AudioCodes CPE & Access Gateway Products

Analog VoIP Gateways

MediaPack™ & Analog Mediant™ 1000 SIP Release Notes

Version 4.6

Document #: LTRT-65606

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: Jul-31-2005

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

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-654xx (e.g., LTRT-65401)	MediaPack SIP User's Manual
LTRT-614xx	MP-1xx Fast Track Installation Guide
LTRT-615xx	MP-11x Fast Track Installation Guide
LTRT-657xx	Analog Mediant 1000 SIP User's Manual
LTRT-659xx	Analog Mediant 1000 SIP 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 gateways having similar functionality except for the number of channels.

Note: These Release Notes describe the MP-1xx SIP VoIP gateways, the MP-11x SIP 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 4xx 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. Media, Control and Management (OAM) traffic in the MediaPack can now be separated into three dedicated networks. Instead of a single IP address, the MediaPack can be assigned three IP addresses and subnet masks, each relates to a different traffic type. This architecture enables users to integrate the MediaPack into a three-network environment that is focused on security and segregation. Each entity in the MediaPack (e.g., Web, RTP) is mapped to a single traffic type in which it operates.
   Relevant Parameters: EnableMultipleIPs, LocalMediaIPAddress, LocalMediaSubnetMask, LocalMediaDefaultGW, LocalControlIPAddress, LocalControlSubnetMask, LocalControlDefaultGW, LocalOAMIPAddress, LocalOAMSubnetMask, LocalOAMDefaultGW, EnableDNSasOAM, EnableNTPasOAM.

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

9. 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.

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

11. 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.

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

13. 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.

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

15. 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.

16. The default base UDP port was changed to 6000.
    Relevant parameter: BaseUDPPort.

1.2 SIP New Features

17. MP-1xx FXO and Mediant 1000 FXO only – Voice Mail (VM) application. The MP-1xx can now be used to mediate between an analog PBX and an IP VM application. The supported architecture includes an MP-1xx connected to a PBX, using voice mail lines and connected to a voice mail application via the IP network.
The MP-1xx communicates with the PBX by using either Simplified Message Desk Interface (SMDI) via the serial RS-232 connection (MP-1xx FXO only), or special in-band DTMF digit patterns.
Relevant Parameters: VoiceMailInterface, DigitPatternForwardOnBusy, DigitPatternForwardOnNoAnswer, DigitPatternForwardOnDND, DigitPatternForwardNoReason, DigitPatternInternalCall, DigitPatternExternalCall, SMDI, SMDITimeOut, LineTransferMode, SerialData, SerialParity, SerialStop, SerialFlowControl, WaitForDialTime, MWIOffCode, MWIOnCode, TelDisconnectCode.

18. MP-11x and Mediant 1000 only - Support was added for TLS and SIPS (Secured SIP) connections. The gateway initiates a TLS connection if its selected transport type is TLS. If a TLS connection is initiated to the gateway, it responds using TLS even if TLS isn't enabled. When SIPS is enabled, TLS is used all the way to the destination (over multiple hops). TLS and SIPS use the Certificate Exchange process described in the MediaPack SIP User's Manual.
Relevant parameters: TLSLocalSIPPort, EnableSIPS, SIPTransportType, SIPSRequireClientCertificate.

19. Support was added for SIP over TCP. A TCP session is established if the selected transport type is TCP, or if a TCP connection is initiated by a remote gateway (even if the local gateway isn't configured to use TCP).
Relevant parameters: TCPLocalSIPPort, SIPTransportType.

20. It is now possible to configure a specific destination port, in addition to the IP address, for the Proxy, Registrar and Destination IP Address entries of the Tel to IP Routing table.
Relevant parameters: ProxyIP, RegistrarIP, Prefix.

21. Distinctive Call Waiting Tones – The gateway can now play a specific Call Waiting Tone from the Call Progress Tones file. This option enables the called party to distinguish between four different call origins (e.g., external vs. internal calls). This feature is relevant only to Broadsoft's application servers (the tone is played using INFO message).
Relevant parameter: FirstCallWaitingToneID.

22. DNS Service Record (SRV) queries can now also be used to resolve domain names of the Registrar server and any domain name that appears in the Contact and Record-Route headers. SRV can be used to resolve all domain names or just for Proxy servers. If a port is part of the domain name (i.e., <FQDN>:<port>) SRV isn't used.
Relevant parameters: EnableSRVQuery, EnableProxySRVQuery, RegistrarIP.

23. Full support was added for the following coders:

- G.729 Annex B (with no correlation to EnableSilenceCompression).
  G.729 support for Silence Suppression is negotiated between both sides by using the 'annex b' parameter in the SDP body of the SIP messages.

Relevant parameters: CoderName, CoderName_ID.

24. If the coder G.723 is used when silence suppression is enabled, the gateway now includes the string 'annex a' in the SDP.

25. Fax fallback – If T.38 negotiation fails, the gateway can now re-initiate a fax session using the coder G.711 A-law/μ-law with adaptations.
Relevant parameter: IsFaxUsed.

26. It is now possible to configure the gateway to route a call according to its Called Number received in the To header of the SIP INVITE message instead of the user-part of the Request-URI. When configured, the gateway also uses the Username parameter as the user-part of the Contact header.
Relevant parameters: IsUseToHeaderAsCalledNumber, Username.

1.3 Web, SNMP and Command Line New Features

27. 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.

28. 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.

29. 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.

30. 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).

31. 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.

32. 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'.

33. 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 and FQDN (if used) of the Proxy server the gateway currently operates with.

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

35. 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.

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

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

38. 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. Domain names are now resolved using DNS A-Record mechanism if the SRV process fails. In addition, DNS resolution of the Proxy domain name is now applicable even when the Keep-Alive mechanism isn't used.

2. 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.

3. 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 12 to 22)

***ini* File [Web Interface] Parameter Name**	**Description**
CoderName_ID	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 32 kbps (Payload Type = 2). 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) **Note:** If the coder G.729 is selected, the gateway includes 'annexb=no' in the SDP of the relevant SIP messages. If G.729 Annex B is selected, 'annexb=yes' is included. An exception to this logic is when the remote gateway is a Cisco device (IsCiscoSCEMode). ***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 12 to 22)

***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 10 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 32 kbps (Payload Type = 2). g729 – G.729A. g729_AnnexB – G.729 Annex B. **Note:** If the coder G.729 is selected, the gateway includes 'annexb=no' in the SDP of the relevant SIP messages. If G.729 Annex B is selected, 'annexb=yes' is included. An exception to this logic is when the remote gateway is a Cisco device (IsCiscoSCEMode). The RTP packetization period (ptime, in msec) depends on the selected coder name, and can have the following values: G.711 – 10, 20, 30, 40, 50, 60, 80, 100, 120 (default=20). G.729 – 10, 20, 30, 40, 50, 60 (default=20). G.723 – 30, 60, 90 (default = 30). G.726 – 10, 20, 40, 60, 80, 100, 120 (default=20).
SIPTransportType [SIP Transport Layer]	Determines the *default* transport layer used for outgoing SIP calls initiated by the gateway. 0 = UDP (default). 1 = TCP. 2 = TLS (SIPS) (applicable to MP-11x and Mediant 1000 only). **Note:** It is recommended to use TLS to communicate with a SIP Proxy and not for direct gateway-gateway communication.
TCPLocalSIPPort [SIP TCP Local Port]	Local TCP port used to receive SIP messages. The default value is 5060.
EnableSIPS [Enable SIPS]	Applicable to MP-11x and Mediant 1000 only. Enables secured SIP (SIPS) connections over multiple hops. 0 = Disabled (default). 1 = Enabled. When SIPTransportType = 2 (TLS) and EnableSIPS is disabled, TLS is used for the next network hop only. When SIPTransportType = 2 (TLS) or 1 (TCP) and EnableSIPS is enabled, TLS is used through the entire connection (over multiple hops). **Note:** If SIPS is enabled and SIPTransportType = UDP, the connection fails.
TLSLocalSIPPort [SIP TLS Local Port]	Applicable to MP-11x and Mediant 1000 only. Local TLS port used to receive SIP messages. The default value is 5061. **Note:** The value of 'TLSLocalSIPPort' must be different to the value of 'TCPLocalSIPPort'.
SIPSRequireClientCertificate	Applicable to MP-11x and Mediant 1000 only. 0 = The gateway doesn't require client certificate (default). 1 = The gateway (when acting as a server for the TLS connection) requires reception of client certificate to establish the TLS connection. **Note:** The SIPS certificate files can be changed using the parameters 'HTTPSCertFileName' and 'HTTPSRootFileName'.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 12 to 22)

***ini* File [Web Interface] Parameter Name**	**Description**
RegistrarIP [Registrar IP Address]	IP address and optionally port number of Registrar server. Enter the IP address in dotted format notation, for example 201.10.8.1:<5080>. **Note 1:** If not specified, the REGISTER request is sent to the primary Proxy server (refer to 'Proxy IP address' parameter). **Note 2**: When port number is specified, DNS SRV queries aren't performed, even if 'EnableSRVQuery' is set to 1.
Prefix	Prefix = <Destination Phone Prefix>,<Destination IP Address>,<Source Phone Prefix>,<Profile ID> For example: Prefix = 20,10.2.10.2,202,1 Prefix = 10[340-451]xxx#,10.2.10.6,*,1 Prefix = *,gateway.domain.com,* **Note 1:** <destination / source phone prefix> can be single number or a range of numbers. **Note 2:** This parameter can appear up to 50 times. **Note 3:** Parameters can be skipped by using the sign "$$", for example: Prefix = $$,10.2.10.2,202,1 **Note 4:** The <Destination IP Address> field can be either in dotted format notation or a FQDN. This field can also include a selected port to use (in the format: <IP Address>:<Port>).
FirstCallWaitingToneID	Determines the index of the first Call Waiting Tone in the CPT file. This feature enables the called party to distinguish between four different call origins (e.g., external vs. internal calls). The gateway plays the tone received in the 'play tone CallWaitingTone#' parameter of an INFO message + the value of this parameter - 1. The valid range is -1 to 100. The default value is -1 (not used). **Note 1:** It is assumed that all Call Waiting Tones are defined in sequence in the CPT file. **Note 2:** This feature is relevant only to Broadsoft's application servers (the tone is played using INFO message).
EnableProxySRVQuery [Enable Proxy SRV Queries]	Enables the use of DNS Service Record (SRV) queries to discover Proxy servers. 0 = Disabled (default). 1 = Enabled. If enabled and the Proxy IP address parameter contains a domain name without port definition (e.g., ProxyIP = domain.com), an SRV query is performed. The SRV query returns up to four Proxy host names and their weights. The gateway then performs DNS A-record queries for each Proxy host name (according to the received weights) to locate up to four Proxy IP addresses. Therefore, if the first SRV query returns two domain names, and the A-record queries return 2 IP addresses each, no more searches are performed. If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the gateway performs a regular DNS A-record query. **Note:** When enabled, SRV queries are used to discover Proxy servers even if the parameter 'EnableSRVQuery' is disabled.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 12 to 22)

ini File [Web Interface] Parameter Name	Description
EnableSRVQuery [Enable SRV Queries]	Enables the use of DNS Service Record (SRV) queries to resolve Proxy and Registrar servers and to resolve all domain names that appear in the Contact and Record-Route headers. 0 = Disable (default). 1 = Enable. If enabled and the Proxy / Registrar IP address parameter or the domain name in the Contact / Record-Route headers contains a domain name without port definition, an SRV query is performed. The gateway uses the first host name received from the SRV query. The gateway then performs DNS A-record query for the host name to locate an IP address. If the Proxy / Registrar IP address parameter or the domain name in the Contact / Record-Route headers contains a domain name with port definition, the gateway performs a regular DNS A-record query. To enable SRV queries only for Proxy servers, set the parameter 'EnableProxySRVQuery' to 1.
IsUseToHeaderAsCalledNumber	0 = Sets the destination number to the user part of the Request-URI for IP→Tel calls, and sets the 'Contact' header to the source number for Tel→ IP calls (default). 1 = Sets the destination number to the user part of the 'To' header for IP→Tel calls, and sets the 'Contact' header to the *username* parameter for Tel→IP calls.
UseDisplayNameAsSourceNumber [Use Display Name as Source Number]	0 = Interworks the IP Source Number to the Tel Source Number (default). 1 = Sets the Tel Source Number to IP Display Name. Applicable to IP→Tel calls. If enabled, the outgoing Source Number is set to the IP Display Name and Presentation is set to Allowed. If there isn't a Display Name, the user part of the SIP URI is used as the Source Number, and the Presentation is set to Restricted. For example: When the following is received 'from: 100 <sip:200@201.202.203.204>', the outgoing Source Number is set to '100', the Display Name is set to '100' and the Presentation is set to Allowed (0). When the following is received 'from: <sip:100@101.102.103.104>', the outgoing Source Number is set to '100' and the Presentation is set to Restricted (1).
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 12 to 22)

***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> 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 = name1,2,1,0,10,13,15,44,1,1,6000 IPProfile_2 = name2,$$,$$,$$,$,$$,$$,$$,$$,1,$$ $$ = Not configured, the default value of the parameter is used. (*) = Common parameter used in both IP and Tel profiles. **Note 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.
IsFaxUsed [Fax Signaling Method]	Determines the SIP signaling method used to establish and convey a fax session after a fax is detected. 0 = No fax negotiation using SIP signaling (default). 1 = Initiates T.38 fax relay. 2 = Initiates fax using the coder G.711 A-law/μ-law with adaptations (refer to note 1). 3 = Initiates T.38 fax relay. If the T.38 negotiation fails, the gateway re-initiates a fax session using the coder G.711 A-law/μ-law with adaptations (see note 1). **Note 1:** Fax adaptations: Echo Canceller = On Silence Compression = Off Echo Canceller Non-Linear Processor Mode = Off Dynamic Jitter Buffer Minimum Delay = 40 Dynamic Jitter Buffer Optimization Factor = 13 **Note 2:** If the gateway initiates a fax session using G.711 (option 2 and possibly 3), a 'gpmd' attribute is added to the SDP in the following format: For A-law: 'a=gpmd:0 vbd=yes;ecan=on'. For μ-law: 'a=gpmd:8 vbd=yes;ecan=on'. **Note 3:** When 'IsFaxUsed' is set to 1, 2 or 3 the parameter 'FaxTransportMode' is ignored.
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

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 12 to 22)

ini File [Web Interface] Parameter Name	Description
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.
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).
EnableParametersMonitoring	Enables to view changes made on-the-fly to parameters via Web or SNMP. 0 = Deactivate (default). 1 = Activate.
Voice Mail Parameters (MP-1xx FXO and Mediant 1000 FXO only)	
VoiceMailInterface [Voice Mail Interface]	Enables the VM application on the MP-1xx and determines the communication method used between the PBX and the gateway. 0 = None (default). 1 = DTMF. 2 = SMDI (MP-1xx FXO only).
SMDI [Enable SMDI]	Enables the Simplified Message Desk Interface (SMDI) on the gateway. 0 = Normal serial (default). 1 = Enable RS-232 SMDI interface. **Note:** When the RS-232 connection is used for SMDI messages (Serial SMDI) it cannot be used for other applications, for example, to access the Command Line Interface.
SMDITimeOut [SMDI Timeout]	Determines the time (in msec) that the gateway waits for an SMDI Call Status message before or after a Setup message is received. This parameter is used to synchronize the SMDI and analog interfaces. If the timeout expires and only an SMDI message was received, the SMDI message is dropped. If the timeout expires and only a Setup message was received, the call is established. The valid range is 0 to 10000 (10 seconds). The default value is 2000.
LineTransferMode [Line Transfer Mode]	Determines the transfer method used by the gateway. 0 = IP (default). 1 = PBX blind transfer.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 12 to 22)

ini File [Web Interface] Parameter Name	Description
WaitForDialTime [Wait For Dial Time] **Note:** Replaces the obsolete parameter FXOWaitForDialTime.	This parameter is applicable only to FXO gateways. It determines the delay before the gateway starts dialing on the FXO line in the following scenarios: 1. The delay between the time the line is seized and dialing is begun, during the establishment of an IP→Tel call. **Note:** Applicable only to MP-10x/FXO for single stage dialing, when waiting for dial tone (IsWaitForDialTone) is disabled. 2. For call transfer. The delay after hook-flash is generated and dialing is begun. The valid range (in milliseconds) is 0 to 20000 (20 seconds). The default value is 1000 (1 second).
MWIOnCode [MWI On Digit Pattern]	Determines a digit code used by the gateway to notify the PBX of messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string.
MWIOffCode [MWI Off Digit Pattern]	Determines a digit code used by the gateway to notify the PBX that there aren't any messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string.
TelDisconnectCode [Disconnect Call Digit Pattern]	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.
The following digit pattern parameters apply only to VM applications that use the DTMF communication method. For the available patterns' syntaxes, refer to the User's Manual.	
DigitPatternForwardOnBusy [Forward on Busy Digit Pattern]	Determines the digit pattern used by the PBX to indicate 'call forward on busy'. The valid range is a 120-character string.
DigitPatternForwardOnNoAnswer [Forward on No Answer Digit Pattern]	Determines the digit pattern used by the PBX to indicate 'call forward on no answer'. The valid range is a 120-character string.
DigitPatternForwardOnDND [Forward on Do Not Disturb Digit Pattern]	Determines the digit pattern used by the PBX to indicate 'call forward on do not disturb'. The valid range is a 120-character string.
DigitPatternForwardNoReason [Forward on No Reason Digit Pattern]	Determines the digit pattern used by the PBX to indicate 'call forward with no reason'. The valid range is a 120-character string.
DigitPatternInternalCall [Internal Call Digit Pattern]	Determines the digit pattern used by the PBX to indicate an internal call. The valid range is a 120-character string.
DigitPatternExternalCall [External Call Digit Pattern]	Determines the digit pattern used by the PBX to indicate an external call. The valid range is a 120-character string.
Serial parameters (applicable only to the SMDI application).	
SerialBaudRate	Determines the value of the RS-232 baud rate. The valid range is: any value. It is recommended to use the following standard values: 1200, 2400, 9600 (default), 14400, 19200, 38400, 57600, 115200.
SerialData	Determines the value of the RS-232 data bit. 7 = 7-bit. 8 = 8-bit (default).
SerialParity	Determines the value of the RS-232 polarity. 0 = None (default). 1 = Odd. 2 = Even.
SerialStop	Determines the value of the RS-232 stop bit. 1 = 1-bit (default). 2 = 2-bit.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 12 to 22)

ini File [Web Interface] Parameter Name	Description
SerialFlowControl	Determines the value of the RS-232 flow control. 0 = None (default). 1 = Hardware.
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.
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.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 12 to 22)

ini File [Web Interface] Parameter Name	Description
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.
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.
VLAN Parameters	
VlanMode [VLAN Mode]	Sets the VLAN functionality. 0 = Disable (default) 1 = Enable 2 [PassThrough] = N/A.
VlanNativeVlanID [Native VLAN ID]	Sets the native VLAN identifier (PVID, Port VLAN ID). The valid range is 1 to 4094. The default value is 1.
VlanOamVlanID [OAM VLAN ID]	Sets the OAM (Operation, Administration and Management) VLAN identifier. The valid range is 1 to 4094. The default value is 1.
VlanControlVlanID [Control VLAN ID]	Sets the control VLAN identifier. The valid range is 1 to 4094. The default value is 2.
VlanMediaVlanID [Media VLAN ID]	Sets the media VLAN identifier. The valid range is 1 to 4094. The default value is 3.
VlanNetworkServiceClassPriority [Network Priority]	Sets the priority for Network service class content. The valid range is 0 to 7. The default value is 7.
VlanPremiumServiceClassMediaPriority [Media Premium Priority]	Sets the priority for the Premium service class content and media traffic. The valid range is 0 to 7. The default value is 6.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 12 to 22)

ini File [Web Interface] Parameter Name	Description
VlanPremiumServiceClassControlPriority [Control Premium Priority]	Sets the priority for the Premium service class content and control traffic. The valid range is 0 to 7. The default value is 6.
VlanGoldServiceClassPriority [Gold Priority]	Sets the priority for the Gold service class content. The valid range is 0 to 7. The default value is 4.
VlanBronzeServiceClassPriority [Bronze Priority]	Sets the priority for the Bronze service class content. The valid range is 0 to 7. The default value is 2.
EnableDNSasOAM	This parameter applies to both Multiple IPs and VLAN mechanisms. Multiple IPs: Determines the network type for DNS services. VLAN: Determines the traffic type for DNS services. 1 = OAM (default) 0 = Control.
EnableNTPasOAM	This parameter applies to both Multiple IPs and VLAN mechanisms. Multiple IPs: Determines the network type for NTP services. VLAN: Determines the traffic type for NTP services. 1 = OAM (default) 0 = Control.
Multiple IPs Parameters	
EnableMultipleIPs [IP Networking Mode]	Enables / disables the Multiple IPs mechanism. 0 = Disabled (default). 1 = Enabled.
LocalMediaIPAddress [IP Address]	The gateway's source IP address in the Media network. The default value is 0.0.0.0.
LocalMediaSubnetMask [Subnet Mask]	The gateway's subnet mask in the Media network. The default subnet mask is 0.0.0.0.
LocalMediaDefaultGW [Default Gateway Address]	The gateway's default gateway IP address in the Media network. The default value is 0.0.0.0.
LocalControlIPAddress [IP Address]	The gateway's source IP address in the Control network. The default value is 0.0.0.0.
LocalControlSubnetMask [Subnet Mask]	The gateway's subnet mask in the Control network. The default subnet mask is 0.0.0.0.
LocalControlDefaultGW [Default Gateway Address]	N/A. Use the IP Routing table instead (Advanced Configuration > Network Settings).
LocalOAMIPAddress [IP Address]	The gateway's source IP address in the OAM network. The default value is 0.0.0.0.
LocalOAMSubnetMask [Subnet Mask]	The gateway's subnet mask in the OAM network. The default subnet mask is 0.0.0.0.
LocalOAMDefaultGW [Default Gateway Address]	N/A. Use the IP Routing table instead (Advanced Configuration > Network Settings).
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.

Table 1-1: Release 4.6 *ini* File [Web Browser] Parameter Name (continues on pages 12 to 22)

ini File [Web Interface] Parameter Name	Description
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).
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 SIP Compatibility

2.1 Supported SIP Features

The MediaPack SIP main features are:

- Reliable User Datagram Protocol (UDP) transport, with retransmissions.
- Transmission Control Protocol (TCP) Transport layer.
- SIPS using TLS (MP-11x and Mediant 1000 only).
- T.38 real time Fax (using SIP).
  Note: If the remote side includes the fax maximum rate parameter in the SDP body of the INVITE message, the gateway returns the same rate in the response SDP.
- Works with Proxy or without Proxy, using an internal routing table.
- Fallback to internal routing table if Proxy is not responding.
- Supports up to four Proxy servers. If the primary Proxy fails, the MediaPack automatically switches to a redundant Proxy.
- Supports domain name resolving using DNS SRV records for Proxy, Registrar and domain names that appear in the Contact and Record-Route headers.
- Proxy or Registrar Registration (per gateway or per gateway endpoint), such as:

```
REGISTER sip:servername SIP/2.0
VIA: SIP/2.0/UDP 212.179.22.229;branch=z9hG4bRaC7AU234
From: <sip:101@sipgatewayname>;tag=1c29347
To: <sip:101@sipgatewayname>
Call-ID: 10453@212.179.22.229
Seq: 1 REGISTER
Expires: 3600
Contact: sip:101@212.179.22.229
Content-Length: 0
```

The "servername" string is defined according to the following rules:

- The "servername" is equal to "RegistrarName" if configured. The "RegistrarName" can be any string.
- Otherwise, the "servername" is equal to "RegistrarIP" (either FQDN or numerical IP address), if configured.
- Otherwise the "servername" is equal to "ProxyName" if configured. The "ProxyName" can be any string.
- Otherwise the "servername" is equal to "ProxyIP" (either FQDN or numerical IP address).

The **"sipgatewayname"** parameter (defined in the *ini* file or set from the Web browser), can be any string. Some Proxy servers require that the "**sipgatewayname**" (in REGISTER messages) is set equal to the Registrar/Proxy IP address or to the Registrar/Proxy domain name.

The REGISTER message is sent to the Registrar's IP address (if configured) or to the Proxy's IP address. The message is sent per gateway or per gateway endpoint according to the "AuthenticationMode" parameter. Usually the FXS gateways are registered per gateway port, while FXO gateways send a single registration message, where Username is used instead of phone number in From/To headers. The registration request is resent according to the parameter 'RegistrartionTimeDivider'. For example, if 'RegistrationTimeDivider = 70' (%) and Registration Expires time = 3600, the gateway resends its registration request after 3600 x 70% = 2520 sec. The default value of 'RegistrartionTimeDivider' is 50%.

- Proxy and Registrar Authentication (handling 401 and 407 responses) using Basic or Digest methods.
- Single gateway Registration or multiple Registration of all gateway endpoints.
- Configuration of authentication username and password per each gateway endpoint, or single username and password per gateway.
- Supported methods: INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, INFO, REFER, NOTIFY, PRACK, UPDATE and SUBSCRIBE.
- Modifying connection parameters for an already established call (re-INVITE).
- Working with Redirect server and handling 3xx responses.
- Early media (supporting 183 Session Progress).
- PRACK reliable provisional responses (RFC 3262).
- Call Hold and Transfer Supplementary services using REFER, Refer-To, Referred-By, Replaces and NOTIFY.
- Call Forward (using 302 response): Immediate, Busy, No reply, Busy or No reply, Do Not Disturb.
- Supports RFC 3327, Adding 'Path' to Supported header.
- Supports RFC 3581, Symmetric Response Routing.
- Supports RFC 4028, Session Timers in SIP.
- Supports network asserted identity and privacy (RFC 3325 and RFC 3323).
- Supports Tel URI (Uniform Resource Identifier) according to RFC 2806 bis.
- Remote party ID <draft-ietf-sip-privacy-04.txt>.
- Supports obtaining Proxy Domain Name(s) from DHCP (Dynamic Host Control Protocol) according to RFC 3361.
- RFC 2833 Relay for DTMF Digits, including payload type negotiation.
- DTMF out-of-band transfer using:
  - INFO method <draft-choudhuri-sip-info-digit-00.txt>.

- INFO method, compatible with Cisco gateways.
- NOTIFY method <draft-mahy-sipping-signaled-digits-01.txt>.

- SIP URL: sip:"phone number"@IP address (such as 122@10.1.2.4, where "122" is the phone number of the source or destination phone number) or sip:"phone_number"@"domain name", such as 122@myproxy.com. Note that the SIP URI host name can be configured differently per called number.
- Can negotiate coder from a list of given coders.
- Supported 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 32 kbps (10, 20, 30, 40, 50, 60, 80, 100, 120 msec)
  - G.729A/B 8 kbps (10, 20, 30, 40, 50, 60 msec)
- Implementation of MWI IETF <draft-ietf-sipping-mwi-04.txt>, including SUBSCRIBE (to the MWI server). The MediaPack FXS gateways can accept an MWI NOTIFY message that indicates waiting messages or indicates that the MWI is cleared.

2.2 Unsupported SIP Features

The following SIP features are NOT supported:

- MESSAGE method
- Preconditions (RFC 3312)
- SDP - Simple Capability Declaration (RFC 3407)
- Proxy discovery using NAPTR DNS records
- Multicast
- GRUU

2.3 SIP Compliance Tables

The MediaPack SIP gateways comply with RFC 3261, as shown in the following sections.

2.3.1 SIP Functions

Table 2-1: SIP Functions

Function	Supported
User Agent Client (UAC)	Yes
User Agent Server (UAS)	Yes
Proxy Server	Third-party only (Checked with Ubiquity, Delta3, Microsoft, 3Com, Snom and Cisco Proxies)
Redirect Server	Third-party
Registrar Server	Third -party

2.3.2 SIP Methods

Table 2-2: SIP Methods

Method	Supported	Comments
INVITE	Yes	
ACK	Yes	
BYE	Yes	
CANCEL	Yes	
REGISTER	Yes	Send only
REFER	Yes	
NOTIFY	Yes	
INFO	Yes	
OPTIONS	Yes	
PRACK	Yes	
UPDATE	Yes	Receive only

2.3.3 SIP Headers

The following SIP Headers are supported by the MediaPack SIP gateway:

Table 2-3: SIP Headers (continues on pages 26 to 27)

Header Field	Supported
Accept	Yes
Accept–Encoding	Yes
Alert-Info	Yes
Allow	Yes
Also	Yes
Asserted-Identity	Yes
Authorization	Yes
Call-ID	Yes

Table 2-3: SIP Headers (continues on pages 26 to 27)

Header Field	Supported
Call-Info	Yes
Contact	Yes
Content-Encoding	Yes
Content-Length	Yes
Content-Type	Yes
Cseq	Yes
Date	Yes
Diversion	Yes
Encryption	No
Expires	Yes
Fax	Yes
From	Yes
Max-Forwards	Yes
Messages-Waiting	Yes
MIN-SE	Yes
Organization	No
Priority	No
Proxy- Authenticate	Yes
Proxy- Authorization	Yes
Proxy- Require	Yes
Prack	Yes
Record- Route	Yes
Refer-To	Yes
Referred-By	Yes
Remote-Party-ID	Yes
Replaces	Yes
Require	Yes
Remote-Party-ID	Yes
Response- Key	Yes
Retry- After	Yes
Route	Yes
Rseq	Yes
Session-Expires	Yes
Server	Yes
Subject	Yes
Supported	Yes
Timestamp	Yes
To	Yes
Unsupported	Yes
User- Agent	Yes
Via	Yes
Voicemail	Yes
Warning	Yes
WWW- Authenticate	Yes

2.3.4 SDP Headers

The following SDP Headers are supported by the MediaPack SIP gateway:

Table 2-4: SDP Headers

SDP Header Element	Supported
v - Protocol version	Yes
o - Owner/ creator and session identifier	Yes
a - Attribute information	Yes
c - Connection information	Yes
d - Digit	Yes
m - Media name and transport address	Yes
s - Session information	Yes
t - Time alive header	Yes
b - Bandwidth header	Yes
u - Uri Description Header	Yes
e - Email Address header	Yes
i - Session Info Header	Yes
p - Phone number header	Yes
y - Year	Yes

2.3.5 SIP Responses

The following SIP responses are supported by the MediaPack SIP gateway:

- 1xx Response - Information Responses.
- 2xx Response - Successful Responses.
- 3xx Response - Redirection Responses.
- 4xx Response - Request Failure Responses.
- 5xx Response - Server Failure Responses.
- 6xx Response - Global Responses.

2.3.5.1 1xx Response – Information Responses

Table 2-5: 1xx SIP Responses

1xx Response		Supported	Comments
100	Trying	Yes	The SIP gateway generates this response upon receiving of Proceeding message from ISDN or immediately after placing a call for CAS signaling.
180	Ringing	Yes	The SIP gateway generates this response for an incoming INVITE message. On receiving this response, the gateway waits for a 200 OK response.
181	Call is being forwarded	Yes	The SIP gateway does not generate these responses. However, the gateway does receive them. The gateway processes these responses the same way that it processes the 100 Trying response.

Table 2-5: 1xx SIP Responses

1xx Response		Supported	Comments
182	Queued	Yes	The SIP gateway generates this response in Call Waiting service. When SIP gateway receives 182 response, it plays a special waiting Ringback tone to Tel side.
183	Session Progress	Yes	The SIP gateway generates this response if Early Media feature is enabled and if the gateway plays a Ringback tone to IP

2.3.5.2 2xx Response – Successful Responses

Table 2-6: 2xx SIP Responses

2xx Response		Supported	Comments
200	OK	Yes	
202	Accepted	Yes	

2.3.5.3 3xx Response – Redirection Responses

Table 2-7: 3xx SIP Responses

3xx Response		Supported	Comments
300	Multiple Choice	Yes	The gateway responds with an ACK and resends the request to first in the contact list, new address.
301	Moved Permanently	Yes	The gateway responds with an ACK and resends the request to new address.
302	Moved Temporarily	Yes	The SIP gateway generates this response when call forward is used, to redirect the call to another destination. If such response is received, the calling gateway initiates an INVITE message to the new destination.
305	Use Proxy	Yes	The gateway responds with an ACK and resends the request to new address.
380	Alternate Service	Yes	"

2.3.5.4 4xx Response – Request Failure Responses

Table 2-8: 4xx SIP Responses (continues on pages 29 to 31)

4xx Response		Supported	Comments
400	Bad Request	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
401	Unauthorized	Yes	Authentication support for Basic and Digest. On receiving this message the GW issues a new request according to the scheme received on this response
402	Payment Required	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
403	Forbidden	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.

Table 2-8: 4xx SIP Responses (continues on pages 29 to 31)

4xx Response		Supported	Comments
404	Not Found	Yes	The SIP gateway generates this response if it is unable to locate the callee. On receiving this response, the gateway notifies the User with a Reorder Tone.
405	Method Not Allowed	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
406	Not Acceptable	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
407	Proxy Authentication Required	Yes	Authentication support for Basic and Digest. On receiving this message the GW issues a new request according to the scheme received on this response.
408	Request Timeout	Yes	The gateway generates this response if no-answer timeout expired. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
409	Conflict	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
410	Gone	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
411	Length Required	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
413	Request Entity Too Large	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
414	Request-URL Too Long	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
415	Unsupported Media	Yes	If the gateway receives a 415 Unsupported Media response, it notifies the User with a Reorder Tone. The gateway generates this response in case of SDP mismatch.
420	Bad Extension	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
480	Temporarily Unavailable	Yes	If the gateway receives a 480 Temporarily Unavailable response, it notifies the User with a Reorder Tone. This response is issued if there is no response from remote.
481	Call Leg/Transaction Does Not Exist	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
482	Loop Detected	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
483	Too Many Hops	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
484	Address Incomplete	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.

Table 2-8: 4xx SIP Responses (continues on pages 29 to 31)

4xx Response		Supported	Comments
485	Ambiguous	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.
486	Busy Here	Yes	The SIP gateway generates this response if the called party is off hook and the call cannot be presented as a call waiting call. On receiving this response, the gateway notifies the User and generates a busy tone.
487	Request Canceled	Yes	This response indicates that the initial request is terminated with a BYE or CANCEL request.
488	Not Acceptable	Yes	The gateway does not generate this response. On reception of this message, before a 200OK has been received, the gateway responds with an ACK and disconnects the call.

2.3.5.5 5xx Response – Server Failure Responses

Table 2-9: 5xx SIP Responses

5xx Response		Comments
500	Internal Server Error	On reception of any of these Responses, the GW releases the call, sending appropriate release cause to PSTN side. The GW generates 5xx response according to PSTN release cause coming from PSTN.
501	Not Implemented	
502	Bad gateway	
503	Service Unavailable	
504	Gateway Timeout	
505	Version Not Supported	

2.3.5.6 6xx Response – Global Responses

Table 2-10: 6xx SIP Responses

6XX Response		Comments
600	Busy Everywhere	On reception of any of these Responses, the GW releases the call, sending appropriate release cause to PSTN side.
603	Decline	
604	Does Not Exist Anywhere	
606	Not Acceptable	

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 SIP Constraints

3. The 'Netcoder' coder is no longer supported.

4. When using out-of-band DTMF transport (IsDTMFUsed=1), the 'DTMFTransportType' parameter should be set to 0 (erase digits from voice stream).

5. If the (first) incoming INVITE message contains both audio and T.38 coders, the gateway will reply with the first media in SDP and not with an audio coder as was in 4.21 version.

6. G.726, 16 kbps, 24 kbps and 40 kbps coders are not supported. Only G.726 32 kbps is supported.

7. Only the ptime (packetization time) of the first coder in the defined coder list is declared in the SDP section of INVITE / 200 OK messages, even if multiple coders are defined. Therefore, in the Coders screen in the Web Interface only the ptime of the first coder in the list is relevant. For example, if G.711 and G.723 coders are used, the ptime is set to 30 msec.

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

9. In the current Voice Mail (VM) implementation 'Supervised Transfer' isn't supported. Supervised Transfer notifies the VM application if transfer fails because the transferred extension is busy.

3.3 Gateway Constraints

10. 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.

11. It is highly recommended not to select both G.729 and G.729 Annex B coders at the same time.

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. 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.

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

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

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

20. Coder names in *ini* file are case-sensitive.

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

22. 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).

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

24. 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.

25. 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.

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

3.4 Web Constraints

27. 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.

28. When changing gateway parameters from 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.

29. 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.

30. 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.

31. 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.

32. 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

33. Configuration alarm does not clear.

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

35. 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).

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

37. 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 SIP User's Manual.

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

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

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

13. 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.

14. 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.

15. Metering Tones Relay – When an FXO gateway detects a 12/16 kHz metering tone, it now sends an INFO 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.

16. If calling party name is not defined (CallerDisplayInfoX = <name> is not specified per gateway's x port), the calling number can be used instead. Applicable to Tel→IP calls.
    Relevant parameter: UseSourceNumberAsDisplayName.

17. 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.

18. 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.

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

20. 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.

21. 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.

22. 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.

23. 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.

24. Supports the generation of Caller ID with distinctive ringing.
Relevant parameter and value: AnalogCallerIDTimingMode =1.

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

26. 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

27. An option was added to the Tel to IP Routing table to take precedence over a Proxy 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. Only if a match is not found, a Proxy is used.
Relevant parameters: PreferRouteTable, AlwaysSendToProxy, SendInviteToProxy.

28. 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 that if there is no response from the remote party the call is released "internally" with a 408 reason. This "internal" reason can be also used to initiate an alternative call. The timeout for "no response" decision depends on the alternative IP addresses:

    a. If the resolution of the called domain name results with two IP addresses, the "no response" timeout will be according to the number of "Hot-Swap" retransmissions using the parameter 'ProxyHotSwapRtx' (default = 3 retransmissions).

    b. Otherwise the "no response" timeout will be according to the usual number of the SIP retransmissions (7 - default).

    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 Proxy is used to route Tel to IP calls.
    Relevant parameters: AltRouteCauseIP2Tel, AltRouteCauseTel2IP, PSTNPrefix.

29. 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.

30. 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). 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.

31. 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.

32. 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.

33. 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.

34. 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).

35. 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.

36. 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.

37. 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.

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

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

4.1.3 SIP New Features

40. Locating SIP Proxy servers – The gateway can now use DNS Service Record (SRV) queries to discover Proxy servers. If the Proxy IP address parameter contains a domain name without port definition (e.g., ProxyIP = domain.com), an SRV query is performed (if enabled). The SRV query returns up to four Proxy host names and their weights. The gateway then performs DNS A-record queries for each Proxy host name (according to the received weights) to locate up to four Proxy IP addresses. Therefore, if the first SRV query returns two domain names, and the A-record queries return 2 IP addresses each, no more searches are performed.
If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the gateway performs a regular DNS A-record query.
Note: This mechanism is applicable only if 'EnableProxyKeepAlive = 1'.
Relevant parameter: EnableProxySRVQuery.

41. Support for SIP UPDATE method according to RFC 3311 was added (the gateway doesn't initiate UPDATE messages but responds to them).

42. Network Asserted Identity (RFC 3325) supporting both P-Asserted and P-Preferred Identity headers.
Relevant parameters: AssertedIdMode, IsTrustedProxy.

43. Support for the Privacy header (RFC 3323 and RFC 3325) was added. If Caller ID is restricted, the INVITE message will include a Privacy header with "id" parameter (privacy: id). The privacy header is used together with P-asserted or P-preferred headers.

44. Proxy Domain Name(s) can now obtained from a DHCP server according to RFC 3361.

45. Symmetric Response Routing (according to RFC 3581) is now supported. The gateway adds a 'rport' parameter to the Via header field of each SIP message. The first Proxy that receives this message sets the 'rport' value of the response to the actual port from which the request was received. This method is used, for example, to enable the gateway to identify its port mapping outside a NAT.

46. Registration:

- An option was added to configure the gateway's registration name that is used in REGISTER messages.
- A registrar domain name can now be used instead of an IP address.
- Users can now determine the registration timing (in percentage) of the re-register timing that is set by the Registrar.

Relevant parameters: RegistrationTimeDivider, GWRegistrationName, RegistrarName.

47. Registration retry time can now be configured.
Relevant parameter: RegistrationRetryTime.

48. On-the-fly Registration / Unregistration to Proxy/Registrar using the Embedded Web Server's Re-Register button. Users can now unregister and reregister when an endpoint's phone number(s) or other authentication parameters (e.g., username, password) were modified.

49. Message Waiting Indication (MWI) according to IETF <draft-ietf-sipping-mwi-04.txt>, including SUBSCRIBE (to MWI server) is now implemented. MP-1xx/FXS gateways can accept an MWI NOTIFY message that indicates waiting messages or that the MWI is cleared. Users are informed of these messages by a stutter tone, followed by the playing of a continuous dial tone. 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. The gateway can subscribe to this service per port (usually used on FXS) or per gateway (used on FXO).
Relevant parameters: EnableMWI, MWIServerIP, MWIAnalogLamp, MWIDisplay, StutterToneDuration, SubscriptionMode.

50. Subscription / unsubscription to the MWI service can now be controlled via the Supplementary Services screen in the Embedded Web Server.
Relevant parameters: EnableMWISubscription, MWIExpirationTime, SubscribeRetryTime.

51. Support for 'Path Extension Header' according to RFC 3327 was added. The gateway adds a "Path" parameter to the Supported header field of REGISTER messages. This field allows to accumulate the list of Proxies' IP addresses between the gateway and the Registrar. The gateway can also receive the Path header in a response.

52. IP Alert Timeout – Users can now define a timer for the gateway to wait for a 200 OK response from the called party (IP side). If the timer expires, the call is released.
Relevant parameter: IPAlertTimeout.

53. Users can now use the SDP attribute ("a=sendonly") to place the remote party on-hold, in addition to the use of the IP address of 0.0.0.0 and the attribute ("a=inactive").
Relevant parameter: HoldFormat.

54. RFC 2833 Negotiation – If the remote side doesn't include the "telephone-event" parameter in the SDP attributes, the gateway now keeps sending DTMF digits using transparent mode as part of the voice RTP.

55. If the coder G.729 is used with silence suppression enabled, the gateway now includes the string "annex b" in the SDP.

56. Support for Alert-Info header for Distinctive Ringing, for FXS gateways (IP→Tel calls), was added. To use this feature, define several Distinctive Ringing tones in the Call Progress Tones definition file.

57. Can now correctly handle Subscription to DTMF events according to DTMF SUBSCRIBE/ NOTIFY IETF draft (draft-mahy-sipping-signaled-digits-01).

58. Can now configure the sip:URI host part in the OPTIONS message to be either the gateway's IP address or the "gatewayname" parameter.
Relevant parameter: UseGatewayNameForOPTIONS.

4.1.4 SNMP and Web Server New Features

59. 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.

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

61. A 'SIP Channel Status' screen was added to the Embedded Web Server. This screen can be accessed via the 'Channel Status' screen. It contains SIP static information and associated calls information of the selected port.

62. 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.

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

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

65. 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).

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

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

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

69. 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).

70. 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

71. 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".

72. 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 i*ni* 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.

73. 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.

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

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

76. DHCP client improvements. The DHCP client now supports limited IP leasing time and performs lease renewal. In addition, the time server and SIP DHCP options are now supported.

77. 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).

78. 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.

79. 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.

80. 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.

81. 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.

82. 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. Can now handle 401/407 "authentication required" responses for all SIP requests.

2. Passes the called display name to INVITE messages, if it appears in the Refer-To header in a REFER request.

3. Session timer is now supported also for T.38 faxes and for Held calls.

4. Enables SIP destination port configuration for the entire UDP range.

5. Reliable sending of DTMF digits using INFO messages. The gateway now waits for 200OK before sending new DTMF digits.

6. 'SIPDestinationPort', if used, only affects the destination of the INVITE requests, unless 'IsAlwaysUseProxy=1', forcing all SIP messages to be sent to this port.

7. Static NAT is now supported for local IP calls.

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

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

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

11. All request URI's for mid dialog requests issued by the gateway, contains all URI parameters received in contact/record route.

12. Send an immediate NOTIFY (with 100 trying) as a result of a received REFER request.

13. Requests URI's for INVITE request issued as a result of REFER\3xx will contain all URI parameters and new headers received in the REFER to\contact headers.

14. Up to four Proxies are now supported.

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 45 to 58)

***ini* File [Web Interface] Parameter Name**	**Description**
PreferRouteTable [Prefer Routing Table]	Determines if the local Tel to IP routing table takes precedence over a Proxy for routing calls. 0 = Only Proxy is used to route calls (default). 1 = The Proxy checks the 'Destination IP Address' field in the 'Tel to IP Routing' table for a match with the outgoing call. Only if a match is not found, a Proxy is used. **Note:** Applicable only if Proxy is not always used ('AlwaysSendToProxy' = 0, 'SendInviteToProxy' = 0).
EnablePtime	0 = Remove the ptime header from SDP. 1 = Include the ptime header in SDP (default).
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.
CurrentDisconnectDefaultThreshold	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.
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.
SubscriptionMode	Determines the method the gateway uses to subscribe to an MWI server. 0 (Per endpoint) = Each endpoint subscribes separately. This method is usually used for FXS gateways (default). 1 (Per gateway) = Single subscription for the entire gateway. This method is usually used for FXO gateways.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

***ini* File [Web Interface] Parameter Name**	**Description**
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>, <Forwarded SIP User Identification>, <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 Proxy 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.
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).
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.
HoldFormat [Hold Format]	Determines the format of the hold request. 0 = The connection IP address in SDP is 0.0.0.0 (default). 1 = The last attribute of the SDP contains the following "a=sendonly".

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

***ini* File [Web Interface] Parameter Name**	**Description**
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.
EnableProxySRVQuery [Enable Proxy SRV Queries]	Enables the use of DNS Service Record (SRV) queries to discover Proxy servers. 0 = Disabled (default). 1 = Enabled. If enabled and the Proxy IP address parameter contains a domain name without port definition (e.g., ProxyIP = domain.com), an SRV query is performed. The SRV query returns up to four Proxy host names and their weights. The gateway then performs DNS A-record queries for each Proxy host name (according to the received weights) to locate up to four Proxy IP addresses. Therefore, if the first SRV query returns two domain names, and the A-record queries return 2 IP addresses each, no more searches are performed. If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the gateway performs a regular DNS A-record query. **Note:** This mechanism is applicable only if 'EnableProxyKeepAlive = 1'.
ProxyIP [Proxy IP Address]	IP address of the primary Proxy server you are using. Enter the IP address as FQDN or in dotted format notation (for example 201.10.8.1). You can also specify the selected port in the format: <IP Address>:<port>. This parameter is applicable only if you select 'Yes' in the 'Is Proxy Used' field. If you enable Proxy Redundancy (by setting EnableProxyKeepAlive=1), the gateway can function with up to three Proxy servers. If there is no response from the primary Proxy, the gateway tries to communicate with the redundant Proxies. When a redundant Proxy is found, the gateway either continues working with it until the next failure occurs or reverts to the primary Proxy (refer to the 'Redundancy Mode' parameter). If none of the Proxy servers respond, the gateway goes over the list again. The gateway also provides real time switching (hotswap mode), between the primary and redundant proxies ('IsProxyHotSwap=1'). If the first Proxy doesn't respond to INVITE message, the same INVITE message is immediately sent to the second Proxy. **Note 1:** If 'EnableProxyKeepAlive=1', the gateway monitors the connection with the Proxies by using keep-alive messages (OPTIONS). **Note 2:** To use Proxy Redundancy, you must specify one or more redundant Proxies using multiple 'ProxyIP= <IP address>' definitions. **Note 3:** When port number is specified, DNS SRV queries aren't performed, even if 'EnableProxySRVQuery' is set to 1.
ProxyIP [Redundant Proxy IP Address]	IP addresses of the redundant Proxies you are using. Enter the IP address as FQDN or in dotted format notation (for example 192.10.1.255). You can also specify the selected port in the format: <IP Address>:<port>. **Note 1:** This parameter is available only if you select "Yes" in the 'Is Proxy Used' field. **Note 2:** When port number is specified, DNS SRV queries aren't performed, even if 'EnableProxySRVQuery' is set to 1. ***ini* file note:** The IP addresses of the redundant Proxies are defined by the second, third and forth repetition of the *ini* file parameter 'ProxyIP'.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

ini File [Web Interface] Parameter Name	Description
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 INVITE 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.
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 200 OK 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.
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.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

***ini* File [Web Interface] Parameter Name**	**Description**
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 always loads the *cmp* file after it is reset. **Note 2:** The version of the loaded *cmp* file isn't checked.
GWRegistrationName [Gateway Registration Name]	Defines the user name that is used in From and To headers of REGISTER messages. Applicable only to single registration per gateway ('AuthenticationMode = 1). If 'GWRegistrationName' isn't specified (default), the 'Username' parameter is used instead. **Note:** If '"AuthenticationMode=0', all the gateway's endpoints are registered with a user name that equals to the endpoint's phone number.
RegistrarName [Registrar Name]	Registrar Domain Name. If specified, the name is used as Request-URI in REGISTER messages. If isn't specified (default), the Registrar IP address or Proxy name or Proxy IP address is used instead.
RegistrationTimeDivider [Re-registration Timing (%)]	Defines the re-registration timing (in percentage). The timing is a percentage of the re-register timing set by the Registration server. The valid range is 50 to 100. The default value is 50. For example: If 'RegistrationTimeDivider = 70' (%) and Registration Expires time = 3600, the gateway resends its registration request after 3600 x 70% = 2520 sec.
IPAlertTimeout [Tel to IP No Answer Timeout]	Defines the time (in seconds) the gateway waits for a 200 OK response from the called party (IP side) after sending an INVITE message. If the timer expires, the call is released. The valid range is 0 to 3600. The default value is 180.
MINSE [Minimum Session-Expires]	Defines the time (in seconds) that is used in the Min-SE header field. This field defines the minimum time that the user agent supports for session refresh. The valid range is 10 to 100000. The default value is 90.
MaxActiveCalls [Max Number of Active Calls]	Defines the maximum number of calls that the gateway can have active at the same time. If the maximum number of calls is reached, new calls are not established. The default value is max available channels (no restriction on the maximum number of calls). The valid range is 0 to max number of channels.
IsUserPhoneInFrom [Use "user=phone" in From header]	0 = Doesn't use ";user=phone" string in From header (default). 1 = ";user=phone" string is part of the From header.
UseSourceNumberAsDisplayName [Use Source Number as Display Name]	0 = Interworks the Tel calling name to SIP Display Name (default). 1 = Set Display Name to Source Number if not available from Tel. Applicable to Tel→IP calls. If enabled and calling party name is not defined (CallerDisplayInfoX = <name> is not specified per gateway's x port), the calling number is used instead.
UseGatewayNameForOptions [Use Gateway Name for OPTIONS]	0 = Use the gateway's IP address in keep-alive OPTIONS messages (default). 1 = Use 'GatewayName' in keep-alive OPTIONS messages. The OPTIONS Request-URI host part contains either the gateway's IP address or a string defined by the parameter 'Gatewayname'. The gateway uses the OPTIONS request as a keep-alive message to its primary and redundant Proxies.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

ini File [Web Interface] Parameter Name	Description
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:** If NSE mode is enabled the SDP contains the following line: "a=rtpmap:100 X-NSE/8000" **Note 3:** 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.711μ-Law, according to the parameter 'FaxModemBypassCoderType'. The payload type used with these G.711 coders is a standard one (8 for G.711 A-Law and 0 for G.711 μ-Law). The parameters defining payload type for the "old" 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.
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.
RegistrationRetryTime [Registration Retry Time]	Defines the time period (in seconds) after which a Registration request is resent if registration fails with 4xx, or there is no response from the Proxy/Registrar. The default is 30 seconds. The range is 10 to 3600.
AssertedIdMode [Asserted Identity Mode]	0 = None (default). 1 = P-asserted. 2 = P-preferred. The Asserted ID mode defines the header that is used in the generated INVITE request. The header also depends on the calling Privacy: allowed or restricted. The P-asserted (or P-preferred) headers are used if the originating party has a Caller ID name. The Caller ID name is presented as a display name in the P-asserted (or P-preferred) headers. P-asserted (or P-preferred) headers are used together with the Privacy header. If Caller ID is restricted the "Privacy: id" will be included. Otherwise for allowed Caller ID the "Privacy: none" will be used. If Caller ID is restricted (received from Tel or configured in the gateway), the From header is set to <anonymous@anonymous.invalid>.
IsTrustedProxy [Is Proxy Trusted]	0 = The SIP Proxy is not Trusted. 1 = SIP Proxy is Trusted (default). If Proxy is not Trusted, the P-asserted header is not used.
AddTON2RPI [Add Number Plan and Type to Remote Party ID Header]	0 = TON/PLAN parameters aren't included in the RPID header. 1 = TON/PLAN parameters are included in the RPID header (default). If RPID header is enabled (EnableRPIHeader = 1) and 'AddTON2RPI=1', it is possible to configure the calling and called number type and number plan using the Number Manipulation tables for Tel→IP calls.
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 45 to 58)

***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 examples: 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 $$ = 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.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

***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 32 kbps (Payload Type = 35). 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' equals 1 or 2. ***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
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.
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.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

***ini* File [Web Interface] Parameter Name**	**Description**
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.
AltRouteCauseTel2IP [Reasons for Alternative Routing Table]	Table of call failure reason values received from the IP side. 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. For example: AltRouteCauseTel2IP = 408 (Response timeout). AltRouteCauseTel2IP = 486 (User is busy). **Note 1:** The 408 reason can be used to specify that there was no response from the remote party to the INVITE request. **Note 2:** This parameter can appear up to 4 times.
AltRouteCauseIP2Tel [Reasons for Alternative Routing Table]	Table of call failure reason values received from the telephony side (in SIP 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. For example: AltRouteCauseIP2Tel = 3 (No route to destination). AltRouteCauseIP2Tel = 17 (Busy here). **Note:** This parameter can appear up to 4 times.
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 Contact header in the INVITE 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 single 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 45 to 58)

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 $$. i = Source IP address (obtained from the Contact header in the INVITE message). The 'b' to 'd' manipulation rules are applied if the called and calling numbers match the 'a', 'g' and 'i' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign "$$", for example: NumberMapIP2Tel =01,2,972,$$,$$,$$,034,$$,10.13.77.8 NumberMapIP2Tel =03,(2),667,$$,$$,$$,22 **Note:** The Source IP address can include the "x" wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99.
NumberMapTel2IP [Destination Phone Number Manipulation Table for Tel→IP calls]	Manipulates the destination number for Tel to IP calls. NumberMapTel2IP = a,b,c,d,e,f,g a = Destination number prefix b = Number of stripped digits from the left, or (if brackets are used) from the right. A combination of both options is allowed. c = String to add as prefix, or (if brackets are used) as suffix. A combination of both options is allowed. d = Number of remaining digits from the right e = Number Plan used in RPID header f = Number Type used in RPID header g = Source number prefix The 'b' to 'f' manipulation rules are applied if the called and calling numbers match the 'a' and 'g' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign "$$", for example: NumberMapTel2IP=01,2,972,$$,0,0,$$ NumberMaPTel2IP=03,(2),667,$$,0,0,22 **Note:** Number Plan & Type can optionally be used in Remote Party ID (RPID) header by using the 'EnableRPIHeader' and 'AddTON2RPI' parameters.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

***ini* File [Web Interface] Parameter Name**	**Description**
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 = Number Plan used in RPID header f = Number Type used in RPID header 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 **Note 1:** 'Presentation' is set to 'Restricted' only if 'Asserted Identity Mode' is set to 'P-Asserted'. **Note 2:** Number Plan & Type can optionally be used in Remote Party ID (RPID) header by using the 'EnableRPIHeader' and 'AddTON2RPI' parameters.
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' 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 "$$", for example: NumberMapIP2Tel =01,2,972,$$,$$,$$,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 45 to 58)

***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.
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.
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.

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

ini File [Web Interface] Parameter Name	Description
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 KeyCLIRDeact=*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.
EnableMWI [Enable MWI]	Enable 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.
EnableMWISubscription [Subscribe for MWI]	0 = Disable MWI subscription (default). 1 = Enable subscription to MWI (to MWIServerIP address).
MWIExpirationTime [MWI Subscribe Expiration Time]	MWI subscription expiration time in seconds. The default is 7200 seconds. The range is 10 to 72000.
SubscribeRetryTime [MWI Subscribe Retry Time]	Subscription retry time in seconds. The default is 120 seconds. The range is 10 to 7200.
MWIServerIP [MWI Server IP Address]	MWI server IP address. If provided, the gateway subscribes to this IP address. Can be configured as a numerical IP address or as a domain name. If not configured, the Proxy IP address is used instead.
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.
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.
StutterToneDuration [Stutter Tone Duration]	Duration (in msec) of the played stutter dial tone that indicates waiting message(s). The default is 2000 (2 seconds). The range is 1000 to 60000.
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).

Table 4-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 45 to 58)

ini File [Web Interface] Parameter Name	Description
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.
CurrentDisconnectDuration	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.
AnalogCallerIDTimimgMode	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.
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.
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.
IsCiscoSCEMode	0 = There isn't a Cisco gateway at the remote side (default). 1 = There is a Cisco gateway at the remote side. When there is a Cisco gateway at the remote side, the local gateway must set the value of the "annexb" parameter of the fmtp attribute in the SDP to "no". This logic should be used if 'EnableSilenceCompression = 2' (enable without adaptation). In this case, Silence Suppression should be used on the channel but not declared in the SDP.
SNMP Parameters	
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".

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