AudioCodes CPE & Access Gateway Products

Analog VoIP Gateways

MediaPack™ & Analog Mediant™ 1000
H.323 Release Notes

Version 4.6

Document #: LTRT-65207

AudioCodes

Notice

This document describes the release of the AudioCodes analog Mediant 1000 and MediaPack Series 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.

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: Jul-13-2005 Date Printed: Aug-07-2005

Table of Contents

List of Tables

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.

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)	MediaPack H.323 User's Manual
LTRT-614xx	MP-1xx Fast Track Installation Guide
LTRT-615xx	MP-11x Fast Track Installation Guide
LTRT-648xx	Analog Mediant 1000 H.323 User's Manual
LTRT-659xx	Analog Mediant 1000 Fast Track Installation Guide

Note 1:	MP-1xx refers to the MP-124 24-port, MP-108 8-port, MP-104 4-port and MP-102 2-port VoIP gateways having similar functionality except for the number of channels (the MP-124 and MP-102 support only FXS).
Note 2:	MP-10x refers to MP-108 8-port, MP-104 4-port and MP-102 2-port gateways.
Note 3:	MP-1xx/FXS refers only to the MP-124/FXS, MP-108/FXS, MP-104/FXS and MP-102/FXS gateways.
Note 4:	MP-10x/FXO refers only to MP-108/FXO and MP-104/FXO gateways.

Note: MP-11x refers to the MP-118 8-port, MP-114 4-port and MP-112 2-port FXS VoIP FXS gateways having similar functionality except for the number of channels.

Note: These Release Notes describe the MP-1xx H.323 VoIP gateways, the MP-11x H.323 VoIP gateways and the analog Mediant 1000 VoIP gateway. Unless otherwise specified, whenever reference is made to the MediaPack in these Release Notes, it automatically includes the MP-11x and the analog Mediant 1000.

1 What's New in Release 4.6

1.1 General Gateway New Features

1. MP-1xx/FXO and Mediant 1000/FXO only - Line Disconnection – The status of the analog phone line is now examined before proceeding with a new IP to Tel call. If the line is disconnected, the call is released with a 'No Route To Destination' response. If the line is disconnected during a call, the call is released immediately.

2. The gateway now supports the ThroughPacket™ mechanism, a proprietary method to aggregate RTP streams from several channels to reduce the bandwidth overhead caused by the attached Ethernet, IP, UDP and RTP headers, and to reduce the packet / data transmission rate. This option reduces the load on network routers and can typically save 50% (e.g., for G.723) on IP bandwidth. ThroughPacket™ can be applied to the entire gateway or, using IP Profile, to specific IP addresses.
Relevant parameters: BaseUDPPort, RemoteBaseUDPPort, L1L1ComplexTxUDPPort, L1L1ComplexRxUDPPort, IPProfile_ID.

3. Support was added for generation of the following Caller ID type-1 standards: ETSI before ring DT AS, ETSI before ring RP AS, ETSI before ring LR DT AS, ETSI not ring-related DT AS, ETSI not ring-related RP AS, ETSI not ring-related LR DT AS and Bellcore not ring related.
Relevant parameters: BellcoreCallerIDTypeOneSubStandard, ETSICallerIDTypeOneSubStandard.

4. Support was added for generation of the following Message Waiting Indication type-1 standards: ETSI before ring DT AS, ETSI before ring RP AS, ETSI before ring LR DT AS, ETSI not ring-related DT AS, ETSI not ring-related RP AS, ETSI not ring-related LR DT AS, Bellcore not ring-related.
Relevant parameters: ETSIVMWITypeOneStandard, BellcoreVMWITypeOneStandard.

5. MP-11x and Mediant 1000 only - The In-Band-Signaling (IBS) capabilities are enhanced to support more complex tones and additional tones / frequencies:

   - Tones with AM modulation
   - Up to four cadences per tone
   - 32 Call Progress Tones
   - Up to 64 different frequencies
   - Generation of voice during off-time of the tone cadence for Call Waiting Tones
   - Burst tones

6. The Automatic Update mechanism was improved. The gateway can now periodically check for updated software (*cmp*) or *ini* files on a remote server. In addition, new parameters that enable the configuration of a separate URL for each configuration file (e.g., CPT) are introduced. This mechanism can be used even for Customer Premise(s) Equipment (CPE) devices that are installed behind NAT and firewalls. For detailed information on the Automatic Update mechanism, refer to the MediaPack User's Manual.
Relevant Parameters: CmpFileURL, IniFileURL, IniFileTemplateURL, PrtFileURL, CptFileURL, FXOCoeffFileURL, FXSCoeffFileURL, AutoUpdateCmpFile, AutoUpdateFrequency, AutoUpdatePredefinedTime, ResetNow.

7. MP-11x and Mediant 1000 only – Silence Indicator (SID) packets that are sent and received according to RFC 3389 can now contain spectral coefficients information. The number of coefficients that are added to the SID packets can be determined using the parameter RTPSIDCoeffNum.
Relevant parameters: RTPSIDCoeffNum.

8. The IP address translation mechanism used for far-end NAT traversal now supports T.38 in addition to RTP.
Relevant parameters: EnableIPAddrTranslation, DisableNAT.

9. Support for injection and detection of NTT Caller ID type 2 (offhook) was added. In addition, a name field was added to the NTT Caller ID. This field is available in NTT Caller ID type 1 (onhook) and type 2.

10. Detection and bypass of Bell 103 modem signal is now supported and controlled.
Relevant parameter: BellModemTransportType.

11. MP-11x only - You can now use the 'Reset' button (located on the MP-11x rear panel) to restore the networking parameters to their factory default values.

12. Fax CNG tone detection was improved by increasing the detection duration.

13. FXO gateways only. A new DTMF pattern that, when received from the Tel side, indicates the gateway to disconnect the call.
Relevant ini file parameter: TelDisconnectCode.

1.2 H.323 New Features

14. Full support was added for the following coders:

- G.729 Annex B (with no correlation to EnableSilenceCompression).

Relevant parameters: CoderName, CoderName_ID.

1.3 Web, SNMP and Command Line New Features

15. MP-11x and Mediant 1000 only - SSL (Secure Socket Layer) and TLS (Transport Layer Security) protocols can now be used to secure access to the Embedded Web (HTTPS) and Telnet Servers.
Relevant Parameters; HTTPSOnly, HTTPSPort, HTTPSRequireClientCertificate, HTTPSRootFileName, HTTPSCertFileName, TelnetServerEnable.

16. Up to 10 authorized client IP addresses, that are permitted to access the gateway via Web or Telnet interface, can now be defined. This security feature is inactive (the gateway can be accessed from any IP address) by default.
Relevant parameter: WebAccessList_x.

17. An IP routing table that is used by the gateway to determine IP routing rules is now available. Before sending an IP packet, the gateway searches this table for an entry that matches the requested destination host / network. If such entry is found, the gateway sends the packet to the indicated router. If no explicit entry is found, the packet is sent to the default gateway.
Relevant parameters: RoutingTableDestinationsColumn, RoutingTableDestinationMasksColumn, RoutingTableGatewaysColumn, RoutingTableHopsCountColumn, RoutingTableInterfacesColumn.

18. The maximum length of the administrator's username and password was increased to 19 characters. Note that if after a long password is set the user goes back to version 4.4 (or earlier), the username and password are deleted (changed to blank).

19. MP-11x and Mediant 1000 only - Users can now enhance the security and capabilities of logging to the gateway's Web and Telnet embedded servers by using a Remote Authentication Dial-In User Service (RADIUS) to store numerous usernames and passwords, allowing multiple user management on a centralized platform. RADIUS (RFC 2865) is a standard authentication protocol that defines a method for contacting a predefined server and verifying a given name and password pair against a remote database, in a secure manner.
Relevant parameters: EnableRADIUS, WebRADIUSLogin, RADIUSAuthServerIP, RADIUSAuthPort, SharedSecret.

20. To prevent unauthorized access to the Embedded Web Server, two levels of security are now available: Administrator (also used for Telnet access) and Monitoring. Each employs a different username and password. Users can access the Embedded Web Server as either:

    - Administrator - all Web screens are read-write and can be modified.

      Default username 'Admin'
      Default password 'Admin'.

    - Monitoring - all Web screens are read-only and cannot be modified. In addition, the following screens cannot be accessed: 'Reset', 'Save Configuration', 'Software Upgrade Wizard', 'Load Auxiliary Files', 'Configuration File' and 'Regional Settings'. The 'Change Password' screen can only be used to change the monitoring password.

      Default username 'User'
      Default password 'User'.

21. A new Calls Routing Status screen was added. This screen provides information on the current routing method used by the gateway. This information includes the IP address of the Gatekeeper the gateway currently operates with.

22. DateAndTime VarBind (Variable Binding) was added to all AC traps.

23. One of the five available SNMP managers can now be defined using a FQDN. The resolved IP address appears in the bottom row of the trap managers table.
Relevant parameter: SNMPTrapManagerHostName.

24. A new Performance Monitoring infrastructure enables collecting and retrieving current and historical performance data via SNMP.

25. Changes made on-the-fly to parameters via Web or SNMP can now be viewed in the Syslog server.
Relevant parameter: EnableParametersMonitoring.

26. An embedded Command Line Interface (CLI) is now available on the MediaPack. The CLI can be accessed via Telnet, RS-232 and the Embedded Web Server. You can use the CLI for diagnostics and basic configuration, such as to modify most of the *ini* file parameters and to change the network settings (IP address, subnet mask and default gateway IP address) of the gateway.
Relevant Parameters: TelnetServerEnable, TelnetServerIdleDisconnect, TelnetServerPort.

1.4 Resolved Constraints

1. A new allocation mechanism protects the existing configuration files (e.g., CPT, logo) from being deleted during a software upgrade. When upgrading the *cmp* file and burning it to the non-volatile memory the *cmp* is burned independently.

2. Several Web messages that were blocked by popup-blocking Web browsers are now available (when java script is enabled).

1.5 New and Modified Parameters

Most new parameters (described in Table 1-1) 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 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 10 to 16)

***ini* File [Web Interface] Parameter Name**	**Description**
RasDestPort	Defines a RAS destination port to which the gateway sends RAS messages to the Gatekeeper. 0 = Use dynamic port that is selected by the operating system. 1-65535 = Static port. The default port is 1719.
CoderName_ID	The CoderName_ID parameter (ID from 1 to 4) provides groups of coders that can be associated with IP or Tel profiles. You can select the following coders: g711Alaw64k – G.711 A-law. g711Ulaw64k – G.711 µ-law. g7231 – G.723.1 6.3 kbps (default). g7231r53 – G.723.1 5.3 kbps. g726 – G.726 ADPCM 16 kbps (Payload Type = 35). g726r16 – G.726 ADPCM 16 kbps, Cisco mode (PT=23). g726r24 – G.726 ADPCM 24 kbps. g726r32 – G.726 ADPCM 32 kbps (PT=2). g726r40 – G.726 ADPCM 40 kbps. g729 – G.729A. g729_AnnexB – G.729 Annex B. The RTP packetization period (ptime, in msec) depends on the selected Coder name, and can have the following values: G.711 family – 10, 20, 30, 40, 50, 60, 80, 100, 120 (default=20). G.729 family – 10, 20, 30, 40, 50, 60 (default=20). G.723 family – 30, 60, 90 (default = 30). G.726 family – 10, 20, 30, 40, 50, 60, 80, 100, 120 (default=20) ***ini* file note 1:** This parameter (CoderName_ID) can appear up to 20 times (five coders in four coder groups). ***ini* file note 2:** The coder name is case-sensitive. ***ini* file note 3:** Enter in the format: Coder,ptime. For example, the following three coders belong to coder group with ID=1: CoderName_1 = g711Alaw64k,20 CoderName_1 = g711Ulaw64k,40 CoderName_1 = g7231,90

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 10 to 16)

***ini* File [Web Interface] Parameter Name**	**Description**
CoderName	Enter the coders in the format: CoderName=<Coder>,<ptime>. For example: CoderName = g711Alaw64k,20 CoderName = g711Ulaw64k,40 CoderName = g7231,90 **Note 1:** This parameter (CoderName) can appear up to 5 times. **Note 2:** The coder name is case-sensitive. You can select the following coders: g711Alaw64k – G.711 A-law. g711Ulaw64k – G.711 μ-law. g7231 – G.723.1 6.3 kbps (default). g7231r53 – G.723.1 5.3 kbps. g726 – G.726 ADPCM 16 kbps (Payload Type = 35). g726r16 – G.726 ADPCM 16 kbps, Cisco mode (PT=23). g726r24 – G.726 ADPCM 24 kbps. g726r32 – G.726 ADPCM 32 kbps (PT=2). g726r40 – G.726 ADPCM 40 kbps. g729 – G.729A. g729_AnnexB – G.729 Annex B. The RTP packetization period (ptime, in msec) depends on the selected coder name, and can have the following values: G.711 family – 10, 20, 30, 40, 50, 60, 80, 100, 120 (default=20). G.729 family – 10, 20, 30, 40, 50, 60 (default=20). G.723 family – 30, 60, 90 (default = 30). G.726 family – 10, 20, 40, 60, 80, 100, 120 (default=20).
RemoteBaseUDPPort [Remote RTP Base UDP Port]	Determines the lower boundary of UDP ports used for RTP, RTCP and T.38 by a remote gateway. If this parameter is set to a non-zero value, ThroughPacket™ is enabled. Note that the value of 'RemoteBaseUDPPort' on the local gateway must equal the value of 'BaseUDPPort' of the remote gateway. The gateway uses these parameters to identify and distribute the payloads from the received multiplexed IP packet to the relevant channels. The valid range is the range of possible UDP ports: 4000 to 64000. The default value is 0 (ThroughPacket™ is disabled). **Note:** To enable ThroughPacket™ the parameters 'L1L1ComplexTxUDPPort' and 'L1L1ComplexRxUDPPort' must be set to a non-zero value.
L1L1ComplexTxUDPPort [RTP Multiplexing Local UDP Port]	Determines the local UDP port used for outgoing multiplexed RTP packets (applies to the ThroughPacket™ mechanism). The valid range is the range of possible UDP ports: 4000 to 64000. The default value is 0 (ThroughPacket™ is disabled). This parameter cannot be changed on-the-fly and requires a gateway reset.
L1L1ComplexRxUDPPort [RTP Multiplexing Remote UDP Port]	Determines the remote UDP port the multiplexed RTP packets are sent to, and the local UDP port used for incoming multiplexed RTP packets (applies to the ThroughPacket™ mechanism). The valid range is the range of possible UDP ports: 4000 to 64000. The default value is 0 (ThroughPacket™ is disabled). This parameter cannot be changed on-the-fly and requires a gateway reset. **Note:** All gateways that participate in the same ThroughPacket™ session must use the same 'L1L1ComplexRxUDPPort'.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 10 to 16)

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 *>,<EnableSilenceCompression> , <RTPRedundancyDepth>,<RemoteBaseUDPPort> For example: IPProfile_1 = name1,2,1,0,10,13,15,44,1,1,6000 IPProfile_2 = name2,$$,$$,$$,$,$$,$$,$$,$$,1,$$ $$ = Not configured, the default value of the parameter is used. (*) = Common parameter used in both IP and Tel profiles. **Note:** This parameter can appear up to 4 times.
BellcoreCallerIDTypeOneSubStandard	Selects the Bellcore Caller ID sub-standard. 0 = Between rings (default). 1 = Not ring related.
ETSICallerIDTypeOneSubStandard	Selects the ETSI Caller ID Type 1 sub-standard (FXS only). 0 = ETSI between rings (default). 1 = ETSI before ring DT_AS. 2 = ETSI before ring RP_AS. 3 = ETSI before ring LR_DT_AS. 4 = ETSI not ring related DT_AS. 5 = ETSI not ring related RP_AS. 6 = ETSI not ring related LR_DT_AS.
ETSIVMWITypeOneStandard	Selects the ETSI Visual Message Waiting Indication (VMWI) Type 1 sub-standard. 0 = ETSI VMWI between rings (default) 1 = ETSI VMWI before ring DT_AS 2 = ETSI VMWI before ring RP_AS 3 = ETSI VMWI before ring LR_DT_AS 4 = ETSI VMWI not ring related DT_AS 5 = ETSI VMWI not ring related RP_AS 6 = ETSI VMWI not ring related LR_DT_AS
BellcoreVMWITypeOneStandard	Selects the Bellcore VMWI sub-standard. 0 = Between rings (default). 1 = Not ring related.
SNMPTrapManagerHostName [Trap Manager Host Name]	Defines a FQDN of a remote host that is used as an SNMP Manager. The resolved IP address replaces the last entry in the trap manager table (defined by the parameter 'SNMPManagerTableIP_x') and the last trap manager entry of snmpTargetAddrTable in the snmpTargetMIB. For example: 'mngr.corp.mycompany.com'. The valid range is a 99-character string
WebAccessList_x [Web and Telnet Access List Screen]	Defines up to ten IP addresses that are permitted to access the gateway's Web and Telnet interfaces. Access from an undefined IP address is denied. This security feature is inactive (the gateway can be accessed from any IP address) when the table is empty. For example: WebAccessList_0 = 10.13.2.66 WebAccessList_1 = 10.13.77.7 The default value is 0.0.0.0 (the gateway can be accessed from any IP address).
RTPSIDCoeffNum	Determines the number of spectral coefficients added to an SID packet being sent according to RFC 3389. Valid only if 'EnableStandardSIDPayloadType' is set to 1. The valid values are 0 (default), 4, 6, 8 and 10. **Note:** Applicable only to MP-11x and Mediant 1000.
BellModemTransportType	Determines the Bell modem transport method. 0 = Transparent (default). 2 = Bypass. 3 = Transparent with events.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 10 to 16)

ini File [Web Interface] Parameter Name	Description
EnableIPAddrTranslation	0 = Disable IP address translation. 1 = Enable IP address translation for RTP and T.38 packets (default). When enabled, the gateway compares the source IP address of the first incoming packet, to the remote IP address stated in the opening of the channel. If the two IP addresses don't match, the NAT mechanism is activated. Consequently, the remote IP address of the outgoing stream is replaced by the source IP address of the first incoming packet. **Note:** The NAT mechanism must be enabled for this parameter to take effect (DisableNAT = 0).
Debug Level **[GwDebugLevel]**	Syslog logging level. One of the following debug levels can be selected: 0 **[0]** = Debug is disabled (default) 1 **[1]** = Flow debugging is enabled 2 **[2]** = Flow and device interface debugging are enabled 3 **[3]** = Flow, device interface and stack interface debugging are enabled 4 **[4]** = Flow, device interface, stack interface and session manager debugging are enabled 5 **[5]** = Flow, device interface, stack interface, session manager and device interface expanded debugging are enabled. 6 **[6]** = Flow, device interface, stack interface, session manager and device interface expanded debugging are enabled. In addition, all H.323 messages are printed according to their ASN.1 format. **Note:** Usually set to 6 if debug traces are needed.
TelDisconnectCode	Determines a digit pattern that, when received from the Tel side, indicates the gateway to disconnect the call. The valid range is a 25-character string.
EnableParametersMonitoring	Enables to view changes made on-the-fly to parameters via Web or SNMP. 0 = Deactivate (default). 1 = Activate.
Secure Hypertext Transport Protocol (HTTPS) Parameters (MP-11x and Mediant 1000 only)	
HTTPSOnly [Secured Web Connection]	Determines the protocol types used to access the Embedded Web Server. 0 = HTTP and HTTPS (default). 1 = HTTPS only (unencrypted HTTP packets are blocked).
HTTPSPort	Determine the local Secured HTTPS port of the device. The valid range is 1 to 65535 (other restrictions may apply within this range). The default port is 443.
HTTPSRequireClientCertificate	Requires client certificates for HTTPS connection. The client certificate must be preloaded to the gateway, and its matching private key must be installed on the managing PC. Time and date must be correctly set on the gateway, for the client certificate to be verified. 0 = Client certificates are not required (default). 1 = Client certificates are required.
HTTPSRootFileName	Defines the name of the HTTPS trusted root certificate file to be loaded via TFTP. The file must be in base64-encoded PEM (Privacy Enhanced Mail) format. The valid range is a 47-character string. **Note:** This parameter is only relevant when the gateway is loaded via BootP/TFTP. For information on loading this file via the Embedded Web Server, refer to the Security section in the User's Manual.
HTTPSCertFileName	Defines the name of the HTTPS server certificate file to be loaded via TFTP. The file must be in base64-encoded PEM format. The valid range is a 47-character string. **Note:** This parameter is only relevant when the gateway is loaded via BootP/TFTP. For information on loading this file via the Embedded Web Server, refer to the Security section in the User's Manual.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 10 to 16)

ini File [Web Interface] Parameter Name	Description
Telnet Parameters	
TelnetServerEnable [Embedded Telnet Server]	Enables or disables the embedded Telnet server. Telnet is disabled by default for security reasons. 0 = Disable (default). 1 = Enable (Unsecured). 2 = Enable Secured (SSL). Applicable only to MP-11x and Mediant 1000.
TelnetServerPort [Telnet Server TCP Port]	Defines the port number for the embedded Telnet server. The valid range = valid port numbers. The default port is 23.
TelnetServerIdleDisconnect [Telnet Server Idle Timeout]	Sets the timeout for disconnection of an idle Telnet session (in minutes). When set to zero, idle sessions are not disconnected. The valid range is any value. The default value is 0.
IP Routing Table parameters: The IP routing *ini* file parameters are array parameters. Each parameter configures a specific column in the IP routing table. The first entry in each parameter refers to the first row in the IP routing table, the second entry to the second row and so forth. In the following example two rows are configured when the gateway is in network 10.31.x.x: RoutingTableDestinationsColumn = 130.33.4.6, 83.4.87.6 RoutingTableDestinationMasksColumn = 255.255.255.255, 255.255.255.0 RoutingTableGatewaysColumn = 10.31.0.1, 10.31.0.112 RoutingTableInterfacesColumn = 0, 1 RoutingTableHopsCountColumn = 20, 20	
RoutingTableDestinationsColumn	Specifies the IP address of the destination host / network.
RoutingTableDestinationMasksColumn	Specifies the subnet mask of the destination host / network.
RoutingTableGatewaysColumn	Specifies the IP address of the router to which the packets are sent if their destination matches the rules in the adjacent columns.
RoutingTableHopsCountColumn	The maximum number of allowed routers between the gateway and destination.
RoutingTableInterfacesColumn	Specifies the network type the routing rule is applied to. 0 = OAM (default). 1 = Control. 2 **=** Media.
RADIUS Login Authentication Parameters (MP-11x and Mediant 1000 only)	
EnableRADIUS [Enable RADIUS Access Control]	Enables / disables the RADIUS application. 0 = RADIUS application is disabled (default). 1 = RADIUS application is enabled. **Note:** In the current version RADIUS is used only for HTTP authentication (CDR over RADIUS isn't supported).
WebRADIUSLogin [Use RADIUS for Web/Telnet Login]	Uses RADIUS queries for Web and Telnet interface authentication. 0 = Disabled (default). 1 = Enabled. When enabled, logging to the gateway's Web and Telnet embedded servers is performed via a RADIUS server. The gateway contacts a predefined server and verifies the given username and password pair against a remote database, in a secure manner. **Note 1:** The parameter 'EnableRADIUS' must be set to 1. **Note 2:** RADIUS authentication requires HTTP basic authentication, meaning the username and password are transmitted in clear text over the network. Therefore, users are recommended to set the parameter 'HttpsOnly = 1' to force the use of HTTPS, since the transport is encrypted.
RADIUSAuthServerIP [RADIUS Authentication Server IP Address]	IP address of the RADIUS authentication server.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 10 to 16)

ini File [Web Interface] Parameter Name	Description
RADIUSAuthPort [RADIUS Authentication Server Port]	Port number of the RADIUS authentication server. The default value is 1645.
SharedSecret [RADIUS Shared Secret]	"Secret" used to authenticate the gateway to the RADIUS server. Should be a cryptographically strong password.
RADIUSRetransmission	Determines the number of RADIUS retransmission retries for the same request. The valid range is 1 to 10. The default value is 3.
RADIUSTo	Determines the time interval (measured in seconds) the gateway waits for a response before a RADIUS retransmission is issued. The valid range is 1 to 30. The default value is 10.
Automatic Update Parameters	
CmpFileURL	Specifies the name of the *cmp* file and the location of the server (IP address or FQDN) from which the gateway loads a new *cmp* file and updates itself. The *cmp* file can be loaded using: TFTP, HTTP or HTTPS. For example: tftp://192.168.0.1/filename **Note 1:** When this parameter is set in the *ini* file, the gateway always loads the *cmp* file after it is reset. **Note 2:** The *cmp* file is validated before it is burned to flash. The checksum of the *cmp* file is also compared to the previously-burnt checksum to avoid unnecessary resets.
IniFileURL	Specifies the name of the *ini* file and the location of the server (IP address or FQDN) from which the gateway loads the *ini* file. The *ini* file can be loaded using: TFTP, HTTP or HTTPS. For example: tftp://192.168.0.1/filename http://192.8.77.13/config<MAC> https://<username>:<password>@<IP address>/<file name> **Note 1:** When using HTTP or HTTPS, the date and time of the *ini* file are validated. Only more recently-dated *ini* files are loaded. **Note 2:** The optional string '<MAC>' is replaced with the gateway's MAC address. Therefore, the gateway requests an *ini* file name that contains its MAC address. This option enables loading different configurations for specific gateways.
IniFileTemplateURL	Specifies the name of a second *ini* file (in addition to IniFileURL) and the location of the server (IP address or FQDN) from which it is loaded. http://server_name/file, https://server_name/file.
PrtFileURL	Specifies the name of the Prerecorded Tones file and the location of the server (IP address or FQDN) from which it is loaded. http://server_name/file, https://server_name/file.
CptFileURL	Specifies the name of the CPT file and the location of the server (IP address or FQDN) from which it is loaded. http://server_name/file, https://server_name/file.
FXOCoeffFileURL	Specifies the name of the FXO coefficients file and the location of the server (IP address or FQDN) from which it is loaded. http://server_name/file, https://server_name/file.
FXSCoeffFileURL	Specifies the name of the FXS coefficients file and the location of the server (IP address or FQDN) from which it is loaded. http://server_name/file, https://server_name/file.
AutoUpdateCmpFile	Enables / disables the Automatic Update mechanism for the cmp file. 0 = The Automatic Update mechanism doesn't apply to the cmp file (default). 1 = The Automatic Update mechanism includes the cmp file.
AutoUpdateFrequency	Determines the number of minutes the gateway waits between automatic updates. The default value is 0 (the update at fixed intervals mechanism is disabled).

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 10 to 16)

ini File [Web Interface] Parameter Name	Description
AutoUpdatePredefinedTime	Schedules an automatic update to a predefined time of the day. The range is 'HH:MM' (24-hour format). For example: 20:18 **Note:** The actual update time is randomized by five minutes to reduce the load on the Web servers.
ResetNow	Invokes an immediate restart of the gateway. This option can be used to activate offline (not on-the-fly) parameters that are loaded via IniFileUrl. 0 = The immediate restart mechanism is disabled (default). 1 = The gateway immediately restarts after an ini file with this parameter set to 1 is loaded.

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).
- 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 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 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.
- Supports the following coders:
  - G.711 A-law 64 kbps (10, 20, 30, 40, 50, 60, 80, 100, 120 msec)
  - G.711 μ-law 64 kbps (10, 20, 30, 40, 50, 60, 80, 100, 120 msec)
  - G.723.1 5.3, 6.3 kbps (30, 60, 90 msec)
  - G.726 16, 24, 32, 40 kbps (10, 20, 30, 40, 50, 60, 80, 100, 120 msec)

  - G.729A/B 8 kbps (10, 20, 30, 40, 50, 60 msec)

- 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 automatic discovery (using Multicast) is not supported. Gatekeepers are defined in manual procedure. GRQ, GCF and GRJ messages are not used.
- 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. Mediant 1000 - 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

3. The ‘Netcoder’ coder is no longer supported.

4. The alternative routing mechanism is limited to two destinations (IP addresses for Tel to IP calls or hunt groups for IP to Tel calls).

5. DTMF transfer parameters: IsDtmfUsed, IsQ931Used and IsFlashHookUsed are obsolete. Use the new parameters TxDtmfOption, RxDtmfOption and HookFlashOption that allow better control of DTMF functionality.
   If the old parameters are still used, the new parameters are overridden.

6. 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.

7. H.225 Overlap dialing feature is not supported.

8. The VoIP gateway can’t work with NetMeeting™ if ‘IsFaxUsed’ parameter is set to 1 (enable Annex D/T.38 real time fax relay).

9. Signaling DiffServ cannot be configured using Profiles, but it can be configured for the entire gateway.

10. The number of RTP payloads packed in a single G.729 packet (M channel parameter) is limited to 5.

3.3 Gateway Constraints

11. When upgrading the MediaPack (loading new software onto the gateway) from version 4.4 to version 4.6 using the BootP/TFTP configuration utility, the device’s auxiliary files (CPT, logo, etc.) are erased.

12. 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.

13. Date and Time should be set after each gateway power reset unless NTP (Network Time Protocol) is used.

14. 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.

15. Channel parameters, such as, Voice/DTMF gain, silence suppression (except for G.729) 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.

16. 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.

17. Two versions of the DSP template firmware are available: DSP Template Versions 0 and 2 (default). The DSP template number 2 supports the silence detection feature that is used for FXO disconnect supervision.

18. FXS and FXO gateways use different configuration *Coeff.dat* files.

19. The polarity reversal detection option (on FXO gateways) isn't functional when using a 12 kHz coefficient file ('MP1xx12-1-12khz-fxo').

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

21. Coder names in *ini* file are case sensitive.

22. 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.

23. 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).

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

25. 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.

26. 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.

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

3.4 Web Constraints

28. 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.

29. 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.

30. 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 "Save Configuration" button is pressed.

31. The number of fax calls indicated by the fields: 'Attempted Fax Calls Counter' and 'Successful Fax Calls Counter' in the Calls Count screens isn't accurate.

32. 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.

33. In the current version, the option to save changes to the IP Routing table so they are available after power fail isn't available via the Embedded Web Server. Use *ini* file configuration instead.

34. 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

35. Configuration alarm does not clear.

36. The following RTP MIB objects are not supported: rtpRcvrSRCSSRC, rtpRcvrSSRC, rtpSenderSSRC, rtpRcvrLostPackets, rtpRcvrPackets, rtpSenderPackets, rtpRcvrOctets, rtpSenderOctets.

37. 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).

38. Cold-start trap doesn't appear after soft reset for MediaPack.

39. Only one SNMP manager can access the device simultaneously.

Reader's Notes

4 Recent Revision History

4.1 Revision 4.4

4.1.1 General Gateway New Features

1. Extensive Profiles support was added. Different Profiles can now be assigned on a per call basis, using the Tel to IP and IP to Tel routing tables, or by assigning different Profiles to the gateway's endpoint(s). The Profiles contain parameters such as Coders, T.38 relay, Voice and DTMF gains, Silence suppression, Echo Canceler, RTP DiffServ, current disconnect, reverse polarity and more.
   The Profiles feature allows the user to tune these parameters or turn them on or off, per source or destination routing and/or the specific gateway or its ports. For example, analog ports can be designated for Fax-only by having a profile which always uses G.711. For more detailed information on the Profiles feature, refer to the MP-1xx H.323 User's Manual.

2. Users can now monitor H.323 real-time activity such as call details and call statistics, including the number of call attempts, failed calls, fax calls, etc. The accumulated data can be viewed in the Embedded Web Server (Status and Diagnostics menu) and via SNMP.

3. The following two additional Call Forward modes are now supported:

   - "Busy or No Reply" - In this mode, calls are forwarded either when the gateway's port is busy or when the call is not answered after a configurable period of time.

   - "Do Not Disturb" – In this mode, incoming calls are immediately released.

   This feature is applicable only to MP-1xx/FXS.
   Relevant parameter: FWDInfo_x.

4. FXS gateways now support subscriber activation and deactivation of the Call Forward, Caller ID Restriction (CLIR) and Hotline features directly from the connected telephone's keypad. Activation / deactivation is invoked by dialing a pre-configured sequence. Successful configuration of these features is followed by a confirmation tone.
   Relevant parameters: KeyCFUncond, KeyCFNoAnswer, KeyCFBusy, KeyCFBusyOrNoAnswer, KeyCFDoNotDisturb, KeyCFDeact, KeyCLIR, KeyCLIRDeact, KeyHotLine, KeyHotLineDeact.

5. Japan NTT 'Modem' DID support - FXS gateways can now be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX. (Applicable for FXS gateways). The DID signal can be sent alone or combined with a NTT Caller ID signal. This feature can be enabled / disabled per port (currently can only be configured via the *ini* file).
   Relevant parameters: EnableDID with NTT CallerIDType, EnableDID_X.

6. Caller ID generation (for FXS gateways) and detection (for FXO gateways) can now be enabled or disabled per port and not only for the entire gateway.
   Relevant parameter : EnableCallerID_X.

7. An option was added to configure the number of rings after which the gateway detects Caller ID. Applicable only to FXO gateways.
   Relevant parameter: RingsBeforeCallerID.

8. Call Waiting Indication delay – Users can now configure a delay interval before a Call Waiting Indication is played to the currently busy port. This enables the caller to hang up before disturbing the called party with Call Waiting Indications. Applicable only to FXS gateways.
   Relevant parameter: TimeBeforeWaitingIndication.

9. Max call duration – Users can now limit the maximum duration of a call. When this time expires, the call is released (from both sides - IP and Tel).
   Relevant parameter: MaxCallDuration.

10. Hotline Dial Tone Duration – Users can now define the dial tone duration after which a port acts as a Hotline. If the gateway received digits during this time period, the call process continues as usual and the Hotline feature isn't used.
    Relevant parameter: HotLineDialToneDuration.

11. Cut-Through feature – An option to receive incoming IP calls on a port in an off-hooked state was added. Applicable only to MP-1xx/FXS.
    Relevant parameter: CutThrough.

12. Additional fields were added to CDR reports: Call Setup Time, Call Connect Time, Call Release Time, RTP Delay and Jitter, RTP SSRC of local and remote sides, Redirect number, Redirect TON/NPI and Redirect reason.
    Note: The Call Time parameters are included in the CDR only if NTP is used or if the gateway's local time and date were configured.

13. Metering Tones Relay – When an FXO gateway detects a 12/16 kHz metering tone, it now sends a Facility message (over IP) to the corresponding FXS gateway. The FXS port generates the 12/16KHz metering tone according to the configured metering tone type.
    Relevant parameter: SendMetering2IP (FXO Only), MeteringType.

14. The "Hotline" and Warmline" feature (immediate or with delay) was added. Each gateway port can now be configured to automatically dial a pre-configured number if no digits are entered after handset offhook, after specified timer for playing the dial tone expires.
    Relevant parameters: TargetOfChannelX, HotLineDialToneDuration.

15. An additional column was added to the Caller ID table. This column ('Presentation') determines whether a specific Caller ID is restricted or not. The Caller ID string isn't sent when a call is initiated by a restricted port. To maintain backward compatibility, when a Caller ID name is "private", the Caller ID is restricted and the Presentation value is ignored.
    Relevant parameter: CallerIDInfo.

16. Generation and detection of Indian, Danish, Brazilian, British and Swedish Type-1, DTMF based, Caller ID signals is now supported.
    Relevant parameter: CallerIDType.

17. Support for Caller ID generation during Call Waiting was added. If an incoming IP call is designated to a busy port, the called party can now view the Caller ID string. The feature is supported for the following Caller ID types: Bellcore and ETSI. Applicable only to FXS gateways.

18. An option to configure a separate destination IP address for CDR Syslog reports was added in order to work smoothly with third-party billing servers.
    Relevant parameter: CDRSyslogServerIP.

19. Users can now configure the gateway to receive T.38 fax relay packets into the same port used by the RTP packets, instead of the RTP port + 2. This solves compatibility issues with certain NATs and Firewalls.
    Relevant parameter: T38UseRTPPort.

20. Generation of date and time with Caller ID is now supported. The date and time are obtained from the internal gateway clock or from NTP (Network Time Protocol) if enabled.
    Relevant parameters: NTPServerIP, NTPServerUTCOffset and NTPUpdateInterval.

21. Users can now configure the duration of the current disconnect signal for FXS gateways, and the detection range of the current disconnect signal for FXO gateways.
    Relevant parameter: CurrentDisconnectDuration.

22. Supports the generation of Caller ID with Distinctive Ringing.
    Relevant parameter and value: AnalogCallerIDTimingMode =1.

23. T.38 Redundancy Enhancement - The redundancy of the low-speed data is now determined according to the enhanced redundancy parameter.

24. Cisco™ NSE mode is now supported for fax pass-through, in addition to the existing support for modem.
    Relevant parameters: NSEMode, NSEPayloadType.

25. Optimization of channel parameters when detecting fax or modem signals (applicable only if the channel was opened with the G.711 coder). When detecting a fax or modem signal on the terminating or originating sides, the gateway modifies the channel's settings to work with voice band data signals such as disable NLP, disable or enable Echo Canceler (EC is enabled for fax calls and disabled for modem calls), disable silence suppression and setting optimized Jitter Buffer mode.
    Relevant parameters and values: FaxTransportType = 3 and VxxModemTransportType = 3 (Transparent with events).

4.1.2 Routing and Manipulation New Features

26. Alternative routing for released calls, for both Tel to IP and IP to Tel calls. Users can now define several call release reasons, to be used for alternative routing. If a new call is released as a result of one of these reasons, the gateway tries to find an alternative routing rule to that call. If such a rule is found, the gateway immediately performs a new call according to that rule. In the current release, only one alternative rule can be defined.
    Note: For Tel to IP calls, this feature is relevant only if the internal Tel to IP routing table is used to route the calls. This feature isn't applicable when Gatekeeper is used to route Tel to IP calls.
    Relevant parameters: AltRouteCauseIP2Tel, AltRouteCauseTel2IP, PSTNPrefix.

27. A new Status Only mode was added to the Alternative Routing feature - The new IP Connectivity screen can be used to display the status of IP address connections, using Ping and QoS results, without enabling/disabling the routing rules.
    Relevant parameter: AltRoutingTel2IPEnable.

28. A 'Source IP' column was added to the Destination Phone Number Manipulation Table for IP to Tel Calls. This field enables to manipulate the destination number also according to the source IP address of the call.
    Relevant parameter: NumberMapIP2Tel.

29. Internal DNS table was added - Similar to a DNS resolution, translates hostnames into IP addresses. This table is used when hostname translation is required (e.g., 'Tel to IP Routing' table, 'Gatekeeper IP Address', etc.). Two different IP addresses can be assigned to the same hostname. If the hostname isn't found in this table, the gateway communicates with an external DNS server. Up to 10 hostnames can be configured.
    Relevant parameter: Dns2IP.

30. Enhanced Tel to IP routing selection - Selection of destination IP address and IP Profiles (optional), can now be performed according to both Destination and Source numbers.
    Relevant parameter: Prefix.

31. Enhanced IP to Tel routing selection - Selection of hunt groups and IP Profiles (optional) can now be performed according to Destination number, Source Number and Source IP address.
Relevant parameter: PSTNPrefix.

32. Enhanced Number Manipulation support - In all four manipulation tables, the following functionalities were added:

   - Can now select an entry according to both destination and source numbers.

   - Can now apply the "Digits to add" and "Digits to remove" manipulation rules also on number suffixes in addition to number prefixes.

   Relevant parameters: NumberMapTel2IP, NumberMapIP2Tel, SourceNumberMapTel2IP, SourceNumberMapIP2Tel.

33. An option to allow or restrict sending of Caller ID information on a per call basis was added (using the Tel to IP number manipulation table).

34. IP addresses can now include wildcards – IP addresses in the 'Source IP Address' column of the 'IP to Hunt Group Routing' table and the 'Source IP' column in the 'Destination Phone Number Manipulation Table for IP to Tel Calls' can include the "x" wildcard that represents single digits. For example: 10.8.8.x (10.8.8.0-10.8.8.9), 10.8.8.xx (10.8.8.10-10.8.8.99), 10.8.xx.xxx (10.8.10.100-10.8.99.255).
Relevant parameters: PSTNPrefix, NumberMapIP2Tel.

35. An option was added for the routing tables to take precedence over a Gatekeeper for routing calls. When this option is enabled, the gateway checks the 'Destination IP Address' field in the 'Tel to IP Routing' table for a match with the outgoing call and the 'Source IP Address' field in the 'IP to Hunt Group Routing' table for a match with the incoming call. Only if a match is not found, a Gatekeeper is used.
Relevant parameter: PreferRouteTable.

36. Supports digit delivery to the IP side. Using the manipulation tables the gateway can now be configured to play pre-configured DTMF digits (per call), after the call is answered.
Relevant parameter: EnableDigitDelivery2IP.

37. IP DiffServ code can now be configured for H.323 signaling protocol in addition to RTP Diffserv.
Relevant parameter: ControlIPDiffServ.

38. The Called Number Manipulation table was increased to 50 rows. The Calling Number Manipulation table was increased to 20 rows.

4.1.3 H.323 New Features

39. Can now use domain name resolution to locate the Gatekeeper's IP address.
Note: only the first DNS resolved IP address is used as the Gatekeeper's IP address.
Relevant parameter: GatekeeperIP.

40. Support for Gatekeeper ID configuration per Gatekeeper IP.
Relevant parameter: GatekeeperIP.

41. Lightweight registration support was added.

42. The MP-1xx gateway now supports the H.323 Alternative Gatekeeper mechanism.
Relevant parameter: AlternativeGKUsed.

Previous Version

43. MP-1xx gateways now support the Early H.245 feature. This feature enables opening of an H.245 channel before a Connect message is received. It can be used to send out-of-band DTMF digits before the call is answered.
Relevant parameter: OpenH245OnFS.

44. Redundant Gatekeeper enhancement – Users can now configure the gateway to whether or not use a redundant Gatekeeper when an RRJ (Registration Reject) message is received from the default Gatekeeper. The default is to keep using the default Gatekeeper and not switch to a redundant one.
Relevant parameter: UseRedundantGKOnRRJ.

45. H.450.7 MWI (Message Waiting Indication) - MP-1xx/FXS gateways can accept an H.450.7 message that indicates waiting messages. Users are informed of these messages by a stutter dial tone that is played before the normal dial tone is played. If the MWI display is configured, the number of waiting messages is also displayed. If the MWI lamp is configured, the phone's lamp (on a phone that is equipped with an MWI lamp) is illuminated.
Relevant parameters: EnableMWI, MWIAnalogLamp, MWIDisplay, StutterToneDuration.

46. H.450.8 Name Identification - H.450.8 service enables the MP-1xx gateway to send and receive the calling party name and its presentation (allowed or restricted).
Relevant parameter: EnableNameIdentification.

47. Support was added for the initiation of H.323 Annex D, T.38 procedure on the originator side of a fax session after detection of CNG a signal.
Relevant parameters:
IsFaxUsed – Enables fax T.38 relay on both the caller and the called sides.
CNGDetectorMode – Set to 2 (Event Only) to start a fax session on the caller side after CNG tone is detected (not recommended).

48. Support for relaying the hook-flash signal over IP using RFC 2833 was added.
Relevant parameter: HookFlashOption.

49. Users can now define a RAS source port from which the gateway sends RAS messages to the Gatekeeper. By default, the operating system selects a dynamic port. Currently can only be configured via the *ini* file (not from the Web).
Relevant parameter: RasSourcePort.

50. The gateway now sends Unregister messages to the Gatekeeper if it is reset via the Embedded Web Server or from AudioCodes' BootP/TFTP utility.

51. An option to configure an H.323-ID per MP-1xx port was added.
Relevant parameter: PortName_x.

52. Support for reception of T.38 fax only call was added. If an incoming H.225 Setup message only contains T.38 capabilities, the receiving gateway initiates a T.38 session.

53. If an FXS gateway receives a ReRoute information (from Q.931 ReRoute or from H.450 Derived info), it will now generate a Caller ID that includes this ReRoute information. This feature is only supported on ETSI Caller ID displays.

54. H.245 round trip delay capability was added. If activated, the gateway periodically generates H.245 round trip delay requests. (Note that the capability to answer remote side requests was always supported).
Relevant parameter: H245RoundTripTime.

55. If the MP-1xx gateway is working with a Gatekeeper, it issues an URQ (Unregister request) to the Gatekeeper just before it is reset (assuming the gateway was reset from the Embedded Web Server, from SNMP or from the BootP configuration utility).

56. Pre-Granted ARQ support was added. This feature enables the gateway to skip ARQ messages for incoming or outgoing calls (Gatekeeper support is required).
Relevant parameter: EnablePregrantARQ.

57. Gatekeeper 'ReRegister' (unregister + register) support was added. Users can now use the Embedded Web Server or SNMP, update the Gatekeeper with new gateway configuration parameters such as phone numbers and registration prefixes.

58. Support for FCR (Fast Connect Refused) message for both sides was added.

59. MP-1xx gateways now support Ringback tone control according to H.225/Q.931 Info message with Signal IE. The gateway plays a Ringback tone if Signal IE=1 "Ring Back tone on", and stops playing the Ringback tone if Signal IE=63 "Tones off". You don't need to configure any parameters to activate this feature.

4.1.4 SNMP and Web Server New Features

60. After changing at least one of the networking parameters (IP address, subnet mask or the default gateway's IP address) in the 'Network Settings' screen and pressing the button 'Submit', a prompt appears indicating that for the change/s to take effect, the gateway will reset and the current configuration will be burned to flash memory.

61. The gateway's Web Interface appearance was updated and enhanced.

62. An 'H.323 Channel Status' screen was added to the Embedded Web Server. This screen can be accessed via the 'Channel Status' screen. It contains H.323 static information and associated calls information of the selected port.

63. A new Web wizard guides the user through the process of software upgrade – selection of files and loading them to the gateway. The wizard also enables the user to upgrade the software and to maintain the existing configuration.

64. A radio button was added alerting the user whether to burn or not to burn changes to flash during reset.

65. New SNMP MIB for collection and monitoring system performance.

66. Introduction of a carrier-grade alarm system with the following characteristics:
    1. Allows an Element Manager (EM) to determine which alarms are currently active (active alarm table).
    2. Allows an EM to detect lost alarm raise and clear traps.
    3. Allows an EM to recover lost alarm raise and clear traps (alarm history table).

67. Enable private labeling of the Web browser's title when a graphical logo is used.

68. The FXO gateway can now detect unconnected analog ports. These ports are marked using a color indication on the Web channel status page.

69. Adding the capability to provision the table of authorized SNMP managers.

70. In addition to acBoard MIB, a new set of MIBs for configuration and status is introduced. The new MIBs are divided by functionality (Media, Analog, Control, System).

71. Users can now configure the detection range of a Flash-Hook signal for FXO ports via the 'Channel Settings' screen in the Embedded Web Server.

4.1.5 Miscellaneous New Features

72. Support for prerecorded Call Progress Tones was added. Using the TrunkPack Downloadable Conversion Utility, users can now create a file that contains prerecorded tones. Each tone is assigned with a tone type. After loading it to the device, the prerecorded tones are played as regular Call Progress Tones according to the tone types. No detection is supported for these tones. The prerecorded tones file can be burned to the non-volatile memory.
Relevant parameter: PrerecordedTonesFileName = 'filename".

73. Users can now instruct the gateway to load a new software (*cmp*) file and / or configuration files from a preconfigured TFTP server after a Web / SNMP reset. Therefore, the gateway can now obtain its networking parameters from BootP or DHCP servers and its software and configuration files from a different TFTP server (preconfigured in *ini* file).
The *ini* file can be loaded according to a specific gateway's MAC address enabling easy configuration for different gateways.
Relevant parameters: IniFileURL, CmpFileURL.

74. An external utility *CPTWizard* simplifies the MP-10x/FXO configuration task by automatically detecting the local set of Call Progress Tones generated by the switch / PBX. The utility creates a CPT *ini* configuration file.

75. NTP support. The time of day can now be obtained from a standard NTP server.
Relevant parameters: NTPServerIP, NTPServerUTCOffset, NTPUpdateInterval.

76. When NTP is enabled, a timestamp string [hour:minutes:seconds] is added to all Syslog messages.

77. DHCP client improvements. The DHCP client now supports limited IP leasing time and performs lease renewal. In addition, the time server option is now supported.

78. Operation in a multiple routers network was improved. The gateway now learns the network topology by responding to ICMP redirections and caching them as routing rules (with expiration time).

79. Support was added for loading and retrieving encoded *ini* files from the gateway instead of clear text files. Files are encoded / decoded using the TrunkPack Downloadable Conversion utility.

80. The mechanism for burning configuration files in non-volatile memory was improved. The new mechanism enables users to maintain their configuration when upgrading the software version. Users should note the following changes:

    - Saving the entire configuration (parameters and files) in non-volatile memory is now controlled by a single parameter – SaveConfiguration (default = 1).

    - 'BurnCallProgressToneFile' and 'BurnCoeffFile' parameters are no longer supported.

81. Sending of in-band and out-of-band DTMF digits (RFC 2833) in parallel is now supported.
Relevant parameters: If DisableAutoDTMFMute = 1, in-band DTMF transmission is set according to the DTMFTransportType parameter.

82. When DHCP is enabled, the gateway includes its product name (e.g., 'MP-108 FXS' or 'MP-104 FXO') in the DHCP 'option 60' Vendor Class Identifier. The DHCP server can use this product name to assign an IP address accordingly.
Note: After power-up, the gateway issues two DHCP requests. Only in the second request, the DHCP 'option 60' is contained. If the gateway is reset from the Web/SNMP, only a single DHCP request containing 'option 60' is sent.

83. The error message that indicates an invalid *ini* file configuration now contains the line number of the invalid parameter in the *ini* file.

4.1.6 Resolved Constraints

1. After a T.38 fax relay session is ended, the gateway's channel reverts to voice coder supporting Voice→Fax→Voice calls.

2. Can now fully support the MapAlias feature. This feature is always set to "true" in ACF messages.
   The parameter 'CanMapAlias' is obsolete and is not used.

3. H.323 vulnerability problem was solved by a Radvision patch.

4. Support for a remote side request (RequestMode H.245 message) for changing coders during a call.

5. The parameters ResponceTimeOut and MaxRetries (defining communication with a Gatekeeper) can now be set without mutual dependency. The possible values for each parameter are 1 to 20.

6. The gateway now supports working with redundant Gatekeepers and with the fallback routing table. If all Gatekeepers are not responding, the gateway will start working with the internal routing table.

7. If an empty TCS (Terminal Capability Set) is received as the first H.245 message (before full Terminal capabilities), the voice path is now muted.

8. If the gateway receives an Open Logical Channel Ack message with RTP=0 and IP=0, the voice channel is now opened in Receive Only mode.

9. Several SNMP managers can now be configured to access the gateway concurrently.

10. Caller ID can also be generated for Distinctive Ringing signals if AnalogCallerIDTimingMode=1.

11. DHCP now supports limited IP leasing time. The gateway performs lease renewal and initiates a new DHCP request when the lease time expires.

4.1.7 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 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
GWAppDelayTime [Delay After Reset]	Defines the amount of time (in seconds) the gateway's operation is delayed after a reset cycle. The valid range is 0 to 600. The default value is 5 seconds. **Note:** This feature helps to overcome connection problems caused by some LAN routers or IP configuration parameters change by a DHCP Server.
CurrentDisconnectDefault Threshold	Determines the line voltage threshold which, when reached, is considered a current disconnect detection. **Note:** Applicable only to MP-10x/FXO gateways. The valid range is 0 to 20 Volts. The default value is 4 Volts.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
TimeToSampleAnalogLineVoltage	Determines the frequency at which the analog line voltage is sampled (after offhook), for detection of the current disconnect threshold. **Note:** Applicable only to MP-10x/FXO gateways. The valid range is 100 to 2500 msec. The default value is 1000 msec.
FWDInfo_X [Call Forward Table]	Forward incoming IP calls (using 302 response) based on the gateway port to which the call is routed. FwdInfo_<Gateway Port Number (0 to 23)> = <Forward Type>, <Forward to Phone Number>, <Timeout (in seconds) for No Reply> 0 = Not in use. 1 = On busy: forward incoming calls when the port is busy. 2 = Immediate: always forward any incoming call. 3 = No reply: forward incoming calls that are not answered after a configurable period of time. 4 = On busy or No reply: forward incoming calls when the port is busy or when calls are not answered after a configurable period of time. 5 = Do Not Disturb: immediately reject incoming calls. **Note 1:** Applicable only to MP-1xx/FXS gateways. **Note 2:** When a Gatekeeper isn't used, the 'Forward to Phone Number' must be specified in the 'Tel to IP Routing' table of the forwarding gateway.
EnableDID_X	Enables generation of Japan NTT Modem DID signal per port. EnableDID_<Port> = <Modem DID> Modem DID: 0 = Disabled (default). 1 = Enabled. If not configured, use the global parameter 'EnableDID'. **Note:** Applicable only to MP-1xx/FXS gateways.
EnableCallerID_X [Generate Caller ID to Tel / Detect Caller ID from Tel]	Enables Caller ID generation (FXS) or detection (FXO) per port. EnableCallerID_<Port> = <Caller ID> Caller ID: 0 = Disabled (default). 1 = Enabled. If not configured, use the global parameter 'EnableCallerID'. **Note 1:** The numbering of ports starts with 0. **Note 2:** This parameter can appear up to eight times for MP-108, and up to 24 times for MP-124.
CngDetectorMode [CNG Detector Mode]	0 = Don't detect CNG (default). 2 = Detect CNG on the caller side and start a fax session (if IsFaxUsed=1). Normally T.38 fax session starts when the "preamble" signal is detected by the answering side. Some gateways do not support the detection of this fax signal on the answering side. For these cases, it is possible to configure the MP-1xx gateways to start the T.38 fax session when the CNG tone is detected by the originating side. However this mode is not recommended.
PreferRouteTable [Prefer Routing Table]	Determines if the local routing tables take precedence over a Gatekeeper for routing calls. 0 = Only Gatekeeper is used to route calls (default). 1 = The gateway checks the 'Destination IP Address' field in the 'Tel to IP Routing' table for a match with the outgoing call and the 'Source IP Address' field in the 'IP to Hunt Group Routing' table for a match with the incoming call. Only if a match is not found, a Gatekeeper is used. Applicable only if Gatekeeper is used (IsGateKeeperUsed = 1).

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
HookFlashOption [Hook-flash Option]	Hook-flash Transport Type. Determines the method by which hook-flash is sent and received. 0 = No, hook-flash transport is disabled (default). 1 = H.245 User Input indication message. 2 = H.245 Signal. 3 = Q.931 UserInfo. 4 = RFC 2833 Signal.
RingsBeforeCallerID [Rings before Detecting Caller ID]	Sets the number of rings before the gateway starts detection of Caller ID (FXO only). 0 = Before first ring. 1 = After first ring (default). 2 = After second ring.
TimeBeforeWaitingIndication [Time before Waiting Indication]	Defines the interval (in seconds) before a call waiting indication is played to the port that is currently in a call (FXS only). The valid range is 0 to 100. The default time is 0 seconds.
MaxCallDuration [Max Call Duration]	Defines the maximum call duration in minutes. If this time expires, both sides of the call are released (IP and Tel). The valid range is 0 to 120. The default time is 0 (no limitation).
UseRedundantGKOnRRJ [Use Redundant Gatekeeper on RRJ]	0 = Do not switch to redundant Gatekeeper after an RRJ message is received (default). 1 = Switch to redundant Gatekeeper after a RRJ message is received.
RasSourcePort	Defines a RAS source port from which the gateway sends RAS messages to the Gatekeeper. 0 = Use dynamic port that is selected by the operating system (default). 1-65535 = Static port.
HotLineDialToneDuration [Hot Line Dial Tone Duration]	Duration (in seconds) of the Hotline dial tone. If no digits are received during the Hotline dial tone duration, the gateway initiates a call to a preconfigured number (set in the automatic dialing table). The valid range is 0 to 60. The default time is 16 seconds. Applicable to FXS and FXO gateways.
CutThrough [Enable Calls Cut Through]	Enables users to receive incoming IP calls while the port is in an off-hooked state. 0 = Disabled (default). 1 = Enabled. If enabled, FXS gateways answer the call and “cut through” the voice channel, if there is no other active call on that port, even if the port is in off-hooked state. When the call is terminated (by the remote party), the gateway plays a reorder tone for ‘TimeForReorderTone’ seconds and is then ready to answer the next incoming call, without on-hooking the phone. The waiting call is automatically answered by the gateway when the current call is terminated (EnableCallWaiting=1). **Note:** This option is applicable only to FXS gateways.
EnableDigitDelivery2IP [Enable Digit Delivery to IP]	0 = Disabled (default). 1 = Enable digit delivery to IP. The digit delivery feature enables sending of DTMF digits to the destination IP address after the Tel→IP call was answered. To enable this feature, modify the called number to include at least one ’p’ character. The gateway uses the digits before the ‘p’ character in the initial Setup message. After the call was answered the gateway waits for the required time (# of ‘p’ * 1.5 seconds) and then sends the rest of the DTMF digits using the method chosen (in-band, out-of-band). **Note:** The called number can include several ‘p’ characters (1.5 seconds pause). For example, the called number can be as follows: pp699, p9p300.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
EnableDigitDelivery [Enable Digit Delivery to Tel]	0 = Disabled (default). 1 = Enable Digit Delivery feature for MP-1xx/FXO & FXS. The digit delivery feature enables sending of DTMF digits to the gateway's port after the line is Off-Hooked (FXS) or seized (FXO). For IP→Tel calls, after the line is Off-Hooked / seized, the MP-1xx plays the DTMF digits (of the called number) towards the phone line. **Note 1:** The called number can also include the characters 'p' (1.5 seconds pause) and 'd' (detection of dial tone). If the character 'd' is used, it must be the first "digit" in the called number. The character 'p' can be used several times. For example, the called number can be as follows: d1005, dpp699, p9p300. To add the 'd' and 'p' digits, use the usual number manipulation rules. **Note 2:** To use this feature with FXO gateways, configure the gateway to work in one stage dialing mode. **Note 3:** If the parameter 'EnableDigitDelivery' is enabled, it is possible to configure the gateway to wait for dial tone per destination phone number (before or during dialing of destination phone number), therefore the parameter 'IsWaitForDialTone' (that is configurable for the entire gateway) is ignored. **Note 4:** The FXS gateway sends Connect messages only after it finishes playing the DTMF digits to the phone line.
SendMetering2IP [Send Metering Message to IP]	0 = Disabled (default). 1 = FXO gateways send a metering tone message to IP on detection of 12/16 kHz metering pulse. FXS gateways generate the 12/16 kHz metering tone on reception of a metering message. **Note:** Suitable (12 kHz or 16 kHz) *coeff* file must be used for both FXS and FXO gateways. The 'MeteringType' parameter must be defined in both FXS/FXO gateways.
MeteringType	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* file must be used for both FXS and FXO gateways.
NSEMode	Cisco compatible fax and modem bypass mode. 0 = NSE disabled (default). 1 = NSE enabled. **Note 1:** This feature can be used only if VxxModemTransportType=2 (Bypass). **Note 2:** To use this feature: • The Cisco gateway must include the following definition: "modem passthrough nse payload-type 100 codec g711alaw". • Set the Modem transport type to Bypass mode ('VxxModemTransportType = 2') for all modems. • Configure the gateway parameter NSEPayloadType = 100 In NSE bypass mode the gateway starts using G.711 A-Law (default) or G.711 μ-Law, according to the parameter 'FaxModemBypassCoderType'. The payload type used with these G.711 coders is a standard payload type (8 for G.711 A-Law and 0 for G.711 μ-Law). The parameters defining payload type for the "old" AudioCodes' Bypass mode. 'FaxBypassPayloadType' and 'ModemBypassPayloadType' are not used with NSE Bypass. The bypass packet interval is selected according to the parameter 'FaxModemBypassBasicRtpPacketInterval'.
NSEPayloadType	NSE payload type for Cisco Bypass compatible mode. The valid range is 96-127. The default value is 105. **Note:** Cisco gateways usually use NSE payload type of 100.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
IniFileURL	Specifies the name of the *ini* file and the location of the TFTP server from which the gateway loads the *ini* and configuration files. For example: tftp://192.168.0.1/filename tftp://192.10.77.13/config<MAC> **Note:** The optional string "<MAC>" is replaced with the gateway's MAC address. Therefore, the gateway requests an *ini* file name that contains its MAC address. This option enables loading different configurations for specific gateways.
CmpFileURL	Specifies the name of the *cmp* file and the location of the TFTP server from which the gateway loads a new *cmp* file and updates itself. For example: tftp://192.168.0.1/filename **Note 1:** When this parameter is set in the *ini* file, the gateway <u>always</u> loads the *cmp* file after it is reset. **Note 2:** The version of the loaded *cmp* file isn't checked.
PrerecordedTonesFileName	The name (and path) of the file containing the Prerecorded Tones.
ControlIPDiffServ [Signaling DiffServ]	Defines the value of the 'DiffServ' field in the IP header for the signaling session. The valid range is 0 to 63. The default value is 0.
AlternativeGKUsed	0 = Disabled (default). 1 = Alternative Gatekeepers option is enabled.
PortName_x [H.323 Port ID Table]	Enables you to assign a specific H.323 ID to each port, instead of the global H.323-ID parameter. These IDs are used for registration to the Gatekeeper (RRQ) when 'GWRegistrType' = 1 or 2 and for Gatekeeper admission (ARQ) and call initialization when 'SourceEncodeType' = 1 or 2. PortName_<port> = <H.323 Port ID string> **Note 1:** The numbering of channels starts with 0. **Note 2:** This parameter can appear up to eight times for MP-108, and up to 24 times for MP-124.
OpenH245OnFS [Open H.245 on Fast Start]	0 = The gateway doesn't open an H.245 channel when making a Fast Start connection (default). 1 = The gateway opens an H.245 channel immediately after the Fast Start connection is established. 2 = The gateway opens an H.245 channel as soon as it can. This option applies to Normal and Fast Start. Opening of H.245 channel may be needed for relaying DTMF digits over H.245 channel, during a call.
T38UseRTPPort	Defines that the T.38 packets will be received using the same Rx port as RTP packets. 0 = Use the RTP port +2 to receive T.38 packets (default). 1 = Use the same port as the RTP port to receive T.38 packets.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

***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 *>,<EnableSilenceCompression>, <RTPRedundancyDepth> Preference = (1-10) The preference option is used to determine the priority of the Profile. If both IP and Tel profiles apply to the same call, the coders and other common parameters of the preferred Profile will be applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters will be applied. For example: IPProfile_1 = name1,2,1,0,10,13,15,44,1,1 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 4 times.
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> Preference = (1-10) The preference option is used to determine the priority of the Profile. If both IP and Tel profiles apply to the same call, the coders and other common parameters of the preferred Profile will be applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters will be applied. For example: TelProfile_1 = FaxProfile,1,2,0,10,5,22,33,2,22,34,1,0,1,1 TelProfile_2 = ModemProfile,0,10,13,$$,$$,$$,$$,$$,0,$$,0,0,1,1 $$ = 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 4 times.
TrunkGroup_x [Endpoint Phone Number Table]	TrunkGroup_<Hunt Group ID> = <Starting channel> - <Ending channel>, <Phone Number>, <Tel Profile ID> For example: TrunkGroup_1 = 1-4,100 TrunkGroup_2 = 5-8,200,1 **Note 1:** The numbering of channels starts with 1. **Note 2:** 'Hunt Group ID' can be set to any number in the range 1 to 99. **Note 3:** When 'x' (Hunt Group ID) is omitted, the functionality of the TrunkGroup parameter is similar to the functionality of ChannelList and Channel2Phone parameters. **Note 4:** This parameter can appear up to 8 times for MP-108 gateways and up to 24 times for MP-124 gateways. **Note 5:** An optional Tel ProfileID (1 to 5) can be applied to each group of channels.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
CoderName_ID [Coder Group Settings]	Coder list for Profiles (up to five coders in each group). The CoderName_ID parameter (ID from 1 to 4) provides groups of coders that can be associated with IP or Tel profiles. You can select the following coders: g711Alaw64k – G.711 A-law. g711Ulaw64k – G.711 μ-law. g7231 – G.723.1 6.3 kbps (default). g7231r53 – G.723.1 5.3 kbps. g726 – G.726 ADPCM 16 kbps (Payload Type = 35). g726r16 – G.726 ADPCM 16 kbps, Cisco mode (PT=23). g726r32 – G.726 ADPCM 32 kbps (PT=2). g726r40 – G.726 ADPCM 40 kbps. g729 – G.729A. The RTP packetization period (ptime, in msec) depends on the selected Coder name, and can have the following values: g711 family – 10, 20, 30, 40, 50, 60, 80, 100, 120 (default=20). g729 – 10, 20, 30, 40, 50, 60 (default=20). g723 family – 30, 60, 90 (default = 30). G.726 family – 10, 20, 30, 40, 50, 60, 80, 100, 120 (default=20) **Note 1:** If not specified, the ptime gets a default value. **Note 2:** Each coder should appear only once. **Note 3:** The ptime specifies the maximum packetization time the gateway receives. **Note 4:** G.729B is supported if the coder G.729 is selected and 'EnableSilenceCompression' is enabled. ***ini* file note 1:** This parameter (CoderName_ID) can appear up to 20 times (five coders in four coder groups). ***ini* file note 2:** The coder name is case-sensitive. ***ini* file note 3:** Enter in the format: CoderName,ptime. For example, the following three coders belong to coder group with ID=1: CoderName_1 = g711Alaw64k,20 CoderName_1 = g711Ulaw64k,40 CoderName_1 = g7231,90
DisableAutoDTMFMute	Enables / disables the automatic mute of DTMF digits when out-of-band DTMF transmission is used. 0 = Auto mute is used (default). 1 = No automatic mute of in-band DTMF. When 'DisableAutoDTMFMute=1', the DTMF transport type is set according to the parameter 'DTMFTransportType' and the DTMF digits aren't muted if out-of-band DTMF mode is selected ('IsDTMFUsed =1'). This enables the sending of DTMF digits in-band (transparent of RFC 2833) in addition to out-of-band DTMF messages. **Note:** Usually this mode is not recommended.
DNS2IP [Internal DNS Table]	Internal DNS table, used to resolve host names to IP addresses. Two different IP addresses (in dotted format notation) can be assigned to a hostname. DNS2IP = <Hostname>, <first IP address>, <second IP address> **Note 1:** If the internal DNS table is configured, the gateway first tries to resolve a domain name using this table. If the domain name isn't found, the gateway performs a DNS resolution using an external DNS server. **Note 2:** This parameter can appear up to 10 times.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
AltRouteCauseTel2IP [Reasons for Alternative Routing Table]	Table of call failure reason values received from the IP side (H.323, Q.931 presentation). If a call is released as a result of one of these reasons, the gateway tries to find an alternative route to that call in the 'Tel to IP Routing' table. **Note:** This parameter can appear up to 4 times. For example: AltRouteCauseTel2IP = 3 (No route to destination). AltRouteCauseTel2IP = 18 (User doesn't respond). AltRouteCauseTel2IP = 17 (User is busy).
AltRouteCauseIP2Tel [Reasons for Alternative Routing Table]	Table of call failure reason values received from the Tel side (in Q.931 presentation). If a call is released as a result of one of these reasons, the gateway tries to find an alternative hunt group to that call in the 'IP to Hunt Group Routing' table. **Note:** This parameter can appear up to 4 times. For example: AltRouteCauseIP2Tel = 34 (No circuit is available). AltRouteCauseIP2Tel = 21 (Call rejected). AltRouteCauseIP2Tel = 27 (Destination out of order).
Prefix [Tel to IP Routing Table]	Prefix = <Destination Phone Prefix>, <IP Address>,<Src Phone Prefix>,<IP Profile ID> Selection of IP address (for Tel To IP calls) is according to destination and source prefixes. **Note:** An optional IP ProfileID (1 to 5) can be applied to each routing rule.
PSTNPrefix [IP to Hunt Group Routing Table]	PSTNPrefix = a,b,c,d,e 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 5) can be applied to each routing rule. **Note 3:** The Source IP Address can include the "x" wildcard to represent <u>single</u> digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 to 10.8.8.99.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
NumberMapTel2IP [Destination Phone Number Manipulation Table for Tel→IP calls]	Manipulates the destination number for Tel to IP calls. NumberMapTel2IP = a,b,c,d,e,f,g 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 = H.225/Q.931 Number Plan f = H.225/Q.931 Number Type g = Source number prefix The 'b' to 'f' manipulations rules are applied if the called and calling numbers match the 'a' and 'g' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign "$$", for example: NumberMapTel2IP=01,2,972,$$,0,0,$$ NumberMapTel2IP=03,(2),667,$$,0,0,22
SourceNumberMapTel2IP [Source Phone Number Manipulation Table for Tel→IP calls]	SourceNumberMapTel2IP = a,b,c,d,e,f,g,h a = Source number prefix b = Number of stripped digits from the left, or (if in brackets are used) from right. A combination of both options is allowed. c = String to add as prefix, or (if in brackets are used) as suffix. A combination of both options is allowed. d = Number of remaining digits from the right e = H.225/Q.931 Number Plan f = H.225/Q.931 Number Type g =Destination number prefix h =Calling number presentation (0 to allow presentation, 1 to restrict presentation) The 'b' to 'f' and 'h' manipulation rules are applied if the called and calling numbers match the 'a' and 'g' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign "$$", for example: SourceNumberMapTel2IP=01,2,972,$$,0,0,$$,1 SourceNumberMapTel2IP=03,(2),667,$$,0,0,22,1

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

***ini* File [Web Interface] Parameter Name**	**Description**
NumberMapIP2Tel [Destination Phone Number Manipulation Table for IP→Tel calls]	Manipulate the destination number for IP to Tel calls. NumberMapIP2Tel = a,b,c,d,e,f,g,h,i 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,$$,$$,$$,22 **Note:** The Source IP address can include the “x” wildcard to represent <u>single</u> digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99.
SourceNumberMapIP2Tel [Source Phone Number Manipulation Table for IP→Tel calls]	Manipulate the destination number for IP to Tel calls. NumberMapIP2Tel = a,b,c,d,e,f,g a = Source number prefix b = Number of stripped digits from the left, or (if brackets are used) from the right. A combination of both options is allowed. c = String to add as prefix, or (if brackets are used) as suffix. A combination of both options is allowed. d = Number of remaining digits from the right e = Not in use, should be set to $$ f = Not in use, should be set to $$ g = Destination number prefix The ‘b’ to ‘d’ manipulations rules are applied if the called and calling numbers match the ‘a’ and ‘g’ conditions. The manipulation rules are executed in the following order: ‘b’, ‘d’ and ‘c’. Parameters can be skipped by using the sign "$$", for example: NumberMapIP2Tel =01,2,972,$$,$$,$$,034 NumberMapIP2Tel =03,(2),667,$$,$$,$$,22
TargetOfChannelX [Automatic Dialing Table]	Defines (per port) the automatic dialing configuration. TargetOfChannel<Port> = <Phone>,<Mode> Port = 0 to 7 for MP-108, 0 to 23 for MP-124. Phone = An auto dialed phone string. mode = 0 Normal (collect digits). mode = 1 Auto Dial, the gateway immediately dials after the phone is off-hooked. mode = 2 Hotline, the gateway dials if no digits were collected during a dial tone duration.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
TimeForDialTone [Dial Tone Duration]	Time in seconds that the dial tone is played. The default time is 16 seconds. FXS gateway ports play the dial tone after phone is picked up; while FXO gateway ports play the dial tone after port is seized in response to ringing. **Note 1:** During play of dial tone, the gateway waits for DTMF digits. **Note 2:** 'TimeForDialTone' is not applicable when Automatic Dialing is enabled.
CallerDisplayInfoX [Caller ID Table]	CallerDisplayInfo<channel> = <Caller ID string>, <Restriction> Restriction =0: The CallerID is not restricted (default). Restriction = 1: The CallerID is restricted. For example: CallerDisplayInfo0 = John,0 CallerDisplayInfo7 = David,1 **Note 1:** The numbering of channels starts with 0. **Note 2:** This parameter can appear up to eight times for MP-108, and up to 24 times for MP-124.
H245RoundTripTime [H.245 Round Trip Time]	The time period (in seconds) for generation of H.245 round trip delay requests The range is 0 to 3600. The default time is 0 seconds (H.245 round trip delay requests are not generated).
KeyCFUncond **KeyCFNoAnswer** **KeyCFBusy** **KeyCFDeact** **KeyCFBusyOrNoAnswer** **KeyCFDoNotDisturb** [Keypad Features]	Keypad sequence that activates the call forward features. KeyCFUncond = For unconditional call forward. KeyCFNoAnswer = For call forward on no answer. KeyCFBusy = For call forward on busy. KeyCFBusyOrNoAnswer = For call forward on busy or no answer. KeyCFDoNotDisturb = For call forward on Do Not Disturb configuration. Users can configure the call forward reason and forwarding number directly from their phone (it can also be configured in the Embedded Web Server). For example: KeyCFUncond = *73 KeyCFDeact = *75 To activate the required forward method from the telephone: • Press the preconfigured sequence number on the keypad; a dial tone is heard. • Press the telephone number to which the call is forwarded; a confirmation tone is heard. To deactivate call forward, press the KeyCFDeact sequence; after the sequence is pressed a confirmation tone is heard. **Note:** This option is applicable only to FXS gateways.

Previous Version

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
KeyHotLine **KeyHotLineDeact** [Keypad Features]	Keypad sequence that activates the hotline feature. The hotline feature directs the FXS gateway to dial a preconfigured (hotline) number if no digits were collected during a dial tone duration (about 15 seconds). Users can enable / disable the hotline feature and enter the hotline number directly from their phone (it can also be configured in the Embedded Web Server). For example: KeyHotLine = *83 KeyHotLineDeact = *84 To activate the delayed hotline option from the telephone: • Press the preconfigured sequence number on the keypad; a dial tone is heard. • Press the telephone number to which the phone automatically dials after a configurable delay; a confirmation tone is heard. To deactivate the hotline option, press the KeyHotLineDeact sequence; after the sequence is pressed a confirmation tone is heard. **Note:** This option is applicable only to FXS gateways.
KeyCLIR **KeyCLIRDeact** [Keypad Features]	Keypad sequence that activates the Caller ID restriction (CLIR). Users can enable / disable the CLIR feature directly from their phone (it can also be configured in the Embedded Web Server). For example: KeyCLIR = *43 KeyCLIRDeac t=*44 To activate the CLRI option from the telephone: Press the preconfigured KeyCLIR sequence number on the keypad; a confirmation tone is heard. To deactivate the CLRI option, press the KeyCLIRDeact sequence; after the sequence is pressed a confirmation tone is heard. **Note:** This option is applicable only to FXS gateways.
EnablePregrantARQ [Enable Pre-Grant ARQ]	Enable the H.323 pre granted ARQ mechanism. 0 = Disabled (default). 1 = Enabled.
GatekeeperIP [Gatekeeper IP Address]	Gatekeeper identification. Can be an IP address in numerical format or a FQDN that will be resolved by an external or internal DNS server to IP address. Gatekeeper = IP,ID ID = Gatekeeper-ID string **Note:** This parameter enables the configuration of a Gatekeeper ID per each Gatekeeper. If not configured the global 'GatekeeperID' parameter is used.
EnableMWI [Enable MWI]	Enable H.450.7 MWI (message waiting indication). 0 = Disabled (default). 1 = Enabled. This parameter is applicable only to FXS gateways. **Note:** The MP-1xx only supports reception of MWI.
MWIAnalogLamp [MWI Analog Lamp]	0 = Disable (default). 1 = Enable visual Message Waiting Indication, supplies line voltage of approximately 100 VDC to activate the phone's lamp. This parameter is applicable only to FXS gateways.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
MWIDisplay [MWI Display]	0 = MWI information isn't sent to display (default). 1 = MWI information is sent to display. If enabled, the gateway generates an MWI FSK message that is displayed on the MWI display. This parameter is applicable only to FXS gateways.
EnableNameIdentification [Enable Name Identification]	Enable H.450.8 (name identification). 0 = Disabled (default). 1 = Enabled.
AltRoutingTel2IPEnable [Enable Alt Routing Tel to IP]	Operation modes of the Alternative Routing mechanism: 0 = Disabled (default). 1 = Enabled. 2 = Enabled for status only, not for routing decisions.
CDRSyslogServerIP [CDR Server IP Address]	Defines the destination IP address for CDR logs. The default value is a null string that causes the CDR messages to be sent with all Syslog messages.
NTPServerIP	IP address (in dotted format notation) of the NTP server. The default IP address is 0.0.0.0 (the internal NTP client is disabled).
NTPServerUTCOffset	Defines the UTC (Universal Time Coordinate) offset (in seconds) from the NTP server. The default offset is 0. The offset range is –43200 to 43200 seconds.
NTPUpdateInterval	Defines the time interval (in seconds) the NTP client requests for a time update. The default interval is 86400 seconds (24 hours). The range is 0 to 214783647 seconds. **Note:** It isn't recommended to be set beyond one month (2592000 seconds).
PolarityReversalType	Defines the voltage change slope during polarity reversal or wink. 0 = Soft (default). 1 = Hard. **Note 1:** Some Caller ID signals uses reversal polarity and/or wink. In these cases it is recommended to set PolarityReversalType to 1 (Hard). **Note 2:** Applicable only to FXS gateways.
CurrentDisconnectDuratio n	Duration of the current disconnect pulse (in msec). The default is 900 msec, The range is 200 to 1500 msec. Applicable for both FXS and FXO gateways. **Note:** The FXO gateways' detection range is +/-200 msec of the parameter's value + 100. For example if CurrentDisconnectDuration = 200, the detection range is 100 to 500 msec.
AnalogCallerIDTimimgMod e	0 = Caller ID is generated between the first two rings (default). 1 = The gateway attempts to find an optimized timing to generate the Caller ID according to the selected Caller ID type. Note that when used with distinctive ringing, the Caller ID signal will not change the distinctive ringing timing. **Note:** Applicable only to FXS gateways.
SaveConfiguration	Set to 1 to store the Call Progress Tones and Coefficient files in the non-volatile memory. **Note:** The parameters 'BurnCallProgressToneFile' and 'BurnCoeffFile' are no longer supported.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 32 to 45)

ini File [Web Interface] Parameter Name	Description
BootPSelectiveEnable	Enables the Selective BootP mechanism. 1 = Enabled. 0 = Disabled (default). The Selective BootP mechanism enables the gateway's integral BootP client to filter unsolicited BootP/DHCP replies (accepts only BootP replies that contain the text "AUDC" in the vendor specific information field). This option is useful in environments where enterprise DHCP servers respond to gateway BootP requests. **Note1**: When working with DHCP (EnableDHCP=1) the selective BootP feature must be disabled. **Note 2:** The BootPSelectiveEnable is a special "Hidden" parameter. Once defined and saved in the flash memory, it is used even if it doesn't appear in the *ini* file.
SNMPTrustedMGR_x	Up to five IP addresses of remote trusted SNMP managers from which the SNMP agent accepts and processes get and set requests. **Note 1:** If no values are assigned to these parameters any manager can access the device. **Note 2:** Trusted managers can work with all community strings.
SNMPReadOnlyCommunityString_x	Read-only community string (up to 19 chars). The default string is "public".
SNMPReadWriteCommunityString_x	Read-write community string (up to 19 chars). The default string is "private".
SNMPTrapCommunityString_x	Community string used in traps (up to 19 chars). The default string is "trapuser".

Reader's Notes

5 Previous Releases

Details of previous releases can be found in the Release Notes of Version 4.4, published by AudioCodes on Jan-12-2005.

AudioCodes CPE & Access Gateway Products

Analog VoIP Gateways

www.audiocodes.com