Ltd] vakuuttaa täten että [MP-1xx/FXS Series] tyypinen laite on direktiivin 89/336/EEC, 73/23/EEC oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French	Par la présente [AudioCodes Ltd] déclare que l'appareil [MP-1xx/FXS Series] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 89/336/EEC, 73/23/EEC
German	Hiermit erkläre [AudioCodes Ltd], dass sich dieser/diese/dieses [MP-1xx/FXS Series] in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 89/336/EEC, 73/23/EEC befindet". (BMW)
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [AudioCodes Ltd] ΔΗΛΩΝΕΙ ΟΤΙ [MP-1xx/FXS Series] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 89/336/EEC, 73/23/EEC
Hungarian	Alulírott, [AudioCodes Ltd] nyilatkozom, hogy a [MP-1xx/FXS Series] megfelel a vonatkozó alapvető követelményeknek és az 89/336/EEC, 73/23/EEC irányelv egyéb előírásainak
Icelandic	æki þetta er í samræmi við tilskipun Evrópusambandsins 89/336/EEC, 73/23/EEC
Italian	Con la presente [AudioCodes Ltd] dichiara che questo [MP-1xx/FXS Series] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 89/336/EEC, 73/23/EEC.
Latvian	Ar šo [AudioCodes Ltd] deklarē, ka [MP-1xx/FXS Series] atbilst Direktīvas 89/336/EEC, 73/23/EEC būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian	[AudioCodes Ltd] deklaruoja, kad irenginys [MP-1xx/FXS Series] tenkina 89/336/EEC, 73/23/EEC Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas
Maltese	Hawnhekk, [AudioCodes Ltd], jiddikjara li dan [MP-1xx/FXS Series] jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 89/336/EEC, 73/23/EEC
Norwegian	Dette produktet er i samhörighet med det Europeiske Direktiv 89/336/EEC, 73/23/EEC
Polish	[AudioCodes Ltd], deklarujemy z pełną odpowiedzialnością, że wyrób [MP-1xx/FXS Series] spełnia podstawowe wymagania i odpowiada warunkom zawartym w dyrektywie 89/336/EEC, 73/23/EEC

Portuguese	[AudioCodes Ltd] declara que este [MP-1xx/FXS Series] está conforme com os requisitos essenciais e outras disposições da Directiva 89/336/EEC, 73/23/EEC.
Slovak	[AudioCodes Ltd] týmto vyhlasuje, že [MP-1xx/FXS Series] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 89/336/EEC, 73/23/EEC.
Slovene	Šiuo [AudioCodes Ltd] deklaruoja, kad šis [MP-1xx/FXS Series] atitinka esminius reikalavimus ir kitas 89/336/EEC, 73/23/EEC Direktyvos nuostatas.
Spanish	Por medio de la presente [AudioCodes Ltd] declara que el [MP-1xx/FXS Series] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 89/336/EEC, 73/23/EEC
Swedish	Härmed intygar [AudioCodes Ltd] att denna [MP-1xx/FXS Series] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 89/336/EEC, 73/23/EEC.

Safety Notices

Installation and service of this card must only be performed by authorized, qualified service personnel.
The protective earth terminal on the back of the MP-1xx must be permanently connected to protective earth.

Telecommunication Safety

The safety status of each port is declared and detailed in the table below:

Ports	Safety Status
Ethernet (100 Base-T)	SELV
FXS (ODP P/N's)	TNV-3
FXS	TNV-2

TNV-3: Circuit whose normal operating voltages exceeds the limits for an SELV circuit under normal operating conditions and on which over voltages from Telecommunication Networks are possible.

TNV-2: Circuit whose normal operating voltages exceeds the limits for an SELV circuit under normal operating conditions and is not subjected to over voltages from Telecommunication Networks.

SELV: Safety extra low voltage circuit.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

20.4 Appendix - Regulatory Information - MP-124/FXS

<i>Declaration of Conformity</i>	
Application of Council Directives:	73/23/EEC (including amendments), 89/336/EEC (including amendments),
Standards to which Conformity is Declared:	EN55022: 1998, Class A EN55024:1998 EN61000-3-2: 1995 (including amendments A1: 1998, A2: 1998, A14: 2000) EN61000-3-3: 1995 EN60950: 1992 Including amendments 1,2,3,4 and 11
Manufacturer's Name:	AudioCodes Ltd.
Manufacturer's Address:	1 Hayarden Street, Airport City, Lod 70151, Israel.
Type of Equipment:	Analog VoIP System.
Model Numbers:	MP-124/FXS
I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards.	
	11 th February, 2005 Airport City, Lod, Israel
<i>Signature</i> I. Zusmanovich, Compliance Engineering Manager	<i>Date (Day/Month/Year)</i> <i>Location</i>

Czech	[AudioCodes Ltd] tímto prohlašuje, že tento [MP-124] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 89/336/EEC, 73/23/EEC.
Danish	Undertegnede [AudioCodes Ltd] erklærer herved, at følgende udstyr [MP-124] overholder de væsentlige krav og øvrige relevante krav i direktiv 89/336/EEC, 73/23/EEC.
Dutch	Hierbij verklaart [AudioCodes Ltd] dat het toestel [MP-124] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 89/336/EEC, 73/23/EEC
English	Hereby, [AudioCodes Ltd], declares that this [MP-124] is in compliance with the essential requirements and other relevant provisions of Directive 89/336/EEC, 73/23/EEC.
Estonian	Käesolevaga kinnitab [AudioCodes Ltd] seadme [MP-124] vastavust direktiivi 89/336/EEC, 73/23/EEC põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Finnish	[AudioCodes Ltd] vakuuttaa täten että [MP-124] tyypinen laite on direktiivin 89/336/EEC, 73/23/EEC oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
French	Par la présente [AudioCodes Ltd] déclare que l'appareil [MP-124] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 89/336/EEC, 73/23/EEC
German	Hiermit erkläre [AudioCodes Ltd], dass sich dieser/diese/dieses [MP-124] in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 89/336/EEC, 73/23/EEC befindet". (BMW)
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [AudioCodes Ltd] ΔΗΛΩΝΕΙ ΟΤΙ [MP-124] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 89/336/EEC, 73/23/EEC
Hungarian	Alulírott, [AudioCodes Ltd] nyilatkozom, hogy a [MP-124] megfelel a vonatkozó alapvető követelményeknek és az 89/336/EEC, 73/23/EEC irányelv egyéb előírásainak
Icelandic	æki þetta er í samræmi við tilskipun Evrópusambandsins 89/336/EEC, 73/23/EEC
Italian	Con la presente [AudioCodes Ltd] dichiara che questo [MP-124] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 89/336/EEC, 73/23/EEC.
Latvian	Ar šo [AudioCodes Ltd] deklarē, ka [MP-124] atbilst Direktīvas 89/336/EEC, 73/23/EEC būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lithuanian	[AudioCodes Ltd] deklaruoja, kad irenginys [MP-124] tenkina 89/336/EEC, 73/23/EEC Direktyvos esminius reikalavimus ir kitas sios direktyvos nuostatas
Maltese	Hawnhekk, [AudioCodes Ltd], jiddikjara li dan [MP-124] jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 89/336/EEC, 73/23/EEC
Norwegian	Dette produktet er i samhörighet med det Europeiske Direktiv 89/336/EEC, 73/23/EEC
Polish	[AudioCodes Ltd], deklarujemy z pełną odpowiedzialnością, że wyrób [MP-124] spełnia podstawowe wymagania i odpowiada warunkom zawartym w dyrektywie 89/336/EEC, 73/23/EEC

Portuguese	[AudioCodes Ltd] declara que este [MP-124] está conforme com os requisitos essenciais e outras disposições da Directiva 89/336/EEC, 73/23/EEC.
Slovak	[AudioCodes Ltd] týmto vyhlasuje, že [MP-124 Series] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 89/336/EEC, 73/23/EEC.
Slovene	Šiuo [AudioCodes Ltd] deklaruoja, kad šis [MP-124 Series] atitinka esminius reikalavimus ir kitas 89/336/EEC, 73/23/EEC Direktyvos nuostatas.
Spanish	Por medio de la presente [AudioCodes Ltd] declara que el [MP-124 Series] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 89/336/EEC, 73/23/EEC
Swedish	Härmed intygar [AudioCodes Ltd] att denna [MP-124 Series] står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 89/336/EEC, 73/23/EEC.

Safety Notices

**Installation and service of this card must only be performed by authorized, qualified service personnel.
The protective earth terminal on the back of the MP-1xx must be permanently connected to protective earth.**

Telecommunication Safety

The safety status of each port is declared and detailed in the table below:

Ports	Safety Status
Ethernet (100 Base-T)	SELV
FXS (ODP P/N's)	TNV-3
FXS	TNV-2

TNV-3: Circuit whose normal operating voltages exceeds the limits for an SELV circuit under normal operating conditions and on which over voltages from Telecommunication Networks are possible.

TNV-2: Circuit whose normal operating voltages exceeds the limits for an SELV circuit under normal operating conditions and is not subjected to over voltages from Telecommunication Networks.

SELV: Safety extra low voltage circuit.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

21 List of Abbreviations

Table 21-1: List of Abbreviations

Abbreviation	Meaning
AAL2	ATM Adaptation Layer 2
ADPCM	Adaptive Differential PCM - voice compression
AIS	Alarm Indication Signal
ASN.1	Abstract Syntax Notation
ATM	Asynchronous Transfer Mode
A-law	European Compander Functionality Rule (see μ -law)
bps	Bits per second
BLES	Broadband Loop Emulation Service by the DSL Forum
BRI	Basic Rate Interface in ISDN
CAS	Channel Associated Signaling
cPCI	Compact PCI (Industry Standard)
COLP	Connected Line Identity Presentation
COLR	Connected Line Identity Restriction
DHCP	Dynamic Host Control Protocol
DID	Direct Inward Dial
DS1	1.544 Mbps USA Digital Transmission System (see E1 and T1)
DS3	44.736 Mbps USA Digital Transmission System, Encapsulates 28 T1 streams, also called T3
DSL	Digital Subscriber Line
DSP	Digital Signal Processor (or Processing)
DTMF	Dual Tone Multiple Frequency (Touch Tone)
E1	2.048 Mbps European Digital Transmission System (see T1)
E-ADPCM	Enhanced ADPCM
ETSI	European Telecommunications Standards Institute
FR	Frame Relay
GK	Gatekeeper

Table 21-1: List of Abbreviations

Abbreviation	Meaning
GW	Gateway
G.xxx	An ITU Standard - see References section for details
H.323	A range of protocol standards for IP-based networks
H.323 Entity	Any H.323 Component
IE	Information Element (ISDN layer 3 protocol, basic building block)
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPmedia	AudioCodes series of VoIP Media Processing Boards
IPM-260	AudioCodes IPmedia PCI VoIP Media Processing Board, to 120 ports
IPM-1610	AudioCodes IPmedia cPCI VoIP Media Processing Board, to 240 ports
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ITU	International Telecommunications Union
ITU-T	Telecommunications section of the ITU
IVR	Interactive Voice Response
Jitter	Variation of interpacket timing interval
kbps	Thousand bits per second
LAPD	Line Access Protocol for the D-channel
LFA	Loss of Frame Alignment
LOF	Loss of Frame
Mbps	Million bits per second
MCU	Multipoint Control Unit (H.323)
Mediant	AudioCodes series of Voice over Packet Media Gateways
Mediant for Broadband	AudioCodes series of Broadband Access Gateways, including Cable and V5.2 Access Gateways
MEGACO	Media Gateway Control (Protocol, H.248)
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MP-102 & MP-112	AudioCodes 2-port Analog MediaPack Media Gateway

Table 21-1: List of Abbreviations

Abbreviation	Meaning
MP-104 & MP-114	AudioCodes 4-port Analog MediaPack Media Gateway
MP-108 & MP-118	AudioCodes 8-port Analog MediaPack Media Gateway
MP-124	AudioCodes 24-port Analog MediaPack Media Gateway
ms or msec	Millisecond; a thousandth part of a second
MVIP	Multi Vendor Integration Protocol
NetCoder	AudioCodes Proprietary High Quality, Speech Coder
NIC	Network Interface Card
OSI	Open Systems Interconnection (Industry Standard)
PCI	Personal Computer Interface (Industry Standard)
PCM	Pulse Code Modulation
PDU	Protocol Data Unit
POTS	Plain Old Telephone System or Service
PRI	Primary Rate Interface in ISDN
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAI	Remote Alarm Indication
RAS	Registration, Admission, and Status (control within H.323).
RDK	Reference Design Kit.
RFC	Request for Comment issued by IETF.
RTCP	Real Time Control Protocol.
RTP	Real Time Protocol.
SB-1610	AudioCodes TrunkPack VoIP/ TP-1610 cPCI media streaming board, to 480 ports for Wireless systems
ScBus	Signal Computing Bus - part of SCSA
SCSA	Signal Computing System Architecture
SDK	Software Development Kit
SNMP	Simple Network Management Protocol
Stretto	AudioCodes series of Voice over Wireless Media Gateways
TCP	Transmission Control Protocol.

Table 21-1: List of Abbreviations

Abbreviation	Meaning
TCP/IP	Transmission Control Protocol/Internet Protocol.
TFTP	Trivial File Transfer Protocol.
TPNCP	AudioCodes TrunkPack Network Control Protocol.
TP-260	AudioCodes TrunkPack VoIP/260 Voice over IP PCI media streaming board, up to 128 ports
TP-2810	AudioCodes TrunkPack VoIP/2810 cPCI media streaming board, to 672 ports
TP-1610	AudioCodes TrunkPack VoIP/1610 cPCI media streaming board, to 480 ports
TPM-1100	AudioCodes TrunkPack Module
TrunkPack	AudioCodes series of voice compression boards
T1	1.544 Mbps USA Digital Transmission System (see E1 and DS1)
T3	45 Mbps USA Digital Transmission System, Encapsulates 28 T1 streams, Also called DS3
UDP	User Datagram Protocol
VCC	Virtual Channel Connection
VoAAL2	Voice over AAL2 (see above)
VoATM	Voice over Asynchronous Transfer Mode
VoDSL	Voice over Digital Subscriber Line
VoFR	Voice over Frame Relay
VoIP	Voice over Internet Protocol
VoP	Voice over Packet(s)
VoPN	Voice over Packet Networks
VPN	Virtual Private Network
μ -law	American Compander Functionality Rule, (see A-law)
μ s or μ sec	microsecond; a millionth part of a second

22 Index

A

About SNMP99
 About the Web Interface Screen119, 280
 About this Software287
 Accessing the Embedded Web Server.....117,
 118, 120, 280, 282
 Administrative State Control114
 Advanced Configuration127
 Advanced Configuration Screen. 127, 237, 241
 Alarm Traps273
 Analog Parameters214
 Appendix - BootP/TFTP Server51, 73, 76, 117,
 148, 169, 170, 174, 175, 185, 281, 283
 Appendix - Call Progress Tones Wizard287
 Appendix - Customizing the Web Interface.279
 Appendix - DTMF, Fax and Modem Transport
 Modes233
 Appendix - Individual ini File Parameters51,
 53, 125, 126, 127, 129, 130, 138, 141, 142,
 143, 195
 Appendix - MGCP Compliance257
 Appendix - Regulatory Information295
 Appendix - Regulatory Information - MP-
 11x/FXS295
 Appendix - Regulatory Information - MP-
 1xx/FXO 298, 301, 303
 Appendix - RTP/RTCP Payload Types .86, 229
 Appendix - Security 106, 117, 237
 Appendix - SNMP Traps.....105, 273
 Appendix - Utilities.. 58, 73, 106, 144, 146, 245
 Automatic Update Facility70
 Auxiliary Files58
 Auxiliary Files Download 73, 115, 155, 161

B

Backup Copies of ini and Auxiliary Files76
 Basic Configuration123
 Boot Firmware & Operational Firmware45
 BootP/TFTP Server Installation186

C

Call Progress Tones, User-Defined Tones and
 Distinctive Ringing59
 Carrier-Grade Alarm System101
 Change Password 116, 128, 147
 Changing the Networking Parameters168
 Channel Configuration126
 Channel Status149
 Client Certificates239
 Client Configuration Screen.....187, 191

Cold Start Trap..... 102
 Company & Product Bar Components..... 279
 Component
 AlarmManager#0 274
 Board#<n> 273
 EthernetLink#0..... 275
 Configuration File..... 128, 144, 166
 Configuration Parameters and Files 45, 48
 Configuring Fax Relay Mode 233
 Configuring Fax/Modem ByPass Mode 234
 Configuring Fax/Modem Bypass NSE mode
 234
 Configuring RADIUS Support 241
 Control Protocol Reports 176
 Converting a CPT ini File to a Binary dat File
 246
 Converting a Modified CPT ini File to a dat File
 with the Download Conversion Utility..... 73
 Correlating PC / MediaPack IP Address &
 Subnet Mask 117, 121
 Customizing the Product Name 279, 283
 Customizing the Web Browser Title Bar 284

D

Default Dynamic Payload Types Which are Not
 Voice Coders 230
 Default RTP/RTCP/T.38 Port Allocation 230
 Determining MediaPack Initialization Problems
 169
 Device Information 154
 Diagnostics & Troubleshooting 167
 Diagnostics Overview 167
 Downloading Auxiliary Files 51, 58
 DTMF/MF Relay Settings 233

E

Embedded Web Server 45, 51, 99, 115, 174
 Embedded Web Server Protection & Security
 Mechanisms 115
 Encoding Mechanism 58

F

Fax Transport Type Setting with Local
 Connection Options..... 80, 85
 Fax/Modem Settings 233

G

General Parameters..... 125
 Generating CAS Protocol Configuration Files
 250
 Generating Prerecorded Tones Files..... 252
 Generating Voice Prompts Files 247
 Getting Acquainted with the Web Interface 119
 Graceful Shutdown 114

I

Individual ini File Parameters	195
Infrastructure Parameters.....	140, 195, 199
Initial Settings	287
Initialization (ini) Files	51, 59, 254
Installation	287
Introduction.....	185

K

Key Features	185
--------------------	-----

L

LED Indicators	169, 172
Legal Notice.....	244
Limiting the Embedded Web Server to Read- Only Mode.....	116
List of Abbreviations	305
Log Traps (Notifications)	276
Logging Screen	186

M

Main Screen	186, 188
Media Processing Parameters	195, 205
MediaPack Distinctive Ringing Mechanism...	79
MediaPack Front Panel	172
MediaPack Rear Panel.....	172
Message Log	153, 175
MGCP Coder Negotiation.....	86
MGCP Compliance Matrix.....	257
MGCP Error Conditions.....	176
MGCP FAX	80
MGCP KeepAlive Mechanism	78
MGCP Profiling.....	80, 85
MGCP Tester Utility	255
MGCP-Specific Parameters	124, 195, 223
Modifying ini File Parameters via the Web Interface's AdminPage.....	282, 283, 284
Modifying the Call Progress Tones File & Distinctive Ringing File.....	72, 79, 146, 246
MP-11x Self-Testing	172
MP-11x Visual Front Panel LED Indicators .	172

N

Network Port Usage	242
NEW **** Downloading the dat File to a Device MediaPack	74
Node Maintenance	114
NUM-LIST***Converting a CPT ini File to a Binary dat File	62, 146

O

Operating the Syslog Server	174
Other Traps	277

P

Parameter = Value Construct.....	52
----------------------------------	----

Parameters Common to All Control Protocols	195, 218
Payload Types Defined in RFC 3551	229
Payload Types Not Defined in RFC 3551...	230
Performance Measurements for a Third-Party System	102
Playing Prerecorded Tones (PRT).....	73
Preferences Screen	186, 187, 190, 192
Protocol Management.....	122
Protocol Selection.....	123

R

RADIUS Support.....	240
Recommended Practices.....	243
Recording Dialog – Automatic Mode	289
Recording Dialog – Manual Mode	291
Regional Settings.....	128, 145
Reinitializing the MediaPack.....	51, 169
Reinitializing the MP-11x	172
Replacing the Background Image File	279, 282
Replacing the Main Corporate Logo ..	279, 280, 284
Replacing the Main Corporate Logo with a Text String	282
Replacing the Main Corporate Logo with an Image File.....	280
Reset Button	123, 155, 162, 163, 164
Restoring and Backing Up the Device Configuration	144, 165

S

Save Configuration	115, 163, 175
Saving Changes.....	120
Screen Details.....	188
SDP Support in MGCP	79
Secure Telnet.....	238
Secured Configuration File Download	58
Selected Technical Specifications	179
Server Certificate Replacement.....	238
Setting Up a RADIUS Server.....	240
SNMP Interface Details	106
SNMP NAT Traversal	113
SNMP Parameters	195, 226
SNMP Traps	177
Software Update	155, 255
Software Upgrade Wizard	74, 75, 76, 115, 155, 280, 281, 283
Solutions to Possible General Problems	177
Solutions to Possible Problems	177
Solutions to Possible Voice Problems	177
Specifications.....	185
SSL/TLS.....	237
Status and Diagnostic Menu.....	115, 148
Supporting V.34 Faxes	235
Syslog	173
System Parameters	195

T

Tables of Parameter Value Construct	53
Template Screen	188
Templates Screen	188, 192
TGCP Compatibility	85
The Call Progress Tone ini File	292
The Embedded Web Server's 'Message Log' (Integral Syslog).....	175
Trap Varbinds	278
Troubleshooting MediaPack Devices via the RS-232 Port	168
Trunk Settings	144
TrunkPack Downloadable Conversion Utility	59, 245
TrunkPack-VoP Series Supported MIBs - ALL	103

U

Upgrading MediaPack Software	50, 58, 76
Using BootP/DHCP	45, 51
Using Bypass Mechanism for V.34 Fax Transmission:.....	235
Using DNS with MGCP.....	78
Using Events Only Mechanism for V.34 Fax Transmission.....	235
Using Internet Explorer to Access the Embedded Web Server.....	118
Using Relay Mode for Various Fax Machines (T.30 and V.34)	236
Using the Secure Web Server	237

V

Viewing the Gateway's Information	168
---	-----

W

Web Server Configuration	237
--------------------------------	-----

MGCP**MP-1xx Series & MP-11x Series**

User's Manual 4.6