AudioCodes™ CPE & Access Analog Gateways

H.323

MediaPack™ MP-124 & MP-11x

Release Notes Version 5.0

Document #: LTRT-65209

December 2006

Table of Contents

List of Tables

Notices

Notice

This document describes the release of the AudioCodes MediaPack Analog Series MP-124 24 port, MP-118 8-port, MP-114 4-port and MP-112 2-port.

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 www.audiocodes.com under Support / Product Documentation.

Date Published: Dec-07-2006 Date Printed: Dec-10-2006

Tip: 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.

WEEE EU Directive

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

Customer Support

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

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used, and only Industry standard terms are used throughout this manual. The symbol 0x indicates hexadecimal notation.

Related Documentation

Document #	Manual Name
LTRT-651xx (e.g., LTRT-65101)	MP-11x & MP-124 H.323 User's Manual
LTRT-598xx	MP-11x & MP-124 MGCP-H.323-SIP Fast Track Guide

Notes:

- MediaPack refers to the MP-124, MP-118, MP-114, and MP-112 VoIP gateways.
- MP-11x refers to the MP-118, MP-114,and MP-112 VoIP gateways.

Note: These Release Notes describe the MP-124, MP-118, MP-114, and MP-112 MediaPack series analog VoIP H.323 gateways. Unless otherwise specified, whenever reference is made to the MediaPack in these Release Notes, it automatically includes all these MediaPack products.

1 What's New in Release 5.0

Note: This document uses a one-row table convention to indicate for which products each feature is applicable. The products that do not support the feature are shaded (grayed). In the example below, the feature would be applicable only to MP-114/MP-118.

MP-112	MP-114/MP-118	MP-124	FXS	FXO

1.1 Supported Hardware Platforms

1.1.1 New Hardware Platforms Introduced in this Release

The following hardware platform is introduced in this version:

- MP-114/FXS+FXO with 2 FXS ports and 2 FXO ports. This product also contains a relay that connects the FXS ports to the FXO ports in case of power failure.

1.1.2 Support for Existing Hardware Platforms

- MediaPack MP-118/FXS+FXO with 4 FXS ports and 4 FXO ports
- MediaPack MP-11x/FXS, 2 to 8 analog FXS interfaces, with enhanced CPU resources:
  - MediaPack MP-118/FXS, 8 analog FXS interfaces
  - MediaPack MP-114/FXS, 4 analog FXS interfaces
  - MediaPack MP-112/FXS, 2 analog FXS interfaces
- MediaPack MP-124/FXS, 24 analog FXS interfaces

1.1.3 Hardware Platforms No Longer Supported

N/A.

1.2 General Gateway New Features

1. **Supports separate interfaces for management and control/bearer:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway can now be configured to operate in Dual IP mode by assigning the same IP address to two traffic types.

When operating with multiple IP interfaces, the gateway splits the traffic into three types: Management (OAM), Control, and Media. Each interface has its own IP and subnet address.

The Dual IP mode option allows the gateway to distinguish between only two traffic types, based on IP address. One of the traffic types consists of a combination of two traffic types (Media and Control, OAM and Control, or OAM and Media), while the other is whichever traffic type excluded in this combination. Therefore, in the Dual IP mode, the same IP address is assigned to two traffic types.

2. **Disable LCP Echos and Link disconnection auto-detection support:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now allows the user to disable the Point-to-Point Protocol over Ethernet (PPPoE) disconnection auto-detection feature.

By default, the PPPoE Client (embedded on the gateway's software), sends Link Configuration Protocol (LCP) Echo packets to the server to check that the PPPoE connection is open. Some Access Concentrators don't reply to these LCP Echo requests, resulting in a disconnection. By disabling the LCP disconnection auto-detection feature, the PPPoE Client doesn't send LCP Echo packets to the server (and does not detect PPPoE disconnections).

Relevant parameter: PPPoELCPEchoEnable.

3. **IPSec AES support:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports Advanced Encryption Standard (AES) for IPSec/IKE tables.

Relevant parameters: IKEPolicyProposalEncryption_X; IPSecPolicyProposalEncryption_X.

4. **T.38 packet duplication as No-Op packet (for NAT):**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

To enable Network Address Translator (NAT) port binding for T.38 streams, the gateway now supports the sending of T.38 redundant packets to the remote side (including during silence periods), per user-defined interval (in seconds).

Relevant parameters: NoOperationSendingMode; NoOpInterval.

5. **Jitter buffer defaults changed to 10 msec:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The default values for the Jitter Buffer DJBufMinDelay and DJBufOptFactor *ini* file parameters have been changed to 10 msec.

Relevant parameters: DJBufMinDelay; DJBufOptFactor.

6. Syslog server port definition support:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now allows the user to define the port of the Syslog server. When no port is defined, the default port of 514 is used.

Relevant parameter: SyslogServerPort.

7. HangOver time setting after muting DTMF or MF from Tel /PSTN:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now allows the user to define the HangOver time, which is the voice silence time (in msec) after muting DTMF or MF digits (received from the Tel / PSTN side) before sending to the IP side.

Relevant parameter: TxDTMFHangOverTime.

8. HangOver time setting after playing DTMF or MF from IP network:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now allows the user to define the HangOver time, which is the voice silence time (in msec) after playing DTMF or MF digits (received as Relay from the IP side) to the Tel / PSTN side.

Relevant parameter: RxDTMFHangOverTime.

9. IP addresses support the asterisk ('*') wildcard:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The asterisk ('*') wildcard can now be included in IP addresses. IP addresses that are defined in the Routing tables and Manipulation tables can include the '*' wildcard, which represents any valid value from 0 to 255.

For example, 10.8.8.* represents IP addresses from 10.8.8.0 to 10.8.8.255; 10.8.*.* represents IP addresses from 10.8.0.0 to 10.8.255.255.

Relevant parameters: Prefix; PSTNPrefix; NumberMapIP2Tel; SourceNumberMapIP2Tel.

10. Additional option for Channel Selection algorithm:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

An additional option ('By Source Phone Number') was added to the channel selection algorithm (in addition to the existing 'By Destination Phone Number' option).

Relevant parameters: ChannelSelectMode; TrunkGroupSettings.

11. Supports sending of CDR on call connect:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway can now send a call data record (CDR) when a call is connected (in addition to when the call ends).

Relevant parameter: CDRReportLevel.

12. **Supports Call Forward Indication to user:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

When a phone on an FXS port goes off-hook to make a call, the gateway typically plays a regular dial tone for a period of time, indicating that the user can dial digits. If this port has Call Forwarding active, the user needs to be aware that any calls made to their directory number (DN) are not sent to their phone. To notify users of the call forwarding status, this Call Forward Indication feature plays a stutter dial tone instead of the regular dial tone. This indicates to the user that to receive calls, the user needs to disable call forwarding.

Relevant parameter: StutterToneDuration.

13. **Supports defining of Off-Hook Warning Tone duration:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

It is now possible to set the duration for which the Off-Hook Warning Tone is played.

Relevant parameter: WarningToneDuration.

14. **Support for defining number of rings before FXO answers:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

It is now possible to define the number of rings before the FXO gateway answers a call.

Relevant parameter: FXONumberOfRings.

1.3 H.323 New Features

1. **Hook-Flash Code to IP support:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

When the gateway detects a Hook-Flash event from the Tel side, a digit pattern is sent to the IP side [instead of the exclamation ('!') character]. All methods are supported: H.245 User Input, Q.931 Info, or H.245 Signal. When this pattern is detected from the IP side, a Hook-Flash is generated towards the Tel side.

Relevant parameter: HookFlashCodeIP.

1.4 Web and SNMP New Features

1. **Supports Graceful/Forced Lock and Reset:**

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway now supports a lock/unlock mechanism. The user can select one of the following options:

- Graceful Lock: the gateway rejects all incoming calls. All existing calls are allowed to continue until a user-defined lock timer expires. When this timer expires, the gateway disconnects the calls. At this point, the gateway remains in an idle state.
- Forced Lock: the gateway rejects all incoming calls and all existing calls are disconnected. At this point the gateway remains in an idle state.
- Unlock: the gateway returns from Lock state to normal state and accepts incoming calls from Tel and IP sides.

- Graceful Reset: similar behavior as Graceful Lock except that when all calls are disconnected, the gateway performs reset.
- Forced Reset: similar behavior as Forced Lock except that when all calls are disconnected, the gateway performs reset.

2. Supports assigning of free text description for each port:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

This feature allows the assigning of free-text descriptions for each trunk using the gateway's Embedded Web Server.

3. Web Search Engine support:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

The gateway's Embedded Web Server now provides a search engine (**Search** button) for searching any *ini* file parameter that is configurable by the Web server. The search result provides you a brief description of the parameter as well as a link to the relevant screen in which the parameter is configured in the Web server.

The search can be performed for a specific *ini* parameter (e.g., EnableIPSec) or a sub-string of the parameter (e.g., 'sec'). If you search for a sub-string, the Embedded Web Server lists all parameters that contain the searched sub-string in their parameter names.

4. SNMPv3 support:

MP-112	MP-114/MP-118	MP-124	FXS	FXO

In previous releases, it was assumed that customers could use SNMPv2c over IPsec to meet their SNMP security requirements. While SNMP over IPsec is a viable solution for some customers, others however, demand SNMPv3 security. Therefore, in Release 5.0, support for SNMPv3 authentication and privacy has been provided.

This feature allows customers to define up to 10 User-based Security Model (USM) users (USM users are referred to as 'v3 users'). Each v3 user can be associated with an authentication type (none, MD5, or SHA-1) and a privacy type (none, DES, 3DES, or AES).

The customer still has the option for defining up to five read-only community strings and up to five read-write community strings.

Relevant parameters: SNMPUsers_Index; SNMPUsers_Username; SNMPUsers_AuthProtocol; SNMPUsers_PrivProtocol; SNMPUsers_AuthKey; SNMPUsers_PrivKey; SNMPUsers_Group.

1.5 New and Modified Parameters

Table 1-1 describes the new parameters for Release 5.0. Most of the new parameters (described in the table below) can be configured with the *ini* file and by using the Embedded Web Server. Note that only those parameters contained within square brackets are configurable via the Embedded Web Server.

Table 1-1: Release 5.0 New *ini* File [Web] Parameters (continues on pages 12 to 13)

***ini* File [Web Interface] Parameter Name**	**Description**
SyslogServerPort [Syslog Server Port]	Defines the UDP port of the Syslog server. The valid range is 0 to 65,535. The default port value is 514.
NoOperationSendingMode	Enables or disables the transmission of RTP or T.38 No-Op packets. Valid options include: ▪ 0 = Disable (default) ▪ 1 = Enable This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods.
NoOpInterval	Defines the time interval in which RTP or T.38 No-Op packets are sent in the case of silence (no RTP / T.38 traffic) when No-Op packet transmission is enabled. The valid range is 20 to 65,000 msec. The default is 10,000. **Note:** To enable No-Op packet transmission, use the NoOperationSendingMode parameter.
PPPoELCPEchoEnable	Enables or disables the Point-to-Point Protocol over Ethernet (PPPoE) disconnection auto-detection feature. Valid options include: ▪ 0 = Disable ▪ 1 = Enable (default) By default, the PPPoE Client (i.e., embedded in the gateway) sends LCP Echo packets to the server to check that the PPPoE connection is open. Some Access Concentrators (PPPoE servers) don't reply to these LCP Echo requests, resulting in a disconnection. By disabling the LCP disconnection auto-detection feature, the PPPoE Client does not send LCP Echo packets to the server (and does not detect PPPoE disconnections).
RxDTMFHangOverTime	Defines the Voice Silence time (in msec) after playing DTMF or MF digits to the Tel / PSTN side that arrive as Relay from the IP side. The valid range is 0 to 2,000 msec. The default is 1,000 msec.
TxDTMFHangOverTime	Defines the Voice Silence time (in msec units) after detecting the end of DTMF or MF digits at the Tel / PSTN side when the DTMF Transport Type is either Relay or Mute. The Valid range is 0 to 2,000 msec. The default is 100 msec.
SNMPUsers_Index [Index]	SNMP v3 user table index. The valid range is 0 to 9.
SNMPUsers_Username [Username]	Name of the SNMP v3 user. This name must be unique.
SNMPUsers_AuthProtocol [AuthProtocol]	Authentication protocol for the SNMP v3 user. Valid options include: ▪ 0 = None (default) ▪ 1 = MD5 ▪ 2 = SHA-1

Table 1-1: Release 5.0 New *ini* File [Web] Parameters (continues on pages 12 to 13)

***ini* File [Web Interface] Parameter Name**	**Description**
SNMPUsers_PrivProtocol [PrivProtocol]	Privacy protocol for the SNMP v3 user. Valid options include: ▪ 0 = None (default) ▪ 1 = DES ▪ 2 = 3DES ▪ 3 = AES128 ▪ 4 = AES192 ▪ 5 = AES256
SNMPUsers_AuthKey [AuthKey]	Authentication key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
SNMPUsers_PrivKey [PrivKey]	Privacy key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
SNMPUsers_Group [Group]	The group with which the SNMP v3 user is associated. Valid options include: ▪ 0 = Read-only group (default) ▪ 1 = Read-write group ▪ 2 = Trap group **Note:** All groups can be used to send traps.
HookFlashCodeIP [Hook-Flash Code to IP]	Defines a digit pattern that is sent to the IP when the gateway detects a Hook-Flash event from the Tel side. All transport methods are supported: H.245 User Input, Q.931 Info, and H.245 Signal. When this pattern is detected from the IP side, a Hook-Flash is generated towards the Tel side. The valid range is a 25-character string. The default is '!'.
Max Echo Canceller Length [**MaxEchoCancellerLength**]	Maximum Echo Canceller length (in msec). Valid options include: ▪ 0 = based on various internal gateway settings -- 64 msec (default) ▪ 4 = 32 msec ▪ 1 = 64 msec **Note 1:** The gateway must be reset after the value of MaxEchoCancellerLength is changed. **Note 2:** It isn't necessary to configure the parameter EchoCancellerLength as it automatically acquires its value from the parameter MaxEchoCancellerLength.
WarningToneDuration	Defines the duration (in seconds) for which Off-Hook Warning Tone is played to the user. The valid range is -1 to 2,147,483,647 seconds. The default is 600 seconds. **Note:** A negative value indicates that the tone is played indefinitely.
FXONumberOfRings	Defines the number of rings before the FXO gateway answers a call. The valid range is 0 to 255. The default is 0 seconds.

1.6 Modified Parameters

Table 1-2 lists existing parameters that have been modified. Note that only those parameters contained within square brackets are configurable via the Embedded Web Server.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 14 to 19)

ini File [Web Interface] Parameter Name	Description
DJBufMinDelay [Dynamic Jitter Buffer Minimum Delay]	(**Modification:** default value.) Dynamic Jitter Buffer Minimum Delay. The valid range is 0 to 150 msec (default is 10).
DJBufOptFactor [Dynamic Jitter Buffer Optimization Factor]	(**Modification:** default value.) Dynamic Jitter Buffer frame error / delay optimization factor. The valid range is 0 to 13 (default is 10). **Note:** Set to 13 for data (fax and modem) calls.
IKEPolicyProposalEncryption_X [First to Fourth Proposal Encryption Type]	(**Modification:** additional enumeration value for AES support.) Determines the encryption type used in the main mode negotiation for up to four proposals. 'X' denotes the proposal number (0 to 3). Valid options include: ▪ Not Defined (default) ▪ 1 = DES-CBC ▪ 2 = Triple DES-CBC ▪ 3 = AES
IPSecPolicyProposalEncryption_X [First to Fourth Proposal Encryption Type]	(**Modification:** additional enumeration value for AES support.) Determines the encryption type used in the quick mode negotiation for up to four proposals. 'X' denotes the proposal number (0 to 3). Valid options include: ▪ Not Defined (default) ▪ 0 = None (no encryption) ▪ 1 = DES-CBC ▪ 2 = Triple DES-CBC ▪ 3 = AES

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 14 to 19)

ini File [Web Interface] Parameter Name	Description
NumberMapIP2Tel [Destination Phone Number Manipulation Table for IP→Tel calls]	(**Modification:** asterisk ('*') wildcard supported in IP addresses.) Manipulates the destination number for IP-to-Tel calls. The format for NumberMapIP2Tel is as follows: a,b,c,d,e,f,g,h,i Where, ▪ a = Destination number prefix. ▪ b = Number of stripped digits from the left, or (if brackets are used) from the right. A combination of both options is allowed. ▪ c = String to add as prefix, or (if brackets are used) as suffix. A combination of both options is allowed. ▪ d = Number of remaining digits from the right. ▪ e = Not applicable, set to $$. ▪ f = Not applicable, set to $$. ▪ g = Source number prefix. ▪ h = Not applicable, set to $$. ▪ i = Source IP address (obtained from the Setup message). The 'b' to 'd' manipulation rules are applied if the called and calling numbers match the 'a', 'g' and 'i' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign '$$', for example: ▪ NumberMapIP2Tel =01,2,972,$$,$$,$$,034,$$,10.13.77.8 ▪ NumberMapIP2Tel =03,(2),667,$$,$$,$$,22 **Note:** The Source IP address can include wildcards. The 'x' wildcard is used to represent single digits, e.g. 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g. 10.8.8.* represents all the addresses between 10.8.8.0 and 10.8.8.255.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 14 to 19)

ini File [Web Interface] Parameter Name	Description
SourceNumberMapIP2Tel [Source Phone Number Manipulation Table for IP→Tel calls]	(**Modification:** asterisk ('*') wildcard supported in IP addresses.) Manipulates the source number for IP-to-Tel calls. The format for SourceNumberMapIP2Tel is as follows: a,b,c,d,e,f,g,h,i Where, ▪ a = Source number prefix ▪ b = Number of stripped digits from the left, or (if brackets are used) from the right. A combination of both options is allowed. ▪ c = String to add as prefix, or (if brackets are used) as suffix. A combination of both options is allowed. ▪ d = Number of remaining digits from the right ▪ e = Not in use, should be set to $$ ▪ f = Not in use, should be set to $$ ▪ g = Destination number prefix ▪ h = Not in use, should be set to $$ ▪ i = Source IP address The 'b' to 'd' manipulations rules are applied if the called and calling numbers match the 'a', 'g' and 'i' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign '$$', for example: ▪ NumberMapIP2Tel =01,2,972,$$,$$,$$,034 ▪ NumberMapIP2Tel =03,(2),667,$$,$$,$$,22 **Note:** The Source IP address can include wildcards. The 'x' wildcard is used to represent single digits, e.g. 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g. 10.8.8.* represents all the addresses between 10.8.8.0 and 10.8.8.255.
Prefix [Tel to IP Routing Table]	(**Modification:** asterisk ('*') wildcard supported in IP addresses.) Prefix = <Destination Phone Prefix>, <IP Address>,<Src Phone Prefix>,<IP Profile ID>,<Charge Code> For example: ▪ Prefix = 20,10.2.10.2,202,1,15 ▪ Prefix = 10[340-451]xxx#,10.2.10.6,*,1,1 ▪ Prefix = *,gateway.domain.com,*,20 **Note 1:** <destination / source phone prefix> can be single number or a range of numbers. **Note 2:** This parameter can appear up to 50 times. **Note 3:** Parameters can be skipped by using the sign '$$', for example: Prefix = $$,10.2.10.2,202,1 **Note 4:** An optional IP ProfileID (1 to 9) can be applied to each routing rule. **Note 5:** The IP address can include wildcards. The 'x' wildcard is used to represent single digits, e.g. 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g. 10.8.8.* represents all the addresses between 10.8.8.0 and 10.8.8.255.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 14 to 19)

ini File [Web Interface] Parameter Name	Description
PSTNPrefix [IP to Trunk Group Routing Table]	(**Modification:** asterisk ('*') wildcard supported in IP addresses.) The format for PSTNPrefix is as follows: a,b,c,d,e Where, ▪ a = Destination Number Prefix ▪ b = Hunt Group ID ▪ c = Source Number Prefix ▪ d = Source IP address (obtained from the Setup message) ▪ e = IP Profile ID Selection of hunt groups (for IP to Tel calls) is according to destination number, source number and source IP address. **Note 1:** To support the 'in call alternative routing' feature, users can use two entries that support the same call, but assigned it with a different hunt groups. The second entree functions as an alternative selection if the first rule fails as a result of one of the release reasons listed in the AltRouteCauseIP2Tel table. **Note 2:** An optional IP ProfileID (1 to 4) can be applied to each routing rule. **Note 3:** The Source IP Address can include wildcards. The 'x' wildcard represents single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 to 10.8.8.99. The '*' wildcard represents any number between 0 and 255, e.g., 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255. **Note 4:** This parameter can appear up to 24 times.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 14 to 19)

ini File [Web Interface] Parameter Name	Description
ChannelSelectMode [Channel Select Mode]	(**Modification:** additional enumeration value for 'By Source Phone Number' for selecting port.) Defines port allocation algorithm for IP-to-Tel calls. Valid options include: ▪ 0 (By phone number) = Select the gateway port according to the called number (called number is defined in the 'Endpoint Phone Number' table). ▪ 1 (Cyclic Ascending) = Select the next available channel in an ascending cycle order. Always select the next higher channel number in the hunt group. When the gateway reaches the highest channel number in the hunt group, it selects the lowest channel number in the hunt group and then starts ascending again. ▪ 2 (Ascending) = Select the lowest available channel. Always start at the lowest channel number in the hunt group and if that channel is not available, select the next higher channel. ▪ 3 (Cyclic Descending) = Select the next available channel in descending cycle order. Always select the next lower channel number in the hunt group. When the gateway reaches the lowest channel number in the hunt group, it selects the highest channel number in the hunt group and then start descending again. ▪ 4 (Descending) = Select the highest available channel. Always start at the highest channel number in the hunt group and if that channel is not available, select the next lower channel. ▪ 5 (Number + Cyclic Ascending) = First select the gateway port according to the called number (called number is defined in the 'Endpoint Phone Number' table). If the called number isn't found, then select the next available channel in ascending cyclic order. Note that if the called number is found, but the port associated with this number is busy, the call is released ▪ 6 (By Source Phone Number) = Select the gateway port according to the calling number (refer to the note below). **Note:** The default method is 'By Phone Number'.

Table 1-2: Release 5.0 Modified *ini* File [Web] Parameters (continues on pages 14 to 19)

ini File [Web Interface] Parameter Name	Description
CDRReportLevel [CDR Report Level]	(**Modification:** Additional enumeration 3.) Valid options include: ▪ 0 = CDR is not used ▪ 1 = Call Detail Record is sent to the Syslog server at the end of each call. ▪ 2 = CDR report is sent to Syslog at the start and end of each call. ▪ 3 = CDR report is sent to Syslog at connection and at the end of each call. The CDR Syslog message complies with RFC 3161 and is identified by: Facility = 17 (local1) and Severity = 6 (Informational) **Note:** This parameter replaces the EnableCDR parameter.
StutterToneDuration [Stutter Tone Duration]	(**Modification:** Added support for Call Forwarding.) Duration (in msec) of the played Stutter dial tone, which indicates that Call Forwarding is enabled or that there is a waiting message(s). The default is 2,000 (i.e., 2 seconds). The range is 1,000 to 60,000. The Stutter tone is played (instead of a regular Dial tone), when a Call Forward is enabled on the specific port or when MWI is received. The tone is composed of a 'Confirmation tone', which is played for a user-defined duration (StutterToneDuration), followed by a 'Stutter tone'. Both tones are defined in the CPT file. **Note 1:** This parameter is applicable only to FXS gateways. **Note 2:** The message waiting notification (MWI) tone takes precedence over the call forwarding reminder tone.

1.7 Obsolete Parameters

Table 1-3 lists parameters from the previous release that are no longer in use.

Table 1-3: Release 5.0 Obsolete *ini* File [Web] Parameters

ini File [Web Interface] Parameter Name	Description
RTPNoOpEnable	This parameter is now obsolete. Please use the parameter NoOperationSendingMode.
RTPNoOpInterval	This parameter is now obsolete. Please use the parameter NoOpInterval.
EnableCDR	This parameter is now obsolete. Please use the parameter CDRReportLevel.

2 H.323 Compatibility

The MediaPack H.323 gateway is built on and implements the RadVision™ H.323 version 4.2 protocol stack. The gateway complies with H.323 Version 4.0 ITU standard, H.245 Version 10 and H.225 Version 4.

In this version, the gateway features the following (except as noted in Section 2.2):

2.1 Supported H.323 Features

2.1.1 Gatekeeper

- Registers to known Gatekeeper.
- Supports Gatekeeper registration with prefixes (useful for FXO gateways).
- Supports sending of Unregister request before reset.
- Uses routed or direct mode calls.
- Supports the Alternative Gatekeepers mechanism, used to obtain the IP addresses of alternative Gatekeepers.
- Uses redundant Gatekeepers (if redundant Gatekeepers are defined).
- Supports Automatic Gatekeeper Discovery (using IP Multicast).
- Works also without a Gatekeeper using the internal routing table with or without dialing plan rules.
- Can fallback to internal routing table if there is no communication with the Gatekeepers.
- Supports the "TimeToLive" parameter. The MediaPack gateway sends Registration requests up to "TimeToLive" expiration.
- Supports Info Request Response (IRR) messages for KeepAlive.
- Supports the mapping of destination (Alias) numbers in ACF message by the Gatekeeper.
- Supports Gatekeeper ID configuration (per Gatekeeper IP) for different Gatekeepers.
- Supports Lightweight Registration.
- Supports RAI (Resource Available Indication) messages, informing Gatekeeper that the gateway's resources are below a threshold.
- Supports registration types: E.164, H323-ID and PartyNumber.
- Supports Pre-granted ARQ
- Supports H.235 Security, Annex D Procedure 1 (authentication with a Gatekeeper).

2.1.2 Call Setup

- Can use the Normal Connect procedure.
- Can use the Fast Connect procedure with or without immediately opening H.245 channel.
- Can use Tunneling.
- Can negotiate a coder from a list of given coders for Normal or Fast Connect procedures.
- Can open an H.245 channel when using Fast Connect.
- Supports Early H.245 procedure, enabling opening of an H.245 channel before a Connect message is received. Can be used for sending out-of-band DTMF digits before a call is answered.
- Can represent SourceNumber and DestinationNumber through: E.164, H323-ID and PartyNumber.
- Can configure (in the manipulation tables) or map (according to H.225 V.4 Table 18) the representation of the Src/Dest number types in H.323 messages.
- Supports collecting Digits from POTS (Plain Old Telephone Service) (for FXS gateways) or from PBX/PSTN (for FXO gateways) using predefined digit map.
- Supports one or two stage dialing for network to PBX/PSTN calls, using MP-10x/FXO gateway.
- Supports answer supervision (FXO) using detection of either polarity reversal or human voice.
- Supports disconnect supervision (FXO) using polarity reversal, current disconnect, detection of Busy/Reorder/Dial tones, or detection of silence.
- Supports configuration of calling number screening indication in H.225 Setup.
- Supports Pre-Grant ARQ, enabling the gateway to skip ARQ messages for incoming or outgoing calls.

2.1.3 General

- AudioCodes MediaPack gateways are identified by Country Code (0xB5) and Manufacturers Code (0x28) in H.323 messages.
- Supports H.323 Annex D, T.38 real time fax.
- Supported coders: G.711 A-law, G.711 μ-law, G.723.1, G.726 and G.729.
- Supports H.450 Call Hold, Call Transfer, Call Forwarding, Call waiting, Message Waiting Indication and Name Identification supplementary services (H.450.1, H.450.2, H.450.3, H.450.4, H.450.6, H.450.7 and H.450.8).
- Supports DTMF negotiation.
- Supports DTMF and hook-flash signal out of band through H.245 channel, (using “Alphanumeric” or "Signal" field).
- Supports DTMF and hook-flash signal in-band according to RFC 2833 including negotiation of payload type.

- Supports DTMF and hook-flash signal out of band using H.225/Q.931 Keypad facility messages.
- Supports reopening of logical channel and implementation of third-party reroute.
- Supports configuration of H.323 Port Range.
- Supports H.225/Q.931 Progress Indicator parameter for Fast Connect, enabling playing of local Ringback tone or to cut through the voice channel to listen to remote Call Progress Tones/messages.
- Supports detection (FXO) and generation (FXS) of Caller ID signal (NTT, Bellcore, ETSI, Indian, Danish, Brazilian, British and Swedish standards) and interworking it to H.323 network.
- Supports Caller ID restriction (Privacy).
- Supports routing of IP→Tel calls to predefined hunt groups.
- Supports a configurable channel select mode per hunt group.
- Supports various number manipulation rules for IP→Tel and Tel→IP, called and calling numbers.
- Supports H.245 round trip delay. When activated the gateway periodically generates H.245 round trip delay requests.

2.2 Unsupported H.323 Features

- Gatekeeper bandwidth QoS control is not supported. BRQ, BCF and BRJ messages aren't used.
- SNMP H.323 MIB (H.341) is not supported.
- H.323 Annex E (over UDP).

Reader's Notes

3 Known Constraints

3.1 Hardware Constraints

1. Only specific combinations of FXS and FXO modules are currently supported. For detailed Information, contact AudioCodes.
2. MP-11x - After running the procedure for restoring the networking parameters to their initial state, the gateway must be reset again using a hardware reset. If a software reset is issued, the gateway reverts to its factory defaults.

3.2 H.323 Constraints

1. The 'Netcoder' coder is no longer supported.
2. The alternative routing mechanism is limited to two destinations (IP addresses for Tel to IP calls or hunt groups for IP to Tel calls).
3. DTMF capability exchange is performed over H.245, therefore, users are recommended to enable parameter OpenH245OnFS, to ensure the opening of the H.245 channel.
   Note that if DTMF transfer is over Q.931 INFO messages, then H.245 is not needed.
4. H.225 Overlap dialing feature is not supported.
5. The VoIP gateway can't work with NetMeeting™ if 'IsFaxUsed' parameter is set to 1 (enable Annex D/T.38 real time fax relay).
6. Signaling DiffServ cannot be configured using Profiles, but it can be configured for the entire gateway.
7. The number of RTP payloads packed in a single G.729 packet (M channel parameter) is limited to 5.
8. NPI/TON are translated according to H.323 standard, table 18, only for Tel→IP calls.
9. For best performance, it is recommended to use the "Fast Connect" procedure.

3.3 Gateway Constraints

1. The device attempts to access the incorrect TFTP server when IniFileUrl specifies a TFTP URL. It is possible to work-around this problem by resetting the device (using the Web interface) after the TFTP error occurs.
2. RFC 2198 redundancy mode with RFC 2833 is not supported (that is, if a complete DTMF digit was lost, it is not reconstructed). The current RFC 2833 implementation does support redundancy for inter-digit information lost.
3. Date and Time should be set after each gateway power reset unless NTP (Network Time Protocol) is used.
4. After resetting the Web password using the *ini* file parameter 'ResetWebPassword' and defining a new password, the user must load an *ini* file with 'ResetWebPassword' set to 0.
5. Channel parameters, such as, Voice/DTMF gain and Jitter buffer are collectively configured in the *ini* file on a per gateway usage (not on a per call basis). By using Profiles this limitation can be overcome.

6. The uploaded *ini* file can contain two (alias) names for some parameters. Both of these parameters must be modified, otherwise, if only the first parameter is changed, the second alias parameter will override its value.
   For example: IsFallbackUsed and IsGKFallbackUsed.

7. The gateway only supports symmetrical coders – the same coder is used for transmit and for receive (though different ptime is supported).

8. The following constraints apply when defining coders via the *ini* file.
   - Coder names are case-sensitive.
   - Don't use obsolete coder names (e.g., g729_AnnexB, g7231r53) with the improved coder interface.
   - When an invalid packetization time is used, the coder definition is disregarded.
   - When an invalid rate is used for dynamic-rate coders, the coder definition is disregarded.

9. The 'RFC2833RxPayloadType' and 'RFC2833TxPayloadType' parameters in the Embedded Web Server's 'Channel Settings' page or in the *ini* file should not be used. Use 'Rfc2833PayloadType' parameter instead.

10. Configuring the board to auto-negotiate mode while the opposite port is set manually to full-duplex (either 10 Base-T or 100 Base-TX) is invalid. It is also invalid to set the board to one of the manual modes while the opposite port is configured differently. It is recommended to use full-duplex connections instead of half-duplex, and 100 Base-TX instead of 10 Base-T (due to the larger bandwidth).

11. It is strongly recommended to use 100 Base-T switches. Use of 10 Base-T LAN hubs should be avoided.

12. In some cases, when the spanning tree algorithm is enabled on the external Ethernet switch port connected to the gateway, the external switch blocks traffic entering and exiting the gateway for some time after the gateway is reset.
    This may cause the loss of important packets (such as BootP and TFTP requests) which in turn may cause the board to fail to start up.
    A possible workaround for this issue is to set the parameter BootPRetries to 5, forcing the gateway to issue 20 BootP requests for 60 seconds.
    A second workaround is to disable the spanning tree algorithm on the port of the external switch that is connected to the gateway.

13. When RTP packets are received after a sudden large network delay (200 to 300 msec), the drift correction could take about 5 seconds. During this period, voice towards the TDM side is silent.

14. Static NAT is not supported for local IP calls.

15. NTT Ring Detection is not supported (with or without caller ID).

16. Indian Caller ID detection is not supported.

17. Metering tone (billing) detection is currently not supported.

18. VLAN Pass-Through mode is not supported.

19. NTT caller ID type 2 constraints - The NTT standard describes the CallerID type 2 generation as a sequence of an incoming-call signal, 'C' & 'D' DTMFs and FSK modulated data. Generation of the incoming call signal remains in the responsibility of the application, but 'C', 'D' and the FSK are generated by the supplied service. The signal can be generated using the UDT signal generation mechanism. Prior to the detection of NTT CallerID type 2 there are 2 DTMF ('C' and 'D') detections which remain unscreened.

3.4 Web Constraints

1. Incorrect values displayed in the 'Firewall Settings' Web page, after the firewall rules, are manipulated using SNMP. The problem occurs when mixing management interfaces, i.e., working with the Web interface, then switching to SNMP, and then switching back to the Web interface.
2. Logo and product name revert to default with empty *ini* file.
3. After resetting the Web password using the *ini* file parameter ResetWebPassword and defining a new password, the user must load an *ini* file with ResetWebPassword set to 0.
4. When 'Access to Restricted Domains' is ON, all attempts to enter security pages sends Syslog message, apart from CERTIFICATES page (Both Security/certificates and SSLCertificateSR pages).
5. Parameter values set commands that are sent to the Syslog. Values are shown which are offset from the values entered in the Web. For example, when VoiceVolume is set to X, the Syslog message indicates the value X+32.
6. Incorrect presentation of dynamic payload in the 'Channel Status' screen.
7. The value of Fax Modem Bypass Coder Type in the Web is absent.
8. SNMPv3 users table returns the “line removed“ notice when adding a new row to an active row index.
9. The 'Fax/Modem Bypass Packing Factor' field doesn't support the 'G726_32' and 'G726_40' options.
10. After adding an empty line to SNMPV3 table, it's impossible to delete it or add new lines.
11. Wizard gets "stuck" when attempting to load an inappropriate file type.
12. Firefox/Mozilla: Port info text box opens too far away from the port.
13. Unintended password reset when changing the username and/or password via the Web and Reset board again from Web.
14. The Embedded Web Server cannot be accessed with HTTPS when DES/3DES is selected on Microsoft Internet Explorer. If the gateway is configured to use the DES cipher, a logic error in Microsoft Internet Explorer causes the HTTPS connection to fail. This problem does not occur when using alternative browsers, such as Firefox.
15. Username and password with 8 characters cannot be entered.
16. The ‘Forward to Phone Number’ field in the ‘Call Forward Table’ screen in the Embedded Web Server is limited to 19 characters. Applicable to MediaPack FXS gateways.
17. Not all parameters can be changed on-the-fly from the Web browser. Parameters that can’t be changed on-the-fly are noted with (!). To change these parameters, reset the gateway, using the Web browser reset button.
18. When changing gateway parameters from the Web browser, the new parameters are permanently stored in flash memory only after the gateway is reset from the Web or after the **BURN** button is clicked in the 'Maintenance Actions' screen.
20. The number of fax calls indicated by the fields: ‘Attempted Fax Calls Counter’ and ‘Successful Fax Calls Counter’ in the Calls Count screens may not be accurate.

21. In the screens 'Coders' and 'Coder Group Settings': When G.729 is used with ptimes 80, 100 and 120 and G.723 is used with ptimes 120 and 150 the voice quality is reduced. Therefore, using these ptimes isn't recommended.
22. The 'Caller ID/Name' column in the 'Caller ID' table in the Embedded Web Server can't contain the inverted commas character ("). For example entering "John" is not allowed. In the *ini* file this string can be used.

3.5 SNMP Constraints

1. The default values created in an IPSec configuration table are incorrect. The user should override the default values before activating the new row.
2. An Ethernet link trap is sent before link is up; manager does not receive clear. This occurs because a spanning tree algorithm is being calculated in the Ethernet switch.
3. The following encryptions types are currently supported (for SNMP v3 users only):
   - Authentication protocol: MD5 and SHA
   - Privacy protocol: DES and AES128
4. The acBoardConfigurationError alarm trap, generated as a result of a configuration error, does not clear.
5. The range of the faxModemRelayVolume MIB object is wrong. Instead of 0 to 15, it should be -18 to -3, corresponding to an actual volume of (-18.5 dBm) to (-3.5 dBm).
6. Cold-start trap doesn't appear after soft reset for MediaPack.
7. Only one SNMP manager can access the device simultaneously.

4 Previous Release 4.8

4.1 Supported Hardware Platforms

4.1.1 New Hardware Platforms Introduced in This Release

The following hardware platforms are introduced in this version:

- MP-118/FXO with 8 FXO ports and MP-114/FXO with 4 FXO ports.
- MP-118/FXS + FXO with 4 FXS ports and 4 FXO ports. This gateway contains a relay that connects the FXS ports to the FXO ports in case of a power failure.
- MediaPack MP-124/FXS Rev D, 24 analog FXS interfaces.

4.1.2 Existing Hardware Platforms

- Analog Mediant 1000 hosting FXS or FXO modules (up to 4 ports in each module, with a total of 6 modules providing up to 24 ports).
- MediaPack MP-11x/FXS, 2 to 8 analog FXS interfaces, with enhanced CPU resources.
  - MediaPack MP-118/FXS, 8 analog FXS interfaces.
  - MediaPack MP-114/FXS, 4 analog FXS interfaces.
  - MediaPack MP-112/FXS, 2 analog FXS interfaces.

4.1.3 Hardware Platforms No Longer Supported

- MediaPack MP-108/FXS, 8 analog FXS interfaces
- MediaPack MP-108/FXO, 8 analog FXO interfaces
- MediaPack MP-104/FXS, 4 analog FXS interfaces
- MediaPack MP-104/FXO. 4 analog FXO interfaces
- MediaPack MP-102/FXS, 2 analog FXS interfaces
- MediaPack MP-124/FXS Rev A, B, C, 24 analog FXS interfaces.

4.2 General Gateway New Features

1. Support for the IPSec and IKE protocols was added. IPSec and IKE are part of the IETF standards for establishing a secured IP connection between two applications. Providing security services at the IP layer, IPSec and IKE are transparent to IP applications.
   IPSec and IKE are used in conjunction to provide security for control (e.g., H.323) and management (e.g., SNMP and Web) protocols but not for media (i.e., RTP, RTCP and T.38).
   Relevant Parameters: EnableIPSec and the following table parameters: IPSEC_IKEDB_TABLE, IPSEC_SPD_TABLE (for detailed information on the parameters of each table, refer to the User's Manual).

2. Media, Control and Management (OAM) traffic in the MediaPack can now be separated into three dedicated networks (a dual mode that separates the Media from the OAM and Control networks is also supported). Instead of a single IP address, the MediaPack can be assigned three IP addresses and subnet masks, each relates to a different traffic type. This architecture enables users to integrate the MediaPack into a three-network environment that is focused on security and segregation. Each entity in the MediaPack (e.g., Web, RTP) is mapped to a single traffic type in which it operates.
   Relevant Parameters: EnableMultipleIPs, LocalMediaIPAddress, LocalMediaSubnetMask, LocalMediaDefaultGW, LocalControlIPAddress, LocalControlSubnetMask, LocalControlDefaultGW, LocalOAMIPAddress, LocalOAMSubnetMask, LocalOAMDefaultGW.

3. Support for 802.1p/Q (VLANs and priority) was added. The MediaPack can now be integrated into a VLAN-aware environment that includes switches, routers and endpoints.
   Relevant Parameters: VlanMode, VlanNativeVlanID, VlanOamVlanID, VlanControlVlanID, VlanMediaVlanID, VlanNetworkServiceClassPriority, VlanPremiumServiceClassMediaPriority, VlanPremiumServiceClassControlPriority, VlanGoldServiceClassPriority, VlanBronzeServiceClassPriority, EnableDNSasOAM, EnableNTPasOAM.

4. The MediaPack can now be configured to set a different DiffServ value to IP packets according to their class-of-service (Network, Premium Media, Premium Control, Gold and Bronze).
   Relevant Parameters: NetworkServiceClassDiffServ, PremiumServiceClassMediaDiffServ, PremiumServiceClassControlDiffServ, GoldServiceClassDiffServ, BronzeServiceClassDiffServ.

5. If calling party name is not received (CallerDisplayInfoX = <name> is not specified per gateway's x port), the source number can be used instead (Applicable to Tel→IP calls). It is also possible to set the source number to the received calling name (Applicable to IP→Tel calls).
   Relevant parameter: UseSourceNumberAsDisplayName, UseDisplayNameAsSourceNumber.

6. The interface for handling coders was improved. You can now select the coder family, packetization time, rate (where applicable), payload type (where applicable) and silence suppression individually per coder.
   Relevant parameters: CoderName, CoderName_ID.

7. Additional parameters were added to the IP and Tel Profiles. In addition, the number of different IP and Tel Profiles was increased to 10 each.
   Relevant parameters: IPProfile, TelProfile.

8. FXS gateways now support generation of 12/16 KHz metering pulses towards the Tel side (e.g., for connection to a payphone or private meter). Tariff pulse rate is determined according to an internal table. This capability enables users to define different tariffs according to the Source/Destination numbers and the time-of-day. The tariff includes the time interval between the generated pulses and the number of pulses generated on answer.
   Relevant parameters: ChargeCode, MeteringType, PayPhoneMeteringMode, Prefix.

9. The RADIUS Accounting mechanism is now supported. The gateway sends a CDR to the RADIUS Accounting Server at the start and/or end of each call.
   Relevant parameters: AAAIndications, RADIUSAccServerIP, RADIUSAccPort, RADIUSAccountingType.

10. FXO gateways can now disconnect a call after a dial tone from the PBX is detected. This is in addition to the existing capability of call disconnection when either busy or reorder tones are detected.
    Relevant parameters: DisconnectOnDialTone.

11. FXO gateways now support a 'guard' time between accepting successive IP to Tel calls. Occasionally, after a call is ended and onhook is applied, a delay is required before placing a new call (and performing offhook). This is necessary to prevent wrong hook-flash detection or other glare phenomena.
    Relevant parameters: GuardTimeBetweenCalls.

12. FXS gateways can now add a delay between detection of offhook and generation of DID Wink.
    Relevant parameters: DelayBeforeDIDWink.

13. It is now possible to determine the behavior of FXS endpoints that are not defined (in the Endpoint Phone Number table), and the behavior of all FXS endpoints when a Busy-Out condition exists. Up to this version, the gateway played a reorder tone to the connected phone/PBX. It is now possible to set the behavior of such endpoints to either no response, reorder tone, polarity reversal, or both.
    Relevant parameters: FXSOOSBehavior.

14. It is now possible to define a digit pattern that is sent to the Tel side after 200 OK is received from the IP side. The digit pattern is a predefined DTMF sequence that is used to indicate an answer signal (e.g., for billing purposes). Applicable only to FXS gateways.
    Relevant parameter: TelConnectCode.

15. The parameter 'Source Number before Manipulation' was added to CDR messages.

16. To enable NAT traversal for the RTP streams RTP NO-OP packets (according to avt-rtp-noop draft) are now sent. This method ensures that the NAT binding remains open during RTP silence periods.
    Relevant parameters: RTPNoOpEnable, RTPNoOpInterval, RTPNoOpPayloadType.

17. Life line testing – The MediaPack now features a mechanism that performs tests on the telephone lines connected to FXS and FXO ports. These tests provide various line measurements. Line testing is executed via SNMP only.

18. Full Mesh Routing – The MediaPack now supports a combination of FXS and FXO channels (4 FXS and 4 FXO channels). Each FXS channel features a lifeline that is connected to a FXO channel [channel 1 (FXS) to channel 5 (FXO)], [channel 2 (FXS) to channel 6 (FXO)] and so on.
    Relevant parameter: LifeLineType.

19. IP Multicast – Supports the reception of multicast RTP streams. The gateway can join an IP multicast group in order to receive an RTP stream generated by a remote server (e.g., a Music-On-Hold stream) to a multicast IP address.

20. PPPoE – The MediaPack can now operate as a Point-to-Point Protocol over Ethernet (PPPoE) client, enabling it to be integrated in a broadband access architecture (mostly in ISP networks).
    Relevant parameters: EnablePPPoE; PPPoEPassword; PPPoERecoverIPAddress; PPPoERecoverDfgwAddress; PPPoERecoverSubnetMask; PPPoEServerName; PPPoEStaticIPAddress; PPPoEUserName.

21. Internal firewall – The MediaPack now accommodates an internal access list facility, allowing the security administrator to define network traffic filtering rules.
    Relevant table parameter: AccessList.

22. Up to five simultaneous Telnet sessions are now supported.

23. Support for DTMF relay according to RFC 2833 was added to the ThroughPacket™ mechanism.

24. An Activity Log mechanism was added to enable the MediaPack to send log messages (to a Syslog server) that report certain types of web actions according to a pre-defined filter.
    The following filters are available: Parameters Value Change, Auxiliary Files Loading, Device Reset, Flash Memory Burning, Device Software Update, Access to Restricted Domains, Non Authorized Access and Sensitive Parameters Value Change.
    Relevant parameter: ActivityListToLog.

25. The automatic update mechanism enables loading files also via FTP, FTPS and Network File System (NFS).

26. Initial configuration of the gateway can now be performed using a standard touch-tone telephone connected to one of the FXS analog ports. The voice menu can also be used to query and modify basic configuration parameters.
    Relevant parameter: VoiceMenuPassword.

27. As of this version it isn't required to load a coefficients file to FXO gateways; instead there is a single parameter that defines the country variant (doesn't apply to the Mediant 1000).
    Relevant parameter: CountryCoefficients.

4.3 H.323 New Features

1. Support for Gatekeeper Auto Discovery (using IP Multicast) was added. The gateway issues a Gatekeeper Request (GRQ) to the well-known Discovery Multicast IP Address (224.0.1.41) or to a different configured IP address. The gateway can receive several Gatekeeper Confirmation (GCF) messages containing the Transport Address of the Gatekeeper's RAS channel. Note that the redundant Gatekeeper mechanism is disabled when Automatic Discovery is enabled.
   Relevant Parameters: EnableGKAutoDiscovery, GKAutoDiscoveryIP.

2. The gateway now supports fax fallback to G.711. When fax is detected and the remote side doesn't declare support for T.38 in the Terminal Capability Set message, the gateway transmits the fax in-band using G.711 coder. The gateway doesn't switch coders when fax is detected. Therefore, this mechanism functions only if G.711 was previously used for the call.
   Relevant Parameters: IsFaxUsed.

3. It is now possible to prefer the Calling Number received in the Q.931 message instead of the H.225 Dialed number.
   Relevant parameters: PreferQ931CallingNumber.

4.4 Web and SNMP New Features

1. To prevent unauthorized access to the Embedded Web Server, two user accounts are now available, a primary and secondary. Each account is composed of three attributes: username, password and access level. The username and password enable access to the Embedded Web Server itself; the access level determines the extent of the access (i.e., availability of screens and read / write privileges). Relevant parameter: ResetWebPassword.
2. A new channel status screen provides the status of the R factor of RTCP XR packets per channel.
3. The Mediant 1000 chassis can now be managed via SNMP. The status of the CPU and I/O modules, fan tray, power supplies, Power Entry Module (PEM) and other alarms are reported.
4. SNMP community strings can now be configured via the Embedded Web Server. Relevant parameters: SNMPReadOnlyCommunityString_x, SNMPReadWriteCommunityString_x, SNMPTrapCommunityString.
5. An HTTP download report trap is now available. This trap indicates the result of a recent file download (includes an HTTP error code, if available).
6. Support for 'sysObjectID' via SNMP was added. Similar to MIB-Object's definition. Should point to a product that is defined in AC-TYPES.my.
7. Active analog lines performance counter is now supported in analog performance monitoring.

4.5 New and Modified Parameters

Most new parameters (described in Table 4-1) can be configured with the *ini* file and via the Embedded Web Server. Note that only those parameters contained within square brackets are configurable via the Embedded Web Server.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

ini File [Web Interface] Parameter Name	Description
EnableIPSec [Enable IP Security]	Enables / disables the Secure Internet Protocol (IPSec) on the gateway. 0 = Disable (default). 1 = Enable.
EnableGKAutoDiscovery [Enable Gatekeeper Auto Discovery]	Enables / disables the automatic Gatekeeper discovery mechanism. 0 = Disabled (default). 1 = Enabled. **Note:** When Automatic Discovery is enabled, the redundant Gatekeeper mechanism is disabled.
GKAutoDiscoveryIP [Gatekeeper Auto Discovery IP Address]	The IP address to which a Gatekeeper Request (GRQ) is sent. Normally, this is a Multicast address used to distribute the request to a large number of known Gatekeepers. When not configured or configured to 0, the well-known Discovery Multicast Address (224.0.1.41) is used.
IsFaxUsed [Enable Annex D/T.38 Fax Relay]	0 = Disable Annex D/T.38 fax relay (default). 1 = Enable Annex D/T.38 fax relay. When you enable this feature, the gateway can send and receive fax messages using the H.323 Annex D T.38 procedure. The gateway supports a fallback mechanism in case that T.38 isn't supported. When fallback is used, the fax is transmitted in-band using G.711 coder. The conditions for fallback are: • IsFaxUsed = 1. • Fax is detected (either by the generating or the terminating side). • T.38 capability was not declared by the remote gateway in the TCS message. The selected coder is G.711.
UseSourceNumberAsDisplayName [Use Source Number as Display Name]	Applicable to Tel→IP calls. 0 = The Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name (if Tel Display Name is received). If no Display Name is received from the Tel side, the IP Display Name remains empty (default). 1 = If a Tel Display Name is received, the Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name. If no Display Name is received from the Tel side, the Tel Source Number is used as the IP Source Number and also as the IP Display Name. 2 = The Tel Source Number is used as the IP Source Number and also as the IP Display Name (even if the received Tel Display Name is not empty).
UseDisplayNameAsSourceNumber [Use Display Name as Source Number]	Applicable to IP→Tel calls. 0 = The IP Source Number is used as the Tel Source Number and the IP Display Name is used as the Tel Display Name (if IP Display Name is received). If no Display Name is received from IP, the Tel Display Name remains empty (default). 1 = If an IP Display Name is received, it is used as the Tel Source Number and also as the Tel Display Name, the Presentation is set to Allowed (0). If no Display Name is received from IP, the IP Source Number is used as the Tel Source Number and the Presentation is set to Restricted (1).

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

***ini* File [Web Interface] Parameter Name**	**Description**
IPProfile_ID [IP Profile Settings]	IPProfile_<Profile ID> = <Profile Name>,<Preference>,<Coder Group ID>,<IsFaxUsed *>,<DJBufMinDelay *>, <DJBufOptFactor *>,<IpDiffServ *>,<ControlIPDiffServ *>,<N/A use $$ instead>, <RTPRedundancyDepth>, <RemoteBaseUDPPort>, <CNGmode>, <VxxTransportType>, <NSEMode>, <PlayRBTone2IP>, <N/A use $$ instead>, <ProgressIndicator2IP*> Preference = (1-20) The preference option is used to determine the priority of the Profile. Where '20' is the highest preference value. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied. For example: IPProfile_1 = name1,2,1,0,10,13,15,44,1,1,6000,0,2,0,0,1,0 IPProfile_2 = name2,$$,$$,$$,$$,$$,$$,$$,$$,1,$$,$$,$$,$$,$$,$$,$$ $$ = Not configured, the default value of the parameter is used. (*) = Common parameter used in both IP and Tel profiles. **Note 1:** The IP ProfileID can be used in the Tel2IP and IP2Tel routing tables (Prefix and PSTNPrefix parameters). **Note 2:** 'Profile Name' assigned to a ProfileID, enabling User's to identify it intuitively and easily. **Note 3:** This parameter can appear up to 9 times (ID = 1 to 9).
TelProfile_ID [Tel Profile Settings]	TelProfile_<Profile ID> = <Profile Name>,<Preference>,<Coder Group ID>,<IsFaxUsed *>,<DJBufMinDelay *>, <DJBufOptFactor *>,<IPDiffServ *>,<ControlIPDiffServ*>,<DtmfVolume>,<InputGain>, <VoiceVolume>,<EnableReversePolarity>,<EnableCurrentDisconnect>, <EnableDigitDelivery>, <ECE>, <MWIAnalogLamp>, <MWIDisplay>, <FlashHookPeriod>, <N/A use $$ instead>, <ProgressIndicator2IP*> Preference = (1-20) The preference option is used to determine the priority of the Profile. Where '20' is the highest preference value. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied. For examples: TelProfile_1 = FaxProfile,1,1,1,40,13,22,33,$$,$$,$$,0,0,0,1,0,0,$$,0,$$ TelProfile_2 = ModemProfile,2,2,0,40,13,$$,$$,$$,$$,$$,$$,$$,$$,0,0,0,$$,0,$$ $$ = Not configured, the default value of the parameter is used. (*) = Common parameter used in both IP and Tel profiles. **Note 1:** The Tel ProfileID can be used in the Hunt group table (TrunkGroup_x parameter). **Note 2:** 'Profile Name' assigned to a ProfileID, enabling User's to identify it intuitively and easily. **Note 3:** This parameter can appear up to 9 times (ID = 1 to 9).
MeteringType [Metering Tones Type]	Defines the metering tone (12 kHz or 16 kHz) that is detected by FXO gateways and generated by FXS gateways. 0 = 12 kHz metering tone (default). 1 = 16 kHz metering tone. **Note:** Suitable (12 kHz or 16 KHz) *coeff* must be used for both FXS and FXO gateways.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

***ini* File [Web Interface] Parameter Name**	**Description**
PayPhoneMeteringMode [Generate Metering Tones]	Determines the method used to configure the metering tones that are generated to the Tel side (FXS gateways only). 0 (disabled) = Metering tones aren't generated (default). 1 (internal table) = Metering tones are generated according to the internal table configured by the parameter ChargeCode. 2 (RADIUS) = N/A. **Note:** This parameter is not applicable to the Metering Tones Relay mechanism.
ChargeCode [Charge Codes Table]	The charge code table is used to configure the metering tones (and their time interval) that the FXS gateway generates to the Tel side. Up to 25 different metering rules can be defined (by repeating the parameter 25 times). To associate a metering rule to an outgoing Tel to IP call, use the Tel to IP Routing table (Prefix). ChargeCode_<Charge Code ID> = <1st period end time>,<1st period pulse interval>,<1st period pulses on answer>, <2nd period end time>,<2nd period pulse interval>,<2nd period pulses on answer>, <3rd period end time>,<3rd period pulse interval>,<3rd period pulses on answer>, <4th period end time>,<4th period pulse interval>,<4th period pulses on answer> Each Charge Code can include from a single and up to four different time periods in a day (24 hours). Each time period is composed of: - The end (in a 24-hours format) of the time period. - The time interval between pulses (in seconds). - The number of pulses sent on answer. The first time period always starts at midnight (00). It is mandatory that the last time period of each Charge Code ends at midnight (00). This prevents undefined time frames in a day. When a new call is established, the Tel to IP Routing table is searched for the destination IP address. Once a route is found, the Charge Code (configured for that route) is used to associate the route with an entry in the Charge Codes table. The gateway selects the time period by comparing the gateway's current time to the end time of each time period of the selected Charge Code. The gateway generates the Number Of Pulses on Answer once the call is connected and from that point on, it generates a pulse each Pulse Interval. If a call starts at a certain time period and crosses to the next, the information of the next time period is used. For example: ChargeCode_1 = 07,30,1,14,20,2,20,15,1,00,60,1 ChargeCode_2 = 05,60,1,14,20,1,00,60,1 ChargeCode_3 = 00,60,1
Prefix [Tel to IP Routing Table]	Prefix = <Destination Phone Prefix>, <IP Address>,<Src Phone Prefix>,<IP Profile ID>,<Charge Code> Selection of IP address (for Tel To IP calls) is according to destination and source prefixes. **Note 1:** An optional IP ProfileID (1 to 9) can be applied to each routing rule. **Note 2:** An optional Charge Code (1 to 25) can be applied to each routing rule to associate it with an entry in the ChargeCode table.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

<table>
<tr><th>ini File [Web Interface] Parameter Name</th><th>Description</th></tr>
<tr><td>CoderName</td><td>Defines the gateway's coder list (up to five coders can be configured).
Enter coders in the following format:
CoderName=<Coder Name>,<Ptime>,<Rate>,<Payload Type>,<Silence Suppression Mode>.
<table>
<tr><th>Coder Name</th><th>Packetization Time</th><th>Rate</th><th>Payload Type</th><th>Silence Suppression</th></tr>
<tr><td>G.711 A-law [g711Alaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 8</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.711 μ-law [g711Ulaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 0</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.729 [g729]</td><td>10, 20 (default), 30, 40, 50, 60</td><td>Always 8</td><td>Always 18</td><td>Disable [0]
Enable [1]
Enable w/o Adaptations [2]</td></tr>
<tr><td>G.723.1 [g7231]</td><td>30 (default), 60, 90</td><td>5.3 [0], 6.3 [1] (default)</td><td>Always 4</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td rowspan="4">G.726 [g726]</td><td rowspan="4">10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>16 [0] (default)</td><td>23 or 35</td><td rowspan="4">Disable [0]
Enable [1]</td></tr>
<tr><td>24 [1]</td><td>Always 22</td></tr>
<tr><td>32 [2]</td><td>Always 2</td></tr>
<tr><td>40 [3]</td><td>Always 38</td></tr>
</table>
Note 1: The coder name is case-sensitive.
Note 2: If silence suppression is not defined (for a specific coder), the value defined by the parameter EnableSilenceCompression is used.
Note 3: The value of several fields is hard-coded according to well-known standards (e.g., the payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored.

For example:
CoderName = g711Alaw64k,20,,,0
CoderName = g711Ulaw64k,40
CoderName = g7231,90,1,,1
CoderName = g726,$$,2,,0</td></tr>
<tr><td>CoderName_ID</td><td>Defines groups of coders that can be associated with IP or Tel profiles (up to five coders in each group).
Enter coder groups in the following format:
CoderName_<coder group ID from 1 to 4>=<Coder Name>,<Ptime>,<Rate>,<Payload Type>,<Silence Suppression Mode>.
<table>
<tr><th>Coder Name</th><th>Packetization Time</th><th>Rate</th><th>Payload Type</th><th>Silence Suppression</th></tr>
<tr><td>G.711 A-law [g711Alaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 8</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.711 μ-law [g711Ulaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 0</td><td>Disable [0]
Enable [1]</td></tr>
</table></td></tr>
</table>

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

ini File [Web Interface] Parameter Name	Description				
	G.729 [g729]	10, 20 (default), 30, 40, 50, 60	Always 8	Always 18	Disable [0] Enable [1] Enable w/o Adaptations [2]
	G.723.1 [g7231]	30 (default), 60, 90	5.3 [0], 6.3 [1] (default)	Always 4	Disable [0] Enable [1]
	G.726 [g726]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	16 [0] (default)	23 or 35	Disable [0] Enable [1]
			24 [1]	Always 22	
			32 [2]	Always 2	
			40 [3]	Always 38	
	Note 1: The coder name is case-sensitive. **Note 2:** If silence suppression is not defined (for a specific coder), the value defined by the parameter EnableSilenceCompression is used. **Note 3:** The value of several fields is hard-coded according to well-known standards (e.g., the payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored. **Note 4:** This parameter (CoderName_ID) can appear up to 20 times (five coders in four coder groups). For example: CoderName_1 = g711Alaw64k,20,,,0 CoderName_1 = g711Ulaw64k,40 CoderName_1 = g7231,90,1,,1 CoderName_2 = g726,$$,2,,0				
DisconnectOnDialTone [Disconnect on Dial Tone]	FXO gateways can disconnect a call after a dial tone from the PBX is detected. 0 = Call isn't released. 1 = Call is released if dial tone is detected on the gateway's FXO port (default). **Note:** This option is in addition to the mechanism that disconnects a call when either busy or reorder tones are detected.				
PreferQ931CallingNumber	Sets the preferred Calling Number to use. 0 = Use the H.225 Dialed Number (default). 1 = Use the Q.931 Calling Party Number (CGPN).				
AAAIndications [AAA Indications]	Determines the Authentication, Authorization and Accounting (AAA) indications that are used. 0 = No indications (default). 3 = Accounting only.				
RADIUSAccServerIP [RADIUS Accounting Server IP Address]	IP address of accounting server.				
RADIUSAccPort [RADIUS Accounting Port]	Port number of RADIUS accounting server. The default value is 1646.				
RADIUSAccountingType [RADIUS Accounting Type]	Determines when a RADIUS accounting report is issued. 0 = At the release of the call only (default). 1 = At the connect and release of the call. 2 = At the setup and release of the call.				
GuardTimeBetweenCalls [Guard Time Between Calls]	Defines the time interval (in seconds) after a call has ended and a new call can be accepted for IP to Tel calls. Applicable only to FXO gateways. The valid range is 0 to 10. The default value is 1 second. **Note:** Occasionally, after a call is ended and onhook is applied, a delay is required before placing a new call (and performing offhook). This is necessary to prevent wrong hook-flash detection or other glare phenomena.				

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

***ini* File [Web Interface] Parameter Name**	**Description**
DelayBeforeDIDWink [Delay Before DID Wink]	Defines the time interval (in seconds) between detection of offhook and generation of DID Wink. Applicable only to FXS gateways. The valid range is 0 to 1,000. The default value is 0.
WaitForDialTime [Wait For Dial Time]	Determines the delay before the gateway starts dialing on the FXO line in the following scenarios (applicable only to FXO gateways): 1. The delay between the time the line is seized and dialing is begun, during the establishment of an IP→Tel call. **Note:** Applicable only to FXO gateways for single stage dialing, when waiting for dial tone (IsWaitForDialTone) is disabled. 2. The delay between the time when Wink is detected and dialing is begun, during the establishment of an IP→Tel call (for DID lines, EnableDIDWink = 1). 3. For call transfer. The delay after hook-flash is generated and dialing is begun. The valid range (in milliseconds) is 0 to 20000 (20 seconds). The default value is 1000 (1 second).
FXSOOSBehavior [Out-Of-Service Behavior]	Determines the behavior of FXS endpoints that are not defined (in the Endpoint Phone Number table), and the behavior of all FXS endpoints when a Busy-Out condition exists. 0 (None) = Normal operation: No response is provided to undefined endpoints. Dial tone is played to FXS endpoints when a Busy-Out condition exists. 1 (Reorder Tone) = The gateway plays a reorder tone to the connected phone/PBX (default). 2 (Polarity Reversal) = The gateways reverses the polarity of the endpoint, marking it as unusable (relevant, for example, to PBX DID lines). This option can't be configured on-the-fly. 3 (Polarity Reversal + Reorder Tone) = Same as 2 and 3 combined. This option can't be configured on-the-fly.
CountryCoefficients	Determines the FXO line characteristics (AC and DC) according to country of origin. Argentina = 0, Australia = 1, Austria = 2, Bahrain = 3, Belgium = 4, Brazil = 5, Bulgaria = 6, Canada = 7, Chile = 8, China = 9, Colombia = 10, Croatia = 11, Cyprus = 12, Czech_Republic = 13, Denmark = 14, Ecuador = 15, Egypt = 16, El_Salvador = 17, Finland = 18, France = 19, Germany = 20, Greece = 21, Guam = 22, Hong_Kong = 23, Hungary = 24, Iceland = 25, India = 26, Indonesia = 27, Ireland = 28, Israel = 29, Italy = 30, Japan = 31, Jordan = 32, Kazakhstan = 33, Kuwait = 34, Latvia = 35, Lebanon = 36, Luxembourg = 37, Macao = 38, Malaysia = 39, Malta = 40, Mexico = 41, Morocco = 42, Netherlands = 43, New_Zealand = 44, Nigeria = 45, Norway = 46, Oman = 47, Pakistan = 48, Peru = 49, Philippines = 50, Poland = 51, Portugal = 52, Romania = 53, Russia = 54, Saudi_Arabia = 55, Singapore = 56, Slovakia = 57, Slovenia = 58, South_Africa = 59, South_Korea = 60, Spain = 61, Sweden = 62, Switzerland = 63, Syria = 64, Taiwan = 65, TBR21 = 66, Thailand = 67, UAE = 68, United_Kingdom = 69, UnitedStates = 70, Yemen = 71 The default value is 70 (United States).
RTPNoOpEnable	Enables / disables sending of NO-OP packets. 0 = Disabled (default). 1 = Enabled. This mechanism ensures that the NAT binding remains open during RTP silence periods.
RTPNoOpInterval	Determines the time interval (in msec) in which NO-OP packets is sent in the case of silence (no RTP traffic). The valid range is 20 to 600000. The default value is 1000 (10 seconds).
RTPNoOpPayloadType	Determines the payload type of No-Op packets. The valid range is 96 to 127. The default value is 120.
TelConnectCode [Send Digit Pattern on Connect]	Defines a digit pattern that is sent to the Tel side after 200 OK is received from the IP side. The digit pattern is a predefined DTMF sequence that is used to indicate an answer signal (e.g., for billing purposes). Applicable only to FXS gateways. The valid range is 1 to 8 characters.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

ini File [Web Interface] Parameter Name	Description
VoiceMenuPassword [Voice Menu Password]	Password for the voice menu, used for configuration and status. To activate the menu, connect an analog telephone and dial *** (three stars) followed by the password. The default value is 12345.
ActivityListToLog [Activity Types to Report via 'Activity Log' Messages]	The Activity Log mechanism enables the gateway to send log messages (to a Syslog server) that report certain types of web actions according to a pre-defined filter. The following filters are available: **PVC** (Parameters Value Change) - Changes made on-the-fly to parameters. **AFL** (Auxiliary Files Loading) - Loading of auxiliary files (e.g., via Certificate screen). **DR** (Device Reset) - Device reset via the Reset Device screen. **FB** (Flash Memory Burning) - Burning of files / parameters to flash (e.g., Save Configuration screen). **SWU** (Device Software Update) - cmp loading via the Software Upgrade Wizard. **ARD** (Access to Restricted Domains) - Access to Restricted Domains. The following screens are restricted: (1) ini parameters (AdminPage) (2) General Security Settings (3) Configuration File (4) IPSec/IKE tables (5) Software Upgrade Key (6) Internal Firewall (7) Web Access List. (8) Web User Accounts **NAA** (Non Authorized Access) - Attempt to access the Embedded Web Server with a false / empty username or password. **SPC** (Sensitive Parameters Value Change) - Changes made to sensitive parameters: (1) IP Address (2) Subnet Mask (3) Default Gateway IP Address (4) ActivityListToLog For example: ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc'
Internal Firewall Parameters	
AccessList_Source_IP [Source IP]	IP address (or DNS name) of source network, or a specific host.
AccessList_Net_Mask [Mask]	IP network mask. 255.255.255.255 for a single host or the appropriate value for the source IP addresses. The IP address of the sender of the incoming packet is bitwise ANDed with this mask and then compared to the field 'Source IP'.
AccessList_Start_Port **AccessList_End_Port** [Local Port Range]	The destination UDP/TCP ports (on this device) to which packets are sent. The valid range is 0 to 65535. **Note:** When the protocol type isn't TCP or UDP, the entire range must be provided.
AccessList_Protocol [Protocol]	The protocol type (e.g., UDP, TCP, ICMP, ESP or 'Any'), or the IANA protocol number (in the range of 0 (Any) to 255). **Note:** The protocol field also accepts the abbreviated strings 'SIP', 'MGCP', 'MEGACO' and 'HTTP'. Specifying these strings implies selection of the TCP or UDP protocols, and the appropriate port numbers as defined on the device.
AccessList_Packet_Size [Packet Size]	Maximum allowed packet size. The valid range is 0 to 65535. **Note:** When filtering fragmented IP packets, the Packet Size field relates to the overall (reassembled) packet size, not to the size of each fragment.
AccessList_Byte_Rate [Byte Rate]	Expected traffic rate (bytes per second).

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

***ini* File [Web Interface] Parameter Name**	**Description**
AccessList_Byte_Burst [Burst Bytes]	Tolerance of traffic rate limit (number of bytes)
AccessList_Allow_Type [Action Upon Match]	Action upon match (allow or block)
AccessList_MatchCount [Match Count]	A read-only field that provides the number of packets accepted / rejected by a specific rule.
PPPoE Parameters	
EnablePPPoE	Enables the PPPoE (Point-to-Point Protocol over Ethernet) feature. 0 = Disable (default) 1 = Enable
PPPoEPassword	Password for PAP or Secret for CHAP authentication. The valid range is a string of up to 47 characters. The default value is 0.
PPPoERecoverIPAddress	IP address to use when booting from the flash to non-PPPoE (Point-to-Point Protocol over Ethernet) environments. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 10.4.10.4.
PPPoERecoverDfgwAddress	Default GW address to use when booting from the flash to non-PPPoE (Point-to-Point Protocol over Ethernet) environments. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 10.4.10.1.
PPPoERecoverSubnetMask	Subnet Mask to use when booting from the flash to non-PPPoE (Point-to-Point Protocol over Ethernet) environments. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 255.255.0.0.
PPPoEServerName	Server Name for CHAP authentication. The valid range is a string of up to 47 characters. The default value is 0.
PPPoEStaticIPAddress	IP address to use in a static configuration setup. If set, used during PPP negotiation to request this specific IP address from the PPP server. If approved by the server, this IP address is used during the session. The valid IP address range is in dotted notation xxx.xxx.xxx.xxx. The default value is 0.0.0.0.
PPPoEUserName	User Name for PAP or Host Name for CHAP authentication. The valid range is a string of up to 47 characters. The default value is 0.
Differential Services Parameters	
NetworkServiceClassDiffServ [Network QoS]	Sets the DiffServ value for Network service class content. The valid range is 0 to 56. The default value is 48.
PremiumServiceClassMediaDiffServ [Media Premium QoS]	Sets the DiffServ value for Premium Media service class content (only if IPDiffServ is not set in the selected IP Profile). The valid range is 0 to 56. The default value is 46. **Note:** The value for the Premium Control DiffServ is determined by (according to priority): (1) IPDiffServ value in the selected IP Profile. (2) PremiumServiceClassMediaDiffServ.
PremiumServiceClassControlDiffServ [Control Premium QoS]	Sets the DiffServ value for Premium Control service class content (only if ControlIPDiffserv is not set in the selected IP Profile). The valid range is 0 to 56. The default value is 46. **Note:** The value for the Premium Control DiffServ is determined by (according to priority): (1) ControlPDiffserv value in the selected IP Profile. (2) PremiumServiceClassControlDiffServ.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

ini File [Web Interface] Parameter Name	Description
GoldServiceClassDiffServ Gold QoS	Sets the DiffServ value for the Gold service class content. The valid range is 0 to 56. The default value is 26.
BronzeServiceClassDiffServ [Bronze QoS]	Sets the DiffServ value for the Bronze service class content. The valid range is 0 to 56. The default value is 10.
VLAN Parameters	
VlanMode [VLAN Mode]	Sets the VLAN functionality. 0 = Disable (default) 1 = Enable 2 [PassThrough] = N/A.
VlanNativeVlanID [Native VLAN ID]	Sets the native VLAN identifier (PVID, Port VLAN ID). The valid range is 1 to 4094. The default value is 1.
VlanOamVlanID [OAM VLAN ID]	Sets the OAM (Operation, Administration and Management) VLAN identifier. The valid range is 1 to 4094. The default value is 1.
VlanControlVlanID [Control VLAN ID]	Sets the control VLAN identifier. The valid range is 1 to 4094. The default value is 2.
VlanMediaVlanID [Media VLAN ID]	Sets the media VLAN identifier. The valid range is 1 to 4094. The default value is 3.
VlanNetworkServiceClassPriority [Network Priority]	Sets the priority for Network service class content. The valid range is 0 to 7. The default value is 7.
VlanPremiumServiceClassMediaPriority [Media Premium Priority]	Sets the priority for the Premium service class content and media traffic. The valid range is 0 to 7. The default value is 6.
VlanPremiumServiceClassControlPriority [Control Premium Priority]	Sets the priority for the Premium service class content and control traffic. The valid range is 0 to 7. The default value is 6.
VlanGoldServiceClassPriority [Gold Priority]	Sets the priority for the Gold service class content. The valid range is 0 to 7. The default value is 4.
VlanBronzeServiceClassPriority [Bronze Priority]	Sets the priority for the Bronze service class content. The valid range is 0 to 7. The default value is 2.
EnableDNSasOAM	This parameter applies to both Multiple IPs and VLAN mechanisms. Multiple IPs: Determines the network type for DNS services. VLAN: Determines the traffic type for DNS services. 1 = OAM (default) 0 = Control.
EnableNTPasOAM	This parameter applies to both Multiple IPs and VLAN mechanisms. Multiple IPs: Determines the network type for NTP services. VLAN: Determines the traffic type for NTP services. 1 = OAM (default) 0 = Control.
Multiple IPs Parameters	
EnableMultipleIPs [IP Networking Mode]	Enables / disables the Multiple IPs mechanism. 0 = Disabled (default). 1 = Enabled.
LocalMediaIPAddress [IP Address]	The gateway's source IP address in the Media network. The default value is 0.0.0.0.
LocalMediaSubnetMask [Subnet Mask]	The gateway's subnet mask in the Media network. The default subnet mask is 0.0.0.0.

Table 4-1: Release 4.8 *ini* File [Web Browser] Parameter Name (continues on pages 34 to 43)

ini File [Web Interface] Parameter Name	Description
LocalMediaDefaultGW [Default Gateway Address]	The gateway's default gateway IP address in the Media network. The default value is 0.0.0.0.
LocalControlIPAddress [IP Address]	The gateway's source IP address in the Control network. The default value is 0.0.0.0.
LocalControlSubnetMask [Subnet Mask]	The gateway's subnet mask in the Control network. The default subnet mask is 0.0.0.0.
LocalControlDefaultGW [Default Gateway Address]	N/A. Use the IP Routing table instead (Advanced Configuration > Network Settings).
LocalOAMIPAddress [IP Address]	The gateway's source IP address in the OAM network. The default value is 0.0.0.0.
LocalOAMSubnetMask [Subnet Mask]	The gateway's subnet mask in the OAM network. The default subnet mask is 0.0.0.0.
LocalOAMDefaultGW [Default Gateway Address]	N/A. Use the IP Routing table instead (Advanced Configuration > Network Settings).

4.6 Version History

Details of previous releases can be found in the Release Notes of Version 4.6, published by AudioCodes on Jul-13-2005.

AudioCodes™ CPE & Access Analog Gateways

H.323

MediaPack™ MP-124 & MP-11x

Release Notes Version 5.0

AudioCodes

www.audiocodes.com