AudioCodes Systems for Wireline Networks

Mediant™ 2000 VoP Media Gateway

Mediant™ 2000 & TP-1610 SIP Release Notes

Version 4.4

Document #: LTRT-69005

AudioCodes

Notice

This document describes the release of the AudioCodes Mediant 2000™ SIP Gateway and TP-1610/SIP cPCI board.

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: Jan-12-2005 Date Printed: Jan-13-2005

Table of Contents

List of Tables

Tip: When viewing this manual on CD, Web site or other electronic copies, all cross-references are hyperlinked, so just click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly.

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-688xx	Mediant 2000 SIP User's Manual (e.g., LTRT-68801)
LTRT-701xx	Mediant 2000 Fast Track Installation Guide

Document Revision History

Version	LTRT Number	Reason for Change	Date
4.4 Beta	69004	New software release	Aug-01-2004
4.4 GA	69005	New software release	Jan-12-2005

Reader's Notes

1 What's New in Release 4.4

1.1 General Gateway New Features

1. Supporting TDM Tunneling - The Mediant 2000 TDM Tunneling feature allows you to tunnel groups of digital trunk spans or timeslots (B-channels) over the IP network. TDM Tunneling utilizes the internal routing capabilities of the Mediant 2000 (working without Gatekeeper control) to receive voice and data streams from TDM (1 to 16 E1/T1/J1) spans or individual timeslots, convert them into packets and transmit them automatically over the IP network (using point-to-point or point-to-multipoint gateway distributions). A Mediant 2000 opposite it (or several Mediant 2000 gateways, when point-to-multipoint distributions is used) converts the IP packets back into TDM traffic. Each timeslot can be targeted to any other timeslot within a trunk in the opposite Mediant 2000.
   Relevant parameters: EnableTDMoverIP, ProtocolType = 4 or 5 (Transparent), CASTransportType = 1 (CAS signaling relay using RFC 2833).
2. Support for SS7 tunneling was added. The SS7 tunneling feature facilitates peer-to-peer transport of SS7 links between gateways that support AudioCodes' unique MTP2 Tunneling application (M2TN) for transferring SS7 MTP2 link data over IP. In this scenario, both sides of the link are pure TDM switches and are unaware of the IP tandem that is utilized between them. Using M2TN, the network operator can support SS7 connections over IP, carrying MTP level 3, as well as higher level SS7 layers (e.g., user parts and application protocols, such as TUP, ISUP, SCCP, TCAP, etc.).
   For the relevant parameters refer to the Mediant 2000 SIP User's Manual.
3. 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 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 B-channel. For example, B-channels 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 Mediant 2000 SIP User's Manual.
4. 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.
5. Support for VXML calling card application was added. The Mediant 2000 calling card application capability (included in its IVR - Interactive Voice Response - feature) enables Internet Telephony Service Providers (ITSPs) to provide a VoIP telephone service to subscribers who have purchased calling cards in advance.
   For the relevant parameters refer to the Mediant 2000 SIP User's Manual.
6. NI-2 Calling Name – Interworking of PRI to SIP, and SIP to PRI Calling Name.
   The Calling Name can be received via one of these methods:
   - A Facility IE in the Setup message that includes the Calling Name.
   - A Facility IE in the Setup message signals that additional information is following. After the Setup message, a Facility message is received that includes a Facility IE with the Calling Name information (applicable only to NT→TE direction).
7. Cisco™ NSE mode is now supported for fax pass-through, in addition to the existing support for modem.
   Relevant parameters: NSEMode, NSEPayloadType.

8. Advice of Charge (AOC) – The gateway now supports reception of ISDN (Euro ISDN) AOC messages. These messages can be received during a call (Facility messages) or at the end of a call (Disconnect or Release messages). The gateway converts the AOC messages into SIP Info (during a call) and Bye (end of a call) messages using a proprietary AOC SIP header. The gateway supports both Currency and Pulse AOC messages.
   Relevant parameter: EnableAOC.
9. Max call duration – Users can now limit the maximum duration of a call. When this time expires, the call is released (from both sides - IP and Tel).
   Relevant parameter: MaxCallDuration.
10. 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.
11. 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.
12. The following RADIUS enhancements were added:
    - An Accounting Start report.
    - A unique Session-ID was added to the start and stop accounting messages to correlate between messages of the same call.
    - Additional fields were added to the accounting report: Call Setup Time, Call Connect Time and Call Release Time.

    Relevant parameter: RadiusAccountingType.
13. If the gateway receives an ISDN Disconnect message with Progress Indicator = 1 or 8 before a Connect message is received, it now sends a 183 message to IP. If PI is not received in the Disconnect message, the call is released. Thus, a voice channel is opened to play announcements. The 'PIForDisconnectMsg' parameter can be used to override the PI value that is received in the ISDN Disconnect message.
    Relevant parameter: PIForDisconnectMsg.
14. Playing Ringback Tone (RBT) to Tel for ISDN calls– The gateway is now capable of deciding whether the RBT is played to the subscriber by the gateway itself or by the PBX. This feature can be used when the PBX is not capable to play the RBT by itself.
    Relevant parameter: LocalISDNRBToneSource.
15. NI-2 second redirect number – Users can now select and use (in Invite messages) the NI-2 second redirect number, if two redirect numbers were received in Q.931 Setup for incoming Tel→IP calls.
    Relevant parameter: ISDNInCallsBehavior_x = 262144.
16. Support for partial retrieval of the Redirect Number (number only) from a Facility IE in the Setup message was added. Applicable to Redirect number according to ECMA-173 Call Diversion Supplementary Services.
    Relevant parameters: SupportRedirectInFacility, ISDNDuplicateQ931BuffMode = 1.
17. CAS NFA transfer – The gateway now supports the CAS NFA DMS-100 protocol, including blind transfer (using Refer) to remote PBX extension.
    Relevant parameter: TrunkTransferMode_X.
18. If calling party name isn't received in the incoming PRI call Setup, the calling number can be used instead. Applicable to Tel→IP calls.
    For CAS gateways, if 'UseSourceNumberAsDisplayName = 1', the calling number is used as the Caller Name in Invite messages.
    Relevant parameter: UseSourceNumberAsDisplayName.

19. MFC R2 Brazil "Clear Back" feature is now supported – When the PBX sends a Suspend signal to the gateway, the Mediant 2000 starts a Regret Timer and sends a Hold Re-Invite message to the IP. If the gateway receives an Unhold message from the PBX, it sends a Retrieve Re-Invite message to the IP. If the timer expires, a Release message is sent to the IP. If a Release message is received from the PBX, the gateway releases the IP call. If Release message is received from the IP, the gateway releases the PBX call.
Relevant parameters: RegretTime, EnableHold. (If EnableHold = 0, the Re-Invite message isn't sent).
20. MFC R2 Brazil Hold Timeout is now supported – When the gateway receives a Hold message from the IP, it starts a timer. If this timer expires before Unhold Re-Invite is received, the gateway releases the IP call.
Relevant parameter: HeldTimeout.
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. T.38 Redundancy Enhancement - The redundancy of the low speed data is now determined according to the enhanced redundancy parameter.
23. 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 parameter: FaxTransportType = 3 (Transparent with events).
24. Alert Timeout (ISDN T2 timer) for outgoing call to PSTN can now be configured.
Relevant parameter: PSTNAlertTimeout.
Note: The PSTN stack T2 timer can be overridden by a lower value, but it can't be increased.

1.2 Routing and Manipulation New Features

25. 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 1: 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).

    Note 2: 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.
26. 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.

27. Internal DNS table was added - Similar to a DNS resolution, translates hostnames into IP addresses. This table is used when hostname translation is required (e.g., 'Tel to IP Routing' table, 'Gatekeeper IP Address', etc.). Two different IP addresses can be assigned to the same hostname. If the hostname isn't found in this table, the gateway communicates with an external DNS server. Up to 10 hostnames can be configured.
Relevant parameter: Dns2IP.
28. 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.
29. Enhanced IP to Tel routing selection - Selection of trunk groups and IP Profiles (optional) can now be performed according to Destination number, Source Number and Source IP address.
Relevant parameter: PSTNPrefix.
30. 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.
31. IP addresses can now include wildcards – IP addresses in the 'Source IP Address' column of the 'IP to Trunk 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.
32. 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.
33. 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.
34. IP DiffServ code can now be configured for SIP signaling protocol in addition to RTP Diffserv.
Relevant parameter: ControlIPDiffServ.
35. An option to configure the Calling Number Presentation (Allowed or Restricted) per Tel to IP and IP to ISDN calls was added (using the Source Number Manipulation table).
36. The Called Number Manipulation table was increased to 50 rows. The Calling Number Manipulation table was increased to 20 rows.

1.3 SIP New Features

37. Carrier Identification Code (CIC) feature – An option was added to relay the CIC from IP to ISDN in Transit IE. The CIC code (4 digits) is received in the Invite Request-URI.
Relevant parameter: EnableCIC.

38. 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.
39. Connect on Progress Indicator – After receiving a 183 Session Progress, the gateway can optionally send a Connect message to the ISDN side. This enables the opening of a voice channel for receiving announcements from the IP.
    Relevant parameter: ConnectOnProgressInd.
40. Supports SIP2QSIG IETF draft-ietf-sipping-qsig2sip-04.txt, including interworking between 180/183 responses with SDP and Q.931 Progress messages.
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. Support for the 'Transparent' coder was added. The 'Transparent' coder can be used in TDM tunneling applications to relay the TDM signaling bearers.
    Relevant parameters: Coder = Transparent, TransparentPayloadType.
47. 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.
48. Registration retry time can now be configured.
    Relevant parameter: RegistrationRetryTime.
49. On-the-fly Registration / Unregistration to Proxy/Registrar using the Embedded Web Server's Re-Register button. Users can now unregister and reregister after authentication parameters (e.g., username, password) were modified.
50. 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.

51. 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.
52. 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.
53. If the gateway receives a SIP Invite message with an RPID header in which the "privacy" parameter equals "full", the gateway now removes the Calling Display Name IE from the PRI Setup message.
54. Asserted Identity – P-asserted or P-preferred headers are now sent in 180 Ringing and 200 OK messages if received in the initial Invite message.
55. 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.
56. If the coder G.729 is used with silence suppression enabled, the gateway now includes the string "annex b" in the SDP.
57. 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.

1.4 SNMP and Web Server New Features

58. The gateway's Web Interface appearance was updated and enhanced.
59. 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.
60. 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.
61. A radio button was added alerting the user whether to burn or not to burn changes to flash during reset.
62. New SNMP MIB for collection and monitoring system performance.
63. 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).
64. Enable private labeling of the Web browser's title when a graphical logo is used.
65. Adding the capability to provision the table of authorized SNMP managers.
66. In addition to acBoard MIB, a new set of MIBs for configuration and status is introduced. The new MIBs are divided by functionality (Media, Control, System).

1.5 Miscellaneous New Features

67. 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".

68. 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.

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

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

71. 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.

72. 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).

73. 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.

74. 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 'BurnCASFile' parameters are no longer supported.

75. 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.

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

1.6 Resolved Constraints

1. The G.729A internal processing mechanism was enhanced to achieve better performance results on high load situations.

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

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

4. Supports the compact header (x) for Session expires.

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

6. Enables SIP destination port configuration for the entire UDP range.
7. Static NAT is now supported for local IP calls.
8. Reliable sending of DTMF digits using INFO messages. The gateway now waits for 200OK before sending new DTMF digits.
9. 'SIPDestinationPort', if used, only affects the destination of the INVITE requests, unless 'IsAlwaysUseProxy=1', forcing all SIP messages to be sent to this port.
10. Several SNMP managers can now be configured to access the gateway concurrently.
11. DHCP now supports limited IP leasing time. The gateway performs lease renewal and initiates a new DHCP request when the lease time expires.
12. All request URI's for mid dialog requests issued by the gateway, contains all URI parameters received in contact/record route.
13. Send an immediate NOTIFY (with 100 trying) as a result of a received REFER request.
14. 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.
15. Up to four Proxies are now supported.

1.7 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 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

ini File [Web Interface] Parameter Name	Description
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 work 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'). This mode supports only two proxies. 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 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

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.
MaxCallDuration [Max Call Duration (sec)]	Defines the maximum call duration in seconds. If this time expires, both sides of the call are released (IP and Tel). The default time is 0 seconds (no limitation).
RadiusAccountingType [RADIUS Accounting Type]	Determines when a RADIUS accounting report is issued. 0 = At the Release of the call only (default). 1 = At the Connect and Release of the call. 2 = At the Setup and Release of the call.
RegretTime	Determines the time period (in seconds) the gateway waits for an MFC R2 Resume (Reanswer) signal once a Suspend (Clear back) signal was received from the PBX. If this timer expires, the call is released. The valid range is 0 to 255. The default value is 0. Applicable only for MFC R2 CAS Brazil variant.
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".
HeldTimeout	Determines the time period the gateway can stay on-hold. If a Resume (un-hold Re-Invite) message is received before the timer expires, the call is renewed. If this timer expires, the call is released. -1 = Indefinitely (default). 0 - 2400 =Time to wait in seconds. Currently applicable only to MFC R2 CAS variants.
ConnectOnProgressInd	0 = Connect message isn't sent after 183 Session Progress is received (default). 1 = Connect message is sent after 183 Session Progress is received. This feature enables the play of announcements from IP to PSTN without the need to answer the Tel→IP call. It can be used with PSTN networks that don't support the opening of a TDM channel before an ISDN Connect message is received.
EnableCIC	0 = Do not relay the Carrier Identification Code (CIC) to ISDN (default). 1 = CIC is relayed to ISDN in Transit Network Selection IE. If enabled, the CIC code (received in an Invite Request-URI) is included in a TNS IE in ISDN Setup message. For example: INVITE sip:555666;cic=2345@100.2.3.4 sip/2.0. **Note:** Currently this feature is supported only in SIP→ISDN direction.
PIForDisconnectMsg [Send PI in Disconnect Message]	Defines the gateway's behavior when a Disconnect message is received from the ISDN before a Connect message was received. "Not configured" = Sends a 183 message according to the received PI in the ISDN Disconnect message. If PI = 1 or 8, the gateway sends a 183 response, enabling the PSTN to play a voice announcement to the IP side. If there isn't a PI in the Disconnect message, the call is released (default). 0 = Do not send a 183 message to IP. The call is released. 1, 8 = Sends 183 message to IP.
LocalISDNRBToneSource [Local ISDN RBT Source]	Determines whether Ringback tone is played to the ISDN by the PBX / PSTN or by the gateway. 0 = PBX / PSTN (default). 1 = Gateway. This parameter is applicable to ISDN protocols. It is used simultaneously with the parameter 'PlayRBTone2TEL'.

Table 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

ini File [Web Interface] Parameter Name	Description
SupportRedirectInFacility	0 = Not Supported (default). 1 = Supports partial retrieval of Redirect Number (number only) from a Facility IE in ISDN Setup messages. Applicable to Redirect number according to ECMA-173 Call Diversion Supplementary Services. **Note:** To enable this feature, 'ISDNDuplicateQ931BuffMode' must be set to 1.
TrunkTransferMode_X	0 = Not supported (default). 1 = Supports CAS NFA DMS-100 transfer. When a SIP Refer message is received, the gateway performs a Blind Transfer by executing a CAS Wink and dialing the Refer-to number to the Switch and then releasing the call. **Note:** A specific NFA CAS table is required.
IniFileURL	Specifies the name of the *ini* file and the location of the TFTP server from which the gateway loads the *ini* and configuration files. For example: tftp://192.168.0.1/filename tftp://192.10.77.13/config<MAC> **Note:** The optional string "<MAC>" is replaced with the gateway's MAC address. Therefore, the gateway requests an *ini* file name that contains its MAC address. This option enables loading different configurations for specific gateways.
CmpFileURL	Specifies the name of the *cmp* file and the location of the TFTP server from which the gateway loads a new *cmp* file and updates itself. For example: tftp://192.168.0.1/filename **Note 1:** When this parameter is set in the *ini* file, the gateway always loads the *cmp* file after it is reset. **Note 2:** The version of the loaded *cmp* file isn't checked.
TransparentPayloadType	Specifies the payload type that is used when the selected coder is set to 'Transparent'. The valid range is 96-120. The default value is 56.
GWRegistrationName [Gateway Registration Name]	Defines the user name that is used in From and To headers of Register messages. If 'GWRegistrationName' isn't specified (default), the 'Username' parameter is used instead.
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 [Tel2IP 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 240.
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 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

ini File [Web Interface] Parameter Name	Description
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.
UseSourceNumberAsDisplay Name [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 if the incoming Tel to IP call doesn't contain the calling party name, the calling number is used instead. All CAS protocols don't provide the calling party name. Therefore, in CAS, if this parameter is enabled, the Display Name is identical to the calling number.
SIP183Behavior [Behavior of 183 message]	Defines the ISDN message that is sent when 183 Session Progress message is received for IP→Tel calls. 0 = Progress message (default). 1 = Alert message. When set to 1, the gateway sends an Alert message (after the receipt of a 183 response) instead of an ISDN Progress message.
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.

Table 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

ini File [Web Interface] Parameter Name	Description
PlayRBTone2Tel [Play Ringback Tone to TEL]	0 (Don't play) = The ISDN / CAS gateway doesn't play a Ringback Tone (RBT). No PI is sent to the ISDN, unless the parameter 'Progress Indicator to ISDN' is configured differently. 1 (Play) = The CAS gateway plays a local RBT to PSTN after receipt of a 180 ringing response (with or without SDP). **Note:** Reception of a 183 response doesn't cause the CAS gateway to play an RBT (unless 'SIP183Behavior = 1'). The ISDN gateway functions according to the parameter 'LocalISDNRBToneSource': • If the ISDN gateway receives a 180 ringing response (with or without SDP) and 'LocalISDNRBToneSource = 1', it plays a RBT and sends an Alert with PI = 8 (unless the parameter 'Progress Indicator to ISDN' is configured differently). • If 'LocalISDNRBToneSource = 0', the ISDN gateway doesn't play an RBT and an Alert message (without PI) is sent to the ISDN. In this case, the PBX / PSTN should play the RBT to the originating terminal by itself. **Note:** Reception of a 183 response doesn't cause the ISDN gateway to play an RBT; the gateway issues a Progress message (unless 'SIP183Behavior = 1'). If 'SIP183Behavior = 1', the 183 response is treated the same way as a 180 ringing response. 2 = Play according to "early media" (default). If a 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the ISDN / CAS gateway doesn't play the RBT; PI = 8 is sent in an ISDN Alert message (unless the parameter 'Progress Indicator to ISDN' is configured differently). If a 180 response is received but the "early media" voice channel is not opened, the CAS gateway plays an RBT to the PSTN; the ISDN gateway functions according to the parameter 'LocalISDNRBToneSource': • If 'LocalISDNRBToneSource = 1', the ISDN gateway plays an RBT and sends an ISDN Alert with PI = 8 to the ISDN (unless the parameter 'Progress Indicator to ISDN' is configured differently). • If 'LocalISDNRBToneSource = 0', the ISDN gateway doesn't play an RBT. No PI is sent in the ISDN Alert message (unless the parameter 'Progress Indicator to ISDN' is configured differently). In this case, the PBX / PSTN should play an RBT tone to the originating terminal by itself. **Note:** Reception of a 183 response results in an ISDN Progress message (unless 'SIP183Behavior = 1'). If 'SIP183Behavior = 1' (183 is handled in the same way as a 180+SDP), the gateway sends an Alert message with PI = 8, without playing an RBT.
PlayBusyTone2ISDN	This parameter enables the Mediant 2000 ISDN gateway to play a Busy or a Reorder tone to the PSTN after a call is released. 0 = Immediately sends an ISDN Disconnect message (default). 1 = Sends an ISDN Disconnect message with PI=8 and plays a Busy or a Reorder tone to the PSTN (depending on the release cause). 2 = Delays the sending of an ISDN Disconnect message for 'TimeForReorderTone' seconds and plays a Busy or a Reorder tone to the PSTN. Applicable only if the call is released from the IP before it reaches the Connect state. Otherwise, the Disconnect message is sent immediately and no tones are played.
EnableAOC	0 = Not used (default). 1 = ISDN Advice of Charge (AOC) messages are interworked to SIP. The gateway supports reception of ISDN (Euro ISDN) AOC messages. AOC messages can be received during a call (Facility messages) or at the end of a call (Disconnect or Release messages). The gateway converts the AOC messages into SIP Info (during a call) and Bye (end of a call) messages using a proprietary AOC SIP header. The gateway supports both Currency and Pulse AOC messages.

Table 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

ini File [Web Interface] Parameter Name	Description
EnableTDMoverIP	0 = Disabled (default). 1 = TDM Tunneling is enabled. When TDM Tunneling is enabled, the originating Mediant 2000 automatically initiates SIP calls from all enabled B-channels belonging to the E1/T1/J1 spans that are configured with the 'Transparent' protocol. The called number of each call is the internal phone number of the B-channel that the call originates from. The IP to Trunk Group routing table is used to define the destination IP address of the terminating Mediant 2000. The terminating Mediant 2000 gateway automatically answers these calls if its E1/T1 protocol is set to 'Transparent' (ProtocolType = 5).
CASTransportType	0 = Disable CAS relay (default). 1 = Enable CAS relay mode using RFC 2833. The CAS relay mode can be used with the TDM tunneling feature to enable tunneling over IP for both voice and CAS signaling bearers.
ISDNDMSTimerT310	Overrides the T310 timer for the DMS-100 ISDN variant. This parameter enables users to increase the 10 seconds timeout from call Setup until Alert is received up to 30 seconds. The valid range is 10 to 30. The default value is 10 (seconds). **Note:** Applicable only to Nortel DMS and Nortel MERIDIAN PRI variants (ProtocolType = 14 and 35).
ISDNJapanNTTTimerT3JA	T3_JA timer (in seconds). This parameter overrides the internal PSTN T3 timeout on the Users Side (TE side). If an outgoing call from the Mediant 2000 to an ISDN subscriber is not answered during this timeout, the call is released. The valid range is 10 to 180. The default value is 50. Applicable only to Japan NTT PRI variant (ProtocolType = 16).
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 (received from PSTN) is restricted, 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 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

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>, <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,1,2,0,10,5,22,33,2,22,34,1,1 TelProfile_2 = ModemProfile,0,10,13,$$,$$,$$,$$,$$,0,$$,0,1 $$ = Not configured, the default value of the parameter is used. (*) = Common parameter used in both IP and Tel profiles. **Note 1:** The Tel ProfileID can be used in the Trunk 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 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

ini File [Web Interface] Parameter Name	Description
TrunkGroup_x [Trunk Group Table]	TrunkGroup_x = T/a-b,c,d x = Trunk group ID (1 to 99). T = Physical trunk number (0 to 7). a = Starting B-channel (from 1). b = Ending B-channel (up to 31). c = Phone number associated with the first channel (optional). d = Optional Tel Profile ID (1 to 5). For example: TrunkGroup_1 = 0/1-31,1000 (for E1 span). TrunkGroup_1 = 1/1-31,$$,1. TrunkGroup_2 = 2/1-24,3000 (for T1 span). Trunk group is the recommended method to configure the gateway's B-channels. The parameter 'ChannelList' (although still supported) mustn't be used simultaneously with Trunk Groups. **Note 1:** An optional Tel Profile ID (1 to 5) can be applied to each group of B-channels. **Note 2:** Parameters can be skipped by using the sign "$$".
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 6.3 kbps (default). g7231r53 – G.723 5.3 kbps. g726 – G.726 ADPCM 32 kbps (Payload Type = 2). g729 – G.729A. NetCoder6_4 – NetCoder 6.4 kbps. NetCoder7_2 – NetCoder 7.2 kbps. NetCoder8 – NetCoder 8.0 kbps. NetCoder8_8 – NetCoder 8.8 kbps. Transparent – Transparent coder. 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 (default=20). g729 – 10, 20, 30, 40 (default=20). g723 family – 30, 60, 90, 120, 150 (default = 30). G.726 family – 10, 20, 30, 40, 50, 60, 80, 100 (default=20) NetCoder family – 20, 40, 60, 80, 100 (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 will receive. **Note 4:** G.729B is supported if the coder G.729 is selected and 'EnableSilenceCompression' is enabled. ***ini* file note 1:** This parameter (CoderName_ID) can appear up to 20 times (five coders in four coder groups). ***ini* file note 2:** The coder name is case-sensitive. ***ini* file note 3:** Enter in the format: CoderName,ptime. For example, the following three coders belong to coder group with ID=1: CoderName_1 = g711Alaw64k,20 CoderName_1 = g711Ulaw64k,40 CoderName_1 = g7231,90

Table 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

ini File [Web Interface] Parameter Name	Description
DisableAutoDTMFMute	Enables / disables the automatic mute of DTMF digits when out-of-band DTMF transmission is used. 0 = Auto mute is used (default). 1 = No automatic mute of in-band DTMF. When 'DisableAutoDTMFMute=1', the DTMF transport type is set according to the parameter 'DTMFTransportType' and the DTMF digits aren't muted if out-of-band DTMF mode is selected ('IsDTMFUsed =1'). This enables the sending of DTMF digits in-band (transparent of RFC 2833) in addition to out-of-band DTMF messages. **Note:** Usually this mode is not recommended.
DNS2IP [Internal DNS Table]	Internal DNS table, used to resolve host names to IP addresses. Two different IP addresses (in dotted format notation) can be assigned to a hostname. DNS2IP = <Hostname>, <first IP address>, <second IP address> **Note 1:** If the internal DNS table is configured, the gateway first tries to resolve a domain name using this table. If the domain name isn't found, the gateway performs a DNS resolution using an external DNS server. **Note 2:** This parameter can appear up to 10 times.
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 = 486 (Busy here). AltRouteCauseTel2IP = 480 (Temporarily unavailable). AltRouteCauseTel2IP = 408 (No response). **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 5 times.
AltRouteCauseIP2Tel [Reasons for Alternative Routing Table]	Table of call failure reason values received from the pstn side (in Q.931 presentation). If a call is released as a result of one of these reasons, the 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 = 1 (Unallocated number). AltRouteCauseIP2Tel = 17 (Busy here). **Note 1:** This parameter can appear up to 5 times. **Note 2**: If the Mediant 2000 fails to establish a cal to the PSTN because it has no available channels in a specific trunk group (e.g., all of the trunk group's channels are occupied, or the trunk group's spans are disconnected or out of sync), it will use the internal release cause '3' (no route to destination). This cause can be used in the 'AltRouteCauseIP2Tel' table to define routing to an alternative trunk group.
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.

Table 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

ini File [Web Interface] Parameter Name	Description
PSTNPrefix [IP to Trunk Group Routing Table]	PSTNPrefix = a,b,c,d,e a = Destination Number Prefix b = Trunk group ID (1 to 99) c = Source Number Prefix d = Source IP address e = IP Profile ID (1 to 5) Selection of trunk 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 trunk 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.
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' manipulations rules are applied if the called and calling numbers match the 'a' and 'g' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign "$$", for example: NumberMapTel2IP=01,2,972,$$,0,0,$$ NumberMapTel2IP=03,(2),667,$$,0,0,22
SourceNumberMapTel2IP [Source Phone Number Manipulation Table for Tel→IP calls]	SourceNumberMapTel2IP = a,b,c,d,e,f,g,h a = Source number prefix b = Number of stripped digits from the left, or (if in brackets are used) from right. A Combination of both options is allowed. c = String to add as prefix, or (if in brackets are used) as suffix. A Combination of both options is allowed. d = Number of remaining digits from the right e = 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,$$,1 SourceNumberMapTel2IP=03,(2),667,$$,0,0,22,0

Table 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

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 = Q.931 Number Plan f = Q.931 Number Type g = Source number prefix h = Not applicable, set to $$ i = Source IP address The 'b' to 'f' manipulation rules are applied if the called and calling numbers match the 'a', 'g' and 'i' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign "$$", for example: NumberMapIP2Tel =01,2,972,$$,0,$$,034 NumberMapIP2Tel =03,(2),667,$$,$$,0,22,$$,10.13.77.8 **Note:** The Source IP address can include the "x" wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99.
SourceNumberMapIP2Tel [Source Phone Number Manipulation Table for IP→Tel calls]	Manipulate the source number for IP to Tel calls. SourceNumberMapIP2Tel = a,b,c,d,e,f,g,h a = Source number prefix b = Number of stripped digits from the left, or (if brackets are used) from the right. A combination of both options is allowed. c = String to add as prefix, or (if brackets are used) as suffix. A combination of both options is allowed. d = Number of remaining digits from the right e = Q.931 Number Plan f = Q.931 Number Type g = Destination number prefix h =Calling number presentation (0 to allow presentation, 1 to restrict presentation) The 'b' to 'f' and 'h' manipulation rules are applied if the called and calling numbers match the 'a' and 'g' conditions. The manipulation rules are executed in the following order: 'b', 'd' and 'c'. Parameters can be skipped by using the sign "$$", for example: SourceNumberMapIP2Tel =01,2,972,$$,0,$$,034,1 SourceNumberMapIP2Tel =03,(2),667,$$,$$,0,22
PSTNAlertTimeout	Alert Timeout in seconds (ISDN T2 timer) for outgoing calls to PSTN. The default is 180 seconds. The range is 0 to 240. **Note:** The PSTN stack T2 timer can be overridden by a lower value, but it can't be increased.
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).

Table 1-1: Release 4.4 *ini* File [Web Browser] Parameter Name (continues on pages 15 to 26)

ini File [Web Interface] Parameter Name	Description
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).
SaveConfiguration	Set to 1 to store the configuration files (e.g., Call Progress Tones) in the non-volatile memory. **Note:** The parameters 'BurnCallProgressToneFile' and 'BurnCoeffFile' are no longer supported.
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.
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".

2 SIP and PSTN Compatibility

2.1 PSTN to SIP Interworking

The Mediant 2000/SIP Gateway supports various ISDN PRI protocols such as EuroISDN, North American NI2, Lucent 5ESS, Nortel DMS100, Meridian1 DMS100, Japan J1, as well as QSIG (basic call). PRI support includes User Termination or Network Termination side. ISDN-PRI protocols can be defined on an E1/T1 basis (i.e., different variants of PRI are allowed on different E1/T1 spans).

In addition, it supports numerous variants of CAS protocols for E1 and T1 spans, including MFCR2, E&M wink start, E&M immediate start, E&M delay dial/start, loop-start, and ground start. CAS protocols can be defined on an E1/T1 basis (i.e., different variants of CAS are allowed on different E1/T1 spans).

The Mediant 2000 simultaneously supports different variants of CAS and PRI protocols on different E1/T1 spans (no more than four simultaneous PRI variants).

PSTN to SIP and SIP to PSTN Called and Calling numbers can be optionally modified according to rules that are defined in Gateway's *ini* file.

2.1.1 Supported Interworking Features

- Definition and use of Trunk Groups for routing IP→PSTN calls.
- B-channel negotiation for PRI spans.
- ISDN Non Facility Associated Signaling (NFAS).
- Supports SIP2QSIG IETF draft-ietf-sipping-qsig2sip-04.txt, including interworking between 180/183 responses with SDP and Q.931 Progress message.
- PRI to SIP Interworking of Q.931 Display (Calling name) information element.
- PRI (NI-2) to SIP interworking of Calling Name using Facility IE in Setup and Facility messages.
- Configuration of Numbering Plan and Type for IP→ISDN calls
- Interworking of PSTN to SIP release causes
- Interworking of ISDN redirect number to SIP diversion header (according to IETF draft-levy-sip-diversion-05.txt).
- Optional change of redirect number to called number for ISDN→ IP calls.
- Interworking of ISDN calling line Presentation & Screening indicators using RPID header <draft-ietf-sip-privacy-04.txt>.
- Interworking of Q.931 Called and Calling Number Type and Number Plan values using the RPID header.
- Supports ISDN en-block or overlap dialing for incoming Tel→IP calls.
- Supports routing of IP→Tel calls to predefined trunk groups.
- Supports a configurable channel select mode per trunk group.

- Supports various number manipulation rules for IP→Tel and Tel→IP, called and calling numbers.
- Option to configure ISDN Transfer Capability (per Gateway).

2.1.2 Unsupported Interworking Features

- Q.931 and QSIG supplementary services.
- Overlap sending (only en-bloc sending is used).
- QSIG and 5ESS Calling Name Identification.
- QSIG and PRI connected line identification.

2.2 Supported SIP Features

The Mediant 2000 SIP main features are:

- Reliable UDP transport, with retransmissions.
- 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 four Proxy servers. If the primary Proxy fails, the Mediant 2000 automatically switches to a redundant Proxy.
- Supports Proxy discovery using DNS SRV records.
- Proxy or Registrar Registration, such as:

```
REGISTER sip:servername SIP/2.0
VIA: SIP/2.0/UDP 212.179.22.229;branch=z9hG4bRaC7AU234
From: <sip:GWRegistrationName@sipgatewayname>;tag=1c29347
To: <sip:GWRegistrationName@sipgatewayname>
Call-ID: 10453@212.179.22.229
Seq: 1 REGISTER
Expires: 3600
Contact: sip:GWRegistrationName@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 parameter 'GWRegistrationName' can be any string. If the parameter is not defined, the parameter 'UserName' is used instead.

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 once per gateway. 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.
- Supported methods: INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, INFO, REFER, NOTIFY, PRACK, UPDATE and SUBSCRIBE.
- Modifying connection parameters in a 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 messages.
- Session Timer <draft-ietf-sip-session-timer-13.txt>
- Network asserted identity and privacy (RFC 3325 and RFC 3323)
- Can now obtain Proxy Domain Name(s) from a DHCP server 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 1225556@10.1.2.4, where "122556" is the phone number of the source or destination) or sip:"phone_number"@"domain name", such as 122556@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 (10, 20, 30, 40, 50, 60, 80, 100 msec)
  - G.711 μ-law (10, 20, 30, 40, 50, 60, 80, 100 msec)
  - G.723 (5.3, 6.3 kbps, 30, 60, 90, 120, 150 msec)
  - G.729A (8 kbps, 10, 20, 30, 40, 50, 60, 80, 100 msec), G.729B is supported if Silence Suppression is enabled.
  - G.726 (32 kbps, 10, 20, 30, 40, 50, 60, 80, 100 msec)
  - NetCoder (6.4, 7.2, 8.0 and 8.8 kbps, 20, 40, 60, 80, 100, 120 msec).
- Supports RFC 3327 – Adding "Path" to Supported header.
- Supports RFC 3581 – Symmetric Response Routing.

2.3 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.
- TCP, TLS and SIPs

2.4 SIP Compliance Tables

The Mediant 2000/SIP Gateways comply with RFC 3261, as shown in the following sections.

2.4.1 SIP Functions

Table 2-1: Supported 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

2.4.2 SIP Methods

Table 2-2: Supported 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

2.4.3 SIP Headers

Release 4.4 of the Mediant 2000/SIP Gateways support the following SIP Headers:

Table 2-3: Supported SIP Headers (continues on pages 31 to 32)

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

Table 2-3: Supported SIP Headers (continues on pages 31 to 32)

Header Field	Supported
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

2.4.4 SDP Headers

Release 4.4 of the Mediant 2000/SIP Gateways support the following SDP Headers:

Table 2-4: Supported 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

2.4.5 SIP Responses

Release 4.4 of the Mediant 2000/SIP Gateways support the following SIP responses:

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.

2.4.5.1 1xx Response – Information Responses

Table 2-5: Supported 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.
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

2.4.5.2 2xx Response – Successful Responses

Table 2-6: Supported 2xx SIP Responses

2xx Response		Supported	Comments
200	OK	Yes	
202	Accepted	Yes	

2.4.5.3 3xx Response – Redirection Responses

Table 2-7: Supported 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	"

2.4.5.4 4xx Response – Request Failure Responses

Table 2-8: Supported 4xx SIP Responses (continues on pages 34 to 35)

4xx Response		Supported	Comments
400	Bad Request	Yes	The Gateway does not generate this response. On reception of this message, before a 200 OK 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 200 OK 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 200 OK has been received, the gateway responds with an ACK and disconnects the call.
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.

Table 2-8: Supported 4xx SIP Responses (continues on pages 34 to 35)

4xx Response		Supported	Comments
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 the no-answer timer expires. 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.
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.

2.4.5.5 5xx Response – Server Failure Responses

Table 2-9: Supported 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	

2.4.5.6 6xx Response – Global Responses

Table 2-10: Supported 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	

3 Known Constraints

3.1 SIP Constraints

1. When using out of band DTMF transport (IsDTMFUsed=1), the 'DTMFTransportType' parameter should be set to 0 (erase digits from voice stream).
2. 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.
3. Channel parameters, such as, Voice/DTMF gain, silence suppression 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.
4. G.726, 16 kbps, 24 kbps and 40 kbps coders are not supported. Only G.726/32 kbps is supported.
5. Single ptime parameter is used in SDP message to define the packetization period for multiple coders. For example, if G.711 and G.723 coders are used, the ptime is set to 30 msec.
6. Only the ptime (packetization time) of the first coder in the defined coder list is declared in Invite/200 OK SDP, 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.
7. The number of RTP payload packed in a single G.729 packet (M channel parameter) is limited to 5.

3.2 Gateway Constraints

8. The VXML-based Calling Card application is not supported in the current version (will be supported in release 4.4 fix).
9. 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.
10. Date and Time should be set after each Gateway power reset unless NTP (Network Time Protocol) is used.
11. Coder names in *ini* file are case-sensitive.
12. The gateway only supports symmetrical coders – the same coder is used for transmit and for receive (though different ptime is supported).
13. When using G.711 coder with 10 msec packetization time (without silence suppression) the Mediant 2000 can support up to 360 channels, each gateway module supporting up to 180 channels.
14. Usually when using E1 protocols, it is necessary to set the PCMLawselect parameter to A-law, while when using T1 protocols the PCMLawselect parameter should be set to μ-Law (The parameter can be set from the ini file or via the Web Interface in Trunk Settings page).
15. It is not valid to configure the board to auto-negotiate mode while the opposite port is set manually to full-duplex (either 10 Base-T or 100 Base-T). It is also not valid to set the board to one of the manual modes while the opposite port is configured differently.
16. It is strongly recommended to use 100 Base-T switches. Use of 10 Base-T LAN hubs should be avoided.

3.3 Web Constraints

17. Domain names in the 'Tel to IP Routing' table are limited to 15 characters.
18. 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 board, using the Web browser reset button.
19. When changing Gateway parameters from the Web browser, the new parameters are permanently stored in flash memory only after the Gateway is reset from the Web or after "Save Configuration" button is pressed.

3.4 SNMP Constraints

20. The performance monitoring sections in the Trunk MIB are not supported.
21. Configuration alarm does not clear.
22. The following RTP MIB objects are not supported: rtpRcvrSRCSSRC, rtpRcvrSSRC, rtpSenderSSRC, rtpRcvrLostPackets, rtpRcvrPackets, rtpSenderPackets, rtpRcvrOctets, rtpSenderOctets.
23. The CAS tables cannot be correctly set via SNMP.
24. 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).
25. Only one SNMP manager can access the device simultaneously.
26. Channel status is limited to the number of B-channels (determined by the number of trunks) and not by the number of logical channels.

4 Recent Revision History

4.1 Revision 4.2 Rev 03

4.1.1 General New Features (Version 4.2 Rev 03)

1. The Embedded Web Server's username and password can now be changed on-the-fly. A warning message is displayed if the entered password exceeds 7 characters.
2. Network parameters (IP address, Default Gateway and Subnet) entered from the Web are now checked for validity. A warning message is displayed if parameters' value is incorrect.
3. An option to enable / disable call release when an RTP broken connection is detected, using the parameter 'DisconnectOnBrokenConnection'.
4. An option to manipulate source number according to destination number prefix.
5. T.38 fax relay SIP session can now be initiated also when a CED answering tone is detected (using the parameter 'DetFaxOnAnswerTone =1'). Note that this operational mode is not recommended. It is only necessary for specific originating fax machines that require the reception of a CED tone.
6. The Gateway now supports two stage dialing option for IP→Tel calls: placing a call and then sending DTMF digits, using the parameter 'EnableDigitDelivery = 1'.
7. ISDN Transfer Capability for IP→PSTN calls can now be configured.
8. Can now play dial tone to the ISDN user side in Overlap dialing, if an empty called number is received, and 'ISDNINCallsBehavior = 65536' (bit #16) causing the Progress Indicator to be included in the SETUPACK ISDN message.
9. The Gateway now opens voice if an ISDN DISCONNECT message with PI is received.
10. Supports configuration of ISDN overlap dialing per **Mediant 2000** trunk.
11. An optional ISDN IE can now be configured. This IE is used in ISDN SETUP message. It is also possible to configure the specific E1/T1 span(s) from where this IE is sent.
12. Support for Meridian 1 DMS100 PRI variant was added.

4.1.2 SIP New Features (Version 4.2 Rev 03)

13. T.38 fax now supports the reception of T.38 capabilities in the first INVITE.
14. Supports REINVITE for mid-call change of T.38 fax session parameters.
15. A new x-channel header is added. This header provides information on the E1/T1 physical trunk/B-channel on which the call is received or placed. For example: "x-channel: DS/DS1-5/22". This header is generated by the **Mediant 2000** and is sent in the following messages: INVITE and 183/180/200 OK responses. To enable this feature set the parameter 'XChannelHeader'.
16. Diversion header is now supported also for IP→ ISDN calls. It is used to generate a redirect number in ISDN SETUP.
17. Supports the 'maddr' parameter in 'refer_to' URI, and using it in the generated INVITE SIP:URI.
18. Max-Forwards header was added to the Gateway generated INVITE messages. The default value is set to 70.

19. Reception of 180 Ringing after 183 response is received, now causes a Ringback tone to be played to the PSTN. ISDN ALERT (with Progress Indicator) is sent after the receptionof 183 response. If subsequent 180 Ringing message is received and ALERT was already sent, the **Mediant 2000** Gateway plays a Ringback tone.
20. The parameter 'User=Phone', can now be included also in the FROM header (in addition to INVITE URI). Configure 'IsUserPhoneInFrom = 1' in the *ini* file.

4.1.3 Resolved Constraints (Version 4.2 Rev 03)

4.1.3.1 From Version 4.200 to Version 4.202

1. HTTP download of CAS *ini* file(s) is fixed.
2. Single page T.38 fax problem is solved (new DSP version).
3. SNMP memory leaks were solved.
4. Asserted Identity is now supported (for IP→PRI) also if there are no "user=phone" parameters in the Asserted Identity header.
5. Now supports REFER-To SIP URI, without userpart, for example: "Refer-To: sip:10.3.1.35".
6. The Gateway now supports UDP port in REFER-To SIP URI, such as "sip:123@10.3.1.35:5080".
7. Can now send PRACK (and other methods) to the IP address that is provided in the 180/183 Record Route header.
8. Supports DTMF INFO messages while the Gateway is in Hold state.
9. Can now send ACK/BYE messages to "maddr IP" in Contact header.
10. Authorization bug was fixed - if "qop = Auth, Auth-INT", the response contained "Auth, without the right quotation mark.
11. "Remote expire" registration time, was updated according to min-expires that is received from the remote side.
12. Mid call authentication (empty username & wrong URI), is fixed.
13. The missing 'CRLF' at the end of 200 OK message that is sent in response to REINVITE message, was added.
14. During call transfer, if the terminating Gateway is in alert state, the Gateway now plays a Ringback tone.
15. Registration expire timeout bug was fixed.

4.1.3.2 From Version 4.202 to Version 4.2101

16. The Gateway now releases the allocated Gateway internal sessions in an erroneous call scenarios.
17. Can now properly handle T2 timer with provisional responses. Reception of 100 trying in response to non-INVITE SIP requests (such as REGISTER, BYE and others) does not stop the retransmission.
18. Now sends 481 response if BYE or other SIP messages that are not expected are received.
19. Now sends 405 "method not allowed" response if MESSAGE method is received.
20. Can now handle 301/302 responses with contact URI: port number (with or without maddr). The Gateway sends INVITE to the proper IP/port.

21. The Gateway now supports the reception of first INVITE or 200 OK with 0.0.0.0 in SDP (holds the call from its beginning).
22. When first INVITE with 0.0.0.0 in SDP is received, the received PRACK message (sent to acknowledge the 180 Ringing) is now acknowledged with 200 OK.
23. The crash that occurred due to the following scenario was fixed: The Gateway receives an INVITE message with 0.0.0.0, it replies with 200 OK, but no ACK is received. After the retransmission of 200 OK is finished, the call is not released; the Gateway crashes when call is released from the Tel side.
24. The missing local port (other than 5060) in Via and Contact headers of REGISTER message was added.
25. There is now also support for Session timer REINVITE keep alive messages during a call in Hold state, and for a T.38 fax call as well.
26. Can now send ACK message with the same Branch as was received in 481 response (if 481 was sent as a response to the Gateway's initiated INVITE).
27. The Gateway now supports up to 10 coders (instead of 5) in received SDP.
28. A bug that increased the value of Cseq by 2, between INVITEs (after authentication) is fixed.
29. G.723 coder ptimes can now be configured from the Web interface (ranged from 30 to 150 msec).
30. G.723 coder SDP negotiation issue was fixed, for other than 30 msec ptimes.
31. CANCEL request is now sent with the same URI as the URI in the INVITE message, if it is initiated before a 200 OK message is received.
32. The Gateway now supports SIP URI without userpart, in Contact header, for example: Contact: <sip:192.168.1.34:5060>.
33. The Gateway now uses the 'maddr' parameter in an INVITE URI, if it appears in Refer-to, Record-route or Contact headers.
34. DNS resolution, for REFER-to domains isn't used, if 'Send all INVITEs to proxy' or 'always use Proxy' features are enabled.
35. Bug fix: when a call was forwarded on 'no reply', a Ringback tone wasn't played.
36. Double quotes are now added to the names in the FROM headers, even if the names in the received ISDN DISPLAY header has no quotes.
37. Now delays sending of BYE message after call transfer is complete, this enables the party that initiated the REFER to also send BYE message.
38. Now supports 'A'-'D' DTMF digits for out of band (INFO) signaling.
39. The bug that filtered all the text between the (< >) signs in the Web's Message log is fixed. SIP messages are displayed correctly.
40. Proxy and Gateway names were increased to 50 characters each.
41. The IP address field in the Tel to IP routing table was increased to accept up to 30 characters.
42. The destination prefix field in the IP to Tel manipulation table was increased to accept strings up to 40 characters.
43. Can now handle two 'c= IP address' lines in SDP, including video and audio. Using one "c=IP address" that is associated with audio.
44. DMS100 ISDN Protocol violation is fixed. Progress indicator is not sent in ISDN PROCEEDING message (for both TE→NT and NT→TE), and not in ALERTING message (for TE→NT).
45. NI-2 ISDN protocol violation is fixed. Progress indicator is not sent in ISDN PROCEEDING message.

46. Bug fix: the “Add Trunk Group as Prefix” and Overlap dialing features now interoperate correctly.
47. The Calling Number Type / Plan for T1 PRI protocols can now be configured from the *ini* file and from the Web. In the previous version it was automatically set according to the calling number’s length.
48. Redirect number interworking for DMS100, NI-2 and 4ESS/5ESS protocols, is now supported for both NT→TE and TE→NT calls. For Euro ISDN it is supported only for NT→TE direction.
49. Calling name (Display) interworking for DMS-100 and 4ESS/5ESS protocols is now supported for both NT→TE and TE→NT calls. For Euro ISDN it is supported only for NT→TE direction. NI-2 is currently not supported.
50. The following parameters were added to the ‘Protocol Definition’ screen on the Web interface:
    - RFC 2833 Payload Type
    - NTT Caller ID Type
51. The G.726 unsupported coders were removed from the ‘Protocol Definition’ screen in the Web interface. Only G.726 / 32 kbps coder is used with SIP.

4.1.4 New Parameters (Version 4.2 Rev 03)

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: *ini* File [Web Browser] Parameter Name (continues on pages 43 to 44)

ini File [Web Interface] Parameter Name	Description
DisconnectOnBrokenConnection	0 = Don't release the call. 1 = Call is released If RTP packets are not received for a predefined timeout (default). **Note 1**: If enabled, the timeout is set by the parameter 'BrokenConnectionEventTimeout', in 100 msec resolution. The default timeout is 10 seconds: (BrokenConnectionEventTimeout =100). **Note 2:** This feature is applicable only if RTP session is used without Silence Compression. If Silence Compression is enabled, the Gateway doesn't detect that the RTP connection is broken. **Note 3:** During a call, if the source IP address (from where the RTP packets were sent) is changed without notifying the Gateway, the Gateway will filter these RTP packets. To overcome this issue, set 'DisconnectOnBrokenConnection=0'; the Gateway doesn't detect RTP packets arriving from the original source IP address, and will switch (after 300 msec) to the RTP packets arriving from the new source IP address.
EnableDigitDelivery	The digit delivery feature enables sending of DTMF digits to the Gateway's B-channel after the call is answered. 0 = Disabled (default). 1 = Enable Digit Delivery feature for Mediant 2000 (two stage dialing). **Note:** For incoming IP→Tel calls, if the called number includes the characters 'w' or 'p', the Mediant 2000 Gateway places a call with the first part of the called number, and plays DTMF digits after the call is answered. If the character 'p' (pause) is used, the Mediant 2000 waits for 1.5 seconds before playing the next DTMF digit. If the character 'w' is used, the Mediant 2000 waits for detection of dial tone before it starts playing DTMF digits. The character 'w' can appear once in the called number, and must precede any 'p' character. The 'p' character can appear several times. For example: if the number "1007766p100" is defined as the called number, the Mediant 2000 places a call with 1007766 as the destination number, then, after the call is answered, it waits for 1.5 seconds and plays the rest of the number (100) as DTMF digits. Other examples: 1664wpp102, 66644ppp503, 7774w100pp200.
ScreeningInd2IP	The parameter can overwrite the calling number screening indication for ISDN Tel→IP calls. -1 = not configured (interworking from ISDN to IP) or set to 0 for CAS. 0 = user provided, not screened. 1 = user provided, verified and passed. 2 = user provided, verified and failed. 3 = network provided.
SourceMapModeIP2Tel	Source number manipulation option for IP→Tel calls. 0 = Regular mapping (default). 1 = Source number is changed according to destination number's prefix (using source number manipulation table).
SourceMapModeTel2IP	Source number manipulation option for Tel→IP calls. 0 = Regular mapping (default). 1=- Source number is changed according to destination number prefix (using source number manipulation table).

Table 4-1: *ini* File [Web Browser] Parameter Name (continues on pages 43 to 44)

ini File [Web Interface] Parameter Name	Description
PlayRBTone2Tel [Play Ringback Tone to TEL]	0 = Don't play Ringback tone (default). The Gateway doesn't play Ringback tone. No PI is sent to ISDN, unless the parameter 'Progress Indicator to ISDN' is configured differently. 1 = Play. The Gateway plays local Ringback tone to PSTN, after 180/183 response is received. The PRI Gateway sends PI = 8 to the ISDN, unless the parameter 'Progress Indicator to ISDN' is configured differently. 2 = Ringback tone is played according to 180/183. For CAS and PRI protocols: If '183 session progress' with SDP is received, the Gateway cuts through the voice channel and doesn't play Ringback tone; PI=8 is sent in ISDN ALERT message (unless the parameter 'Progress Indicator to ISDN' is configured differently). If '180 ringing' is received, the CAS Gateway plays Ringback tone to PSTN; the ISDN Gateway doesn't play Ringback tone to PSTN. PI is not sent (unless the parameter 'Progress Indicator to ISDN' is configured differently). 3 = Play Ringback tone if 180 Ringing is received Ringback tone is played in all Gateways (including PRI Gateways), if 180 Ringing is received. The PRI Gateway sends PI=8 in ISDN ALERT message.
ISDNRxOverlap_x	Enable / disable Rx ISDN overlap per trunk ID (x = 0 to 7). 0 = Disabled (default). 1 = Enabled. **Note 1:** If enabled, the Mediant 2000 receives ISDN called number that is sent in the "Overlap" mode. **Note 2:** The SETUP message to IP is sent only after the number (including the 'Sending Complete' Info Element) was fully received (via SETUP and/or subsequent INFO Q.931 messages). **Note3:** The 'MaxDigits' parameter can be used to limit the length of the collected number for Mediant 2000 ISDN overlap dialing (if sending complete was not received).
ISDNTransferCapability	Defines the IP→ISDN Transfer Capability of the Bearer Capability IE in ISDN Setup messages. 0 = Audio 3.1 (default). 1 = Speech. 2 = Data. **Note:** If this parameter isn't configured or equals to '–1', Audio 3.1 capability is used.
XChannelHeader	0 = x-channel header is not used (default). 1 = x-channel header is generated, with trunk/B-channel information. The header provides information on the E1/T1 physical trunk/B-channel on which the call is received or placed. For example "x-channel: DS/DS1-5/22". This header is generated by the Mediant 2000 and is sent in the following messages: INVITE and 183/180/200OK responses.
AddIEinSetup	This parameter enables to add an optional Information Element data (in hex format) to ISDN SETUP message. For example: to add the following IE: "0x20,0x02,0x00,0xe1", define: "AddIEinSetup = 200200e1". **Note:** This IE is sent from the Trunk Group IDs defined by the parameter 'SendIEonTG'.
SendIEonTG	A list of Trunk Group IDs (up to 50 characters) from where the optional ISDN IE, defined by the parameter 'AddIEinSetup', is sent. For example: "SendIEonTG = 1,2,4,10,12,6".

4.2 Revision 4.2

4.2.1 SIP New Features (Version 4.2)

1. T.38 Fax is now supported - according to draft-sip-t38callflows-00 and draft-ietf-sipping-realtimefax-01.
   The following call scenario is supported:
   Voice call is established→Called side detects a Fax Preamble→REINVITE for T.38→T.38 fax session.

   Relevant parameters:
   IsFaxUsed – enables fax on both the caller and the called sides.
   CNGDetectorMode –Set to 2 to start fax session on the **caller** side after CNG tone is detected (not recommended), use preamble detection on the fax's answering side instead.

   For detailed information about additional parameters used to configure the fax/modem transfer methods refer to the Mediant 2000 SIP User's Manual".

2. Call Waiting – If the Mediant 2000 receives a 182 response it plays Call Waiting Ringback Tone to the PSTN side.

3. Support for placing call on-hold using one of the two following modes:

   - Locally playing a Hold tone, when a REINVITE message with either the IP address 0.0.0.0 or the "inactive" string in SDP is received.

   - Stop sending RTP packets if "sendonly" is received in REINVITE SDP message. In this mode it is expected that on-hold music (or any other hold tone) will be played over IP by the remote party.

4. Call Pickup - The Gateway performs Directed Call Pickup when it receives REFER message with REPLACES header.
5. Full Support for SIP "REPLACES" header (used in transfer message) as defined in draft-ietf-sip-replaces-02.txt.
6. Supports RFC 2833 DTMF relay payload type negotiation in the SDP.
7. Supports out of band DTMF transport via INFO message.
8. Support for Notify and Subscribe methods for out of band DTMF transport was added (according to draft-mahy-sipping-signaled-digits-01.txt).
9. When using out of band DTMF (IsDTMFUsed=1), the "DTMFTransportType" is automatically set to 0, to erase the DTMF digits from the RTP stream.
10. Support for several operational modes with Outbound-Proxy server:

    - SIP RFC 3261: standard rules are used to define which messages are sent directly to the Proxy server ("IsProxyUsed = 1" and "ProxyIP = <IPaddress>).

    - All INVITE messages including those generated as a result of Transfer or Redirect are sent to Proxy server (IsProxyUsed = 1", "ProxyIP = <IPaddress>" and "SendInvitetoProxy = 1")

    - All SIP messages and responses are sent via Proxy server. ("IsProxyUsed = 1", "ProxyIP = <IPaddress>" and "AlwaysSendtoProxy = 1").

11. Proxy Hot-Swap mode – If the main Proxy server doesn't respond to an INVITE message that was retransmitted for a configurable number of times, the call is routed to a secondary Proxy server.
Relevant parameters: IsProxyHotSwap, ProxyHotSwapRtx

12. Proxy redundancy parking and homing modes -
In homing mode, the Gateway always tries to work with the primary Proxy server (switches back to the main Proxy whenever it is available), while in parking mode the Gateway continues working with the last active Proxy until the next Proxy failure.
Relevant parameters: ProxyRedundancyMode

13. Support for Sendonly/Recvonly/Inactive attributes in received SDP messages. According to RFC 3264.

14. Enhanced coder negotiation – if an SDP reply from a remote Gateway includes more than one coder, the coder is selected (by the receiving gateway) according to order of appearance (of the coder) in the SDP.

15. Support for G.726 32 kbps coder (instead of G.726 16 kbps) was added.

16. PRACK (Provisional Response Acknowledge) mechanism mode for 1XX reliable responses - support for calling and called sides (according to RFC 3262). For requests initiated by the Gateway, PRACK can be configured to: no, optional and mandatory.
Relevant parameters: PRACKMode.

17. The "User-Agent" header (with software version, board type, etc.) is now added to all transmitted messages.

18. Supports Network Asserted Identity (RFC 3325) header for IP→Tel calls.

4.2.2 General New Features (Version 4.2)

19. Providing comprehensive Accounting over RADIUS server support.

20. Enhanced Dialing Plan capabilities – Allows entering ranges of numbers, fixed and opened numbers and the use of wild card characters. Applies to the four manipulation tables, Tel→IP Routing table and to IP→Trunk Group Routing table.
When entering a number in the 'Prefix' column, you can create an entry that represents multiple numbers using the following notation:

- [n-m] represents a range of numbers
- [n,m,l] represents multiple numbers
- x represents any single digit
- # represents the end of a number

For example:

- [5551200-5551300]# represents all of the numbers from 5551200 to 5551300
- [2221,2231,2241] represents three numbers: 2221, 2231 and 2241
- 54324 represents any number that starts with 54324
- 54324xx# represents a 7 digit number that starts with 54324
- 123[100-200]# represents all of the numbers from 123100 to 123200.

21. Call Restriction – when the internal routing table is used (and Proxy isn't used), reject all Tel→IP calls that are associated with the destination IP address: 0.0.0.0 in the Tel to IP routing table.
22. Filter Calls to IP – When Proxy is used, the Gateway checks the Tel to IP routing table before a telephone number is routed to the Proxy. If the number is not allowed (number isn't listed or a call restriction routing rule was applied), the call is released.
    Relevant parameters: "FilterCalls2IP = 1".
23. Alternative Routing (e.g., to implement PSTN Fallback) feature using Tel to IP routing – For PSTN to IP calls, when the internal routing table (Tel2IP) is used, an alternative route can now be added. Call is sent to the alternative IP address when no ping to the initial destination is available or when poor QoS (delay or packet loss, calculated according to previous calls) is detected.
    The alternative routing is configured by adding an additional entry for the same number/prefix in the Tel2IP routing table,
    Note: If the alternative routing destination is the Gateway itself, the call can be configured to be routed back to one of the Gateway trunk groups and back into the PSTN (PSTN Fallback).
24. Supported by AudioCodes' Element Management System (EMS).
25. Channel Select Mode – Several methods for trunk B-channel allocation for IP to TEL calls. Determined per whole Gateway (ChannelSelectMode) or separately for each trunk group (Trunk Group Settings table).
26. Routing calls according to DNS host names – In "Tel to IP Routing Table" Fully Qualified Domain Names (FQDN), such as AudioCodes.com, can be used instead of IP addresses. To use this feature you must configure the IP addresses of the primary and secondary (optional) DNS servers.
27. A new G.168-2000 compliant Echo Canceller, with support for up to 128 msec of echo tail, has been added. Refer to the new configuration parameter MaxEchoCancellerLength.
    Note: When set to 64 msec or more, the number of available gateway channels is reduced (by a factor of 5/6). For example:
    Gateway with 8 E1 spans capacity is reduced to 6 spans (180 channels), while Gateway with 8 T1 spans capacity remains the same (192 channels).
28. ISDN Overlap receiving - the Mediant 2000 can now receive PSTN phone numbers that are sent in the "Overlap" mode (refer to ISDNRxOverlap, *ini* file parameter).
    Note: request to IP is sent only after the number (including "Sending Complete" Info Element) was fully received (via SETUP and/or subsequent INFO Q.931 messages).
29. Transparent Protocol support - if trunks are configured to transparent protocol, then call is established without applying any PSTN protocol, e.g., trunks under SS7 signaling control. RTP is sent and received on the TDM slot.
30. Gateway's channel internal number can now be used as a 'destination number' for Tel→IP calls, if called number, was not received from PSTN (ReplaceEmptyDstWithPortNumber).
31. "Add Port as prefix" feature - For Tel→IP incoming calls, trunk ID number (1-8) is added as prefix to the called phone number. Can be used to define various routing rules.
32. Syslog CDR support enhanced – A Call Detail Record (CDR) can now be sent at both the end and start of a call (after INVITE message was sent/received) to Syslog server.
33. RTP Broken Connection - Call is disconnected if RTP packets aren't received for a configurable time period during the call (BrokenConnectionEventTimeout).
34. Robust reception of RTP streams using a new filtering mechanism. This new mechanism filters out unwanted RTP streams that are sent to the same port on the board. These multiple RTP streams can result from traces of previous calls, call control errors or deliberate attacks. As a result, a port may accept packets only from one known source at a time.
35. Support for reception of RTP packets with the header Padding bit set to 1.
36. Support for reordered RTP packets – a new algorithm was implemented to handle reordered RTP packets. This feature improves the voice quality on a network which suffers from packet reordering problems.

37. Configurable Default Release Cause (to IP or to PSTN) - when the Gateway terminates a call, and if an explicit matching cause for this termination isn't found, a default release cause can be configured (DefaultReleaseCause):

    The default release cause is: NO_ROUTE_TO_DESTINATION (3).
    Other common values are: NO_CIRCUIT_AVAILABLE (34) or NETWORK_OUT_OF_ORDER (38), etc.

    Note: The default release cause is described in the Q.931 notation, and is translated to the corresponding SIP 4xx and 5xx values.

38. Supporting Cisco™ NSE mode for Modem automatic pass-through (NSEMode, NSEPayloadType).

39. Option to delay Gateway's operation – After a reset cycle, the Gateway's operation can now be delayed for a specified time (according to the GWAppDelayTime parameter). This feature helps to overcome connection problems caused by specific routers.

40. Common Debug Level Parameter – Syslog Debug levels can now be configured via a single parameter, GwDebugLevel, instead of separate "logger objects". Usually set to 5 if debug traces are needed.

4.2.3 Embedded Web Server New Features (Version 4.2)

41. Online loading of CAS tables via the Embedded Web Server is now available.

42. Number Plan and Number Type values are presented in Number Manipulation tables according to Table 1 in ETS 300 189 standard.
    The following Plan, Type values are supported:

    - 0,0 – Unknown, Unknown
    - 9,0 – Private, Unknown
    - 9,1 – Private, Level 2 Regional
    - 9,2 – Private, Level 1 Regional
    - 9,3 – Private, PISN Specific
    - 9,4 – Private, Level 0 Regional (local)
    - 1,0 – Public(ISDN/E.164), Unknown
    - 1,1 – Public(ISDN/E.164), International
    - 1,2 – Public(ISDN/E.164), National
    - 1,3 – Public(ISDN/E.164), Network Specific
    - 1,4 – Public(ISDN/E.164), Subscriber
    - 1,6 – Public(ISDN/E.164), Abbreviated

43. Invalid parameter value warning alert – invalid parameters are colored red and a short warning message is displayed.

44. Users can now retrieve the Gateway's configuration in an *ini* file format; the *ini* file (downloaded from the Gateway via the Embedded Web Server) contains all parameters that are different from their default value. The *ini* file can then be uploaded to a second Gateway to apply the same configuration.

45. Message log page – adds the option to watch the error logs directly without an external Syslog server.

46. Save Configuration button - burning the current configuration to the flash memory without resetting the Gateway. Resetting the board should be done before activating traffic (or at a low traffic period).
47. New administration feature - Logo images upload. User can change the logo that appears in the Web pages.
48. A number of parameters have been upgraded with on-the-fly capability. In the Embedded Web Server, parameters that can be changed on-the-fly are noted with an asterisk (*).

4.2.4 SNMP New Features (Version 4.2)

49. Updated SNMP MIB files for SIP parameters and other gateway (ACL MIB) parameters.
50. New Trap Manager Table - SNMPManagers – providing online configuration for up to three Managers used for receiving SNMP Traps. Each of the following parameters can be configured separately for each Manager: IP address, port number and weather it is active or not. (Related parameters: SNMPManagerTableIP, SNMPManagerTrapPort, SNMPManagerIsUsed and SNMPManagerTrapSendingEnable).
To enable SNMP Traps set “SNMPManagerIsUsed=1” in the *ini* file.
51. Traps - Traps are sent when major problems are encountered, clear trap is sent when problem is solved.
Traps Include:
    - General Fatal Error
    - Configuration Error
    - Controller lost (Proxy)
    - Call resources low (EnableRAI parameter must be enabled)
    - Gateway Overload
52. Community Strings for Get and Set are configurable via *ini* file parameter SetCommunityString. The same string (up to 20 characters) is used for Set and for Get.

4.2.5 Resolved Constraints (Version 4.2)

1. Responses are now sent to source IP address and not to the IP address specified in the Via header (RFC 3261).
2. CANCEL, ACK and PRACK messages are now sent to the correct IP addresses.
3. The CANCEL message, sent before 200 OK response is received, now gets the same URI as the originating INVITE message.
4. Configurable ProxyKeepAliveTime and MaxRtx.
5. DomainName was enlarged to 30 characters.
6. Sending 481 "Call/Transaction does not exist" message in response to a re-INVITE or INFO audit requests for session that does not exist.
7. Setting the T38MaxBitRate parameter in SDP during fax negotiation is set according to "FaxRelayMaxRate" parameter.
8. Support for received SIP messages of up to 1700 bytes.

Previous Version

9. Static NAT support.
10. Various call hold and transfer services using REFER and REPLACES were fixed.
11. Out of band DTMF INFO/NOTIFY messages are also sent if Call is in hold state (no RTP is sent).
12. Second Registrar request with MD5 response is sent without the “To” tag, same as the first Registrar request.
13. ISDN NFAS (Non Facility Associated Signaling) support.
14. IP→Trunk group routing table was increased to support 24 rules.
15. Only one simultaneous source of incoming RTP packets is allowed per channel.
16. MFCR2 supports release causes (Busy, congestion, etc.), for PSTN→IP calls.

4.2.6 New Parameters (Version 4.2)

Most new parameters (described in Table 4-2) 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 4-2: *ini* File [Web Browser] Parameter Name (continues on pages 51 to 56)

***ini* File [Web Interface] Parameter Name**	**Description**
ProtocolType	Support for additional protocols: 4 = T1_TRANSPARENT 5 = E1_TRANSPARENT_31 6 = E1_TRANSPARENT_30 15 = J1_TRANSPARENT
ISDNRxOverlap	0 = Disabled (default) 1 = Enabled **Note 1:** If enabled the Mediant 2000 receives ISDN called number that is sent in the "Overlap" mode. **Note 2:** The SETUP to IP is sent only after the number (including “Sending Complete” Info Element) was fully received (via SETUP and/or subsequent INFO Q.931 messages).
AlwaysSendtoProxy	0 = Use standard SIP routing rules (default) 1 = All SIP messages and Responses are sent to Proxy server **Note:** Applicable only if Proxy server is used..
SendInviteToProxy	0 = INVITE messages, generated as a result of Transfer or Redirect, are sent directly to the URL (according to the refer-to header in the REFER message or contact header in 30x response). 1 = All INVITE messages, including those generated as a result of Transfer or Redirect are sent to Proxy. **Note:** Applicable only if Proxy server is used and “AlwaysSendtoProxy=0”.
EnableProxyKeepAlive [Enable Proxy Keep Alive]	0 = Disable (default) 1 = Keep alive with Proxy, by sending "OPTIONS" SIP message every “ProxyKeepAliveTime”.
ProxyKeepAliveTime	Defines the Proxy keep-alive time interval (in seconds) between OPTIONS messages. The default value is 60 seconds.
SIPMaxRtx [SIP MAX Rtx]	Number of UDP retransmissions of SIP messages. The range is 1 to 7. The default value is 7.
EnableRPIHeader [Enable Remote Party ID]	Enable-Remote-Party-ID Headers for calling and called numbers for Tel→IP calls. 0 = Disable (default) 1 = Enable
IsProxyHotSwap [Enable Proxy HotSwap]	Enable Proxy Hot Swap redundancy mode. 0 = Disabled (default) 1 = Enabled If Hot Swap is enabled, SIP INVITE message is first sent to the primary Proxy server. If there is no response from the primary Proxy server for “ProxyHotSwapRtx” retransmissions, the INVITE message is resent to the redundant Proxy server.
ProxyHotSwapRtx [Number of RTX before HotSwap]	Number of retransmitted INVITE messages before call is routed (hot swap) to another Proxy Range: 1-30 Default: 3
ProxyRedundancyMode [Redundancy Mode]	0 = Parking mode: Gateway continues working with the last active Proxy until the next failure. (default) 1 = Homing mode: Gateway always tries to work with the primary Proxy server (switches back to the main Proxy whenever it is available).

Table 4-2: *ini* File [Web Browser] Parameter Name (continues on pages 51 to 56)

ini File [Web Interface] Parameter Name	Description
PRACKMODE [PRACK Mode]	PRACK mechanism mode for 1XX reliable responses: 0 = Disabled 1 = Supported (default) 2 = Required **Note 1:** The Supported and Required headers contain the "100rel" parameter respectively. **Note 2:** Mediant 2000 sends PRACK message if 180/183 response is received with "100rel" in the Supported or the Required headers.
xferPrefix	Defined string that is added, as a prefix, to the transferred called number, using REFER message. **Note 1:** The number manipulation rules apply to the user part of the "REFER-TO" URL before it is sent in the INVITE message. **Note 2:** The xferprefix parameter can be used to apply different manipulation rules to differentiate the transferred number from the original dialed number.
ReplaceEmptyDstWithPortNumber	0 = Disabled (default). 1 = Enabled, Internal channel number is used as a destination number if called number is missing. **Note:** Applicable only to Tel→IP calls, if called number is missing.
MaxEchoCancellerLength	Maximum Echo Canceler Length in msec: 0 = Internal decision to keep max channel capacity (currently 32 msec) 4 = 32 msec 5 = 35 msec 6 = 40 msec 7 = 45 msec 8 = 50 msec 9 = 55 msec 10 = 60 msec 11 = 64 msec, reduced channels (max channels capacity is 200) 22 = 128 msec, reduced channels (max channels capacity is 200) The default value is 0.
AlwaysUseRouteTable [Use Routing Table For Host Names]	Use the internal routing table to obtain the URL Host name, even if Proxy server is used. 0 = Don't use (default) 1 = Use **Note:** This Domain name is used, instead of Proxy name or Proxy IP address, in the INVITE SIP URL.
IsFaxUsed	0 = T.38 Fax relay disabled (default) 1 = Enable T.38 Fax Relay **Note:** FaxTransportMode can be set to 0 (transparent). The gateway automatically changes the Fax transport mode to T.38 if "IsFaxUsed=1" and fax is detected. If "IsFaxUsed=0" fax can be sent (transparently) if G.711 coder is used.
CngDetectorMode	0 = Don't detect CNG (default) 2 = Detect CNG on caller side and start fax session (if IsFaxUsed=1) Usually T.38 fax session starts when the "preamble" signal is detected by the answering side. Some SIP gateways doesn't' support the detection of this fax signal on the answering side, for these cases it is possible to configure the Gateways to start the T.38 fax session when the CNG tone is detected by the originating side. However this mode is not recommended.
AltRoutingTel2IPEnable [Enable Alt Routing Tel2IP]	0 = Alternative Routing is disabled (default) 1 = Alternative Routing is enabled
AltRoutingTel2IPMode [Alt Routing Tel2IP Mode]	Alternative routing is performed if: 0 = Alternative routing according to PING and QoS is disabled 1 = Ping to initial destination failed 2 = QOS, poor quality of service was detected 3 = Both, either Ping to initial destination failed, or poor quality of service was detected (default)

Table 4-2: *ini* File [Web Browser] Parameter Name (continues on pages 51 to 56)

ini File [Web Interface] Parameter Name	Description
ChannelSelectMode [Channel Select Mode]	Defines port allocation algorithm for IP to TEL calls. **Note:** Replaces the obsolete parameter "IsUseFreeChannel" (Cyclic Ascending mode provides a similar functionality to the "IsUseFreeChannel" parameter). ➢ 0 = By phone number - Select the Gateway port according to the called number (called number is defined in the 'Trunk Group' table). ➢ 1 = Cyclic Ascending - Select the next available channel in an ascending cycle order. Always select the next higher channel number in the Hunt Group. When the Gateway reaches the highest channel number in the Hunt Group, it will select the lowest channel number in the Hunt Group and then start ascending again (default). ➢ 2 = Ascending - Select the lowest available channel. Always start at the lowest channel number in the Hunt Group and if that channel is not available, select the next higher channel. ➢ 3 = Cyclic Descending - Select the next available channel in descending cycle order. Always select the next lower channel number in the Hunt Group. When the Gateway reaches the lowest channel number in the Hunt Group, it will select the highest channel number in the Hunt Group and then start descending again. ➢ 4 = Descending - Select the highest available channel. Always start at the highest channel number in the Hunt Group and if that channel is not available, select the next lower channel. ➢ 5 = Number + Cyclic Ascending – First select the Gateway port according to the called number. If the called number isn't found, then select the next available channel in ascending cyclic order. Note that if the called number is found, but the port associated with this number is busy, the call is released.
TrunkGroupSettings [Hunt Group Settings]	Define rules for port allocation for specific Hunt Groups, if such rule doesn't exist, the global rule defined by ChannelSelectMode applies. a, b a = Trunk Group ID number b = Channel select mode for that Trunk Group. Available values are identical to those defined by the ChannelSelectMode parameter.
DNSPriServerIP [DNS Primary Server IP]	IP address of the primary DNS server in dotted format notation.
DNSSecServerIP [DNS Secondary Server IP]	IP address of the primary DNS server in dotted format notation.
DefaultReleaseCause	Default Release Cause (to IP), used when the Gateway initiates a call release, and if an explicit matching cause for this release isn't found, a default release cause can be configured. The default release cause is described in the Q.931 notation, and translated to corresponding SIP equivalent response value The default release cause is: NO_ROUTE_TO_DESTINATION (3). Other common values are: NO_CIRCUIT_AVAILABLE (34) or NETWORK_OUT_OF_ORDER (38), etc.
FilterCalls2IP [Filter Calls To IP]	0 = Disabled (default) 1 = Enabled **Note:** If filter calls to IP feature is enabled, then when Proxy is used, the Gateway checks first the Tel→IP routing table before a telephone number is routed to the Proxy. If the number is not allowed (number isn't listed or a negative routing rule was applied), the call is released.

Table 4-2: *ini* File [Web Browser] Parameter Name (continues on pages 51 to 56)

***ini* File [Web Interface] Parameter Name**	**Description**
RxDTMFOption [Rx DTMF Option]	Defines the supported Receive DTMF negotiation method. 0 = Don't declare RFC 2833 Telephony-event parameter in SDP 1 = n/a 2 = n/a 3 = Declare RFC 2833 "Telephony-event" parameter in SDP (default) The GW is designed to always be receptive to RFC 2833 DTMF relay packets. Therefore, it is always correct to include the "Telephony-event" parameter as a default in the SDP. However some gateways use the absence of the "telephony-event" from the SDP to decide to send DTMF digits inband using G.711 coder, if this is the case you can set "RxDTMFOption=0".
TxDTMFOption [DTMF RFC2833 Negotiation]	0 = No negotiation, DTMF digit is sent according to the "DTMFTransportType" parameter 4 = Enable RFC 2833 payload type (PT) negotiation **Note 1:** This parameter is applicable only if "IsDTMFUsed=0" (out of band DTMF is not used) **Note 2:** If enabled, the Gateway: ➢ Negotiates RFC 2833 payload type using local and remote SDPs. ➢ Sends DTMF packets using RFC 2833 PT according to the received SDP. ➢ Expects to receive RFC 2833 packets with the same PT as configured by the "RFC2833PayloadType" parameter. **Note 3:** If the remote party doesn't support the RFC 2833 DTMF relay, the Gateway uses the same PT for send and receive.
OutOfBandDTMFFormat	The exact method to send out of band DTMF digits 1 = INFO format (Nortel) 2 = INFO format (Cisco) - (default) 3 = NOTIFY format <draft-mahy-sipping-signaled-digits-01.txt> **Note 1:** To use out of band DTMF, set "IsDTMFUsed=1" or "Enable DTMF = yes". **Note 2:** When using out of band DTMF, the "DTMFTransportType" parameter is automatically set to 0, to erase the DTMF digits from RTP path.
AddPortAsPrefix [Add Port as Prefix]	0 = Don't add (default) 1 = Add trunk ID number (single digit in the range 1 to 8) as a prefix to the called phone number for Tel→IP incoming calls. This option can be used to define various routing rules.
GWAppDelayTime	Defines the amount of time (in seconds) the Gateway's operation is delayed after a reset cycle. The default value is 0 seconds **Note:** This feature helps to overcome connection problems caused by some LAN routers.
DisableNAT	0 = NAT is enabled 1 = NAT is disabled (default) If NAT is enabled, then the source IP address, of the first received RTP packet on a new session, is compared to the remote IP address, stated when session was opened; if they are not identical, then destination IP address of the outgoing RTP packets will be the source IP address of the first incoming packet.
SNMP Managers - a device that is used for receiving SNMP Traps.	

Table 4-2: *ini* File [Web Browser] Parameter Name (continues on pages 51 to 56)

ini File [Web Interface] Parameter Name	Description
SNMPManagerISUsed_x	Up to three parameters, each controls the **validity** of the parameters (IP address and port number) of the corresponding SNMP Manager. 0 = Disabled (default) 1 = Enabled (SNMPManagerIsUsed_0, SNMPManagerIsUsed_1, SNMPManagerIsUsed_2)
SNMPManagerTrapSendingEnable_x	Up to three parameters, each controls the activation/deactivation of sending traps to the corresponding SNMP Manager. 0 = Sending is disabled 1 = Sending is enabled (default) (SNMPManagerTrapSendingEnable_0, SNMPManagerTrapSendingEnable_1, SNMPManagerTrapSendingEnable_2)
SNMPManagerTableIP_x	Up to three IP addresses of remote hosts that are used as an SNMP Managers. (SnmpManagerIP_0, SnmpManagerIP_1, SnmpManagerIP_2) Enter the IP address in dotted format notation, for example 108.10.1.255. **Note:** This parameter replaces the obsolete parameter SNMPManagerIP.
SNMPManagerTrapPort_x	Up to three parameters used to define the Port numbers of the remote SNMP Managers (SNMPManagerTrapPort_0, SNMPManagerTrapPort_0 and SNMPManagerTrapPort_2) **Note:** This parameter replaces the obsolete parameter SNMPTrapPort. The default SNMP trap port is 163. The SNMP trap port must be less than 4000.
SetCommunityString	SNMP community string (up to 20 chars). Default community strings are “public” for read, and “private” for set & get.
ModemRtpByPassPayloadType	Modem Bypass dynamic payload type (range 0-127). The default value is 103.
FaxModemBypassBasicRtpPacketInterval	0 = set internally (default) 1 = 5 msec (not recommended) 2 = 10 msec 3 = 20 msec
NSEMode	Cisco compatible 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 105 codec g711alaw". ➢ Set the Modem transport type to Bypass mode (“VxxModemTransportType = 2”) for all modems.
NSEPayloadType	NSE payload type (range 96-127) The default value is 105. **Note:** The Cisco gateways usually use NSE payload type of 100.
BrokenConnectionEventTimeout	The amount of time (in 100 msec units) an RTP packet isn’t received, after which a call is disconnected. The default value is 100 (10 seconds).

Table 4-2: *ini* File [Web Browser] Parameter Name (continues on pages 51 to 56)

ini File [Web Interface] Parameter Name	Description
GwDebugLevel [Debug Level]	Defines the Syslog logging level (usually set to 5 if debug traces are needed). 0 = Debug is disabled (default) 1 = Flow debugging is enabled 2 = Flow and board interface debugging are enabled 3 = Flow, board interface and stack interface debugging are enabled 4 = Flow, board interface, stack interface and session manager debugging are enabled 5 = Flow, board interface, stack interface, session manager and board interface expanded debugging are enabled. Usually set to 5 if debug traces are needed.
RADIUS Related Parameters	
EnableRADIUS	0 = RADIUS server is disabled (default). 1 = RADIUS server is enabled.
MaxRADIUSSessions	Number of concurrent calls that can communicate with the RADIUS server (optional). Range: 0-240. The default value is 240.
SharedSecret	"Secret" used to authenticate the Gateway to the RADIUS server. It should be a cryptographically strong password.
RADIUSRetransmission	Number of retransmission retries. Range: 1-10. The default value is 3.
RadiusTO	The interval between each retry (measured in seconds). Range: 1-30. The default value is 10.
RADIUSAccServerIP	IP address of accounting server.
RADIUSAccPort	Port number of accounting server. The default value is 1646.
AAAIndications	0 = No indications (default). 3 = Accounting only

5 Version History

Details of previous releases can be found in the Release Notes of Version 4.2 Beta, published by AudioCodes on May-30-2003.

AudioCodes Offices

International Headquarters

AudioCodes Ltd, 1 Hayarden Street, Airport City

Lod 70151, Israel.

Tel: +972-3-976 4000

Fax: +972-3-976 4040

USA Headquarters

AudioCodes Inc, 2890 Zanker Road, Suite # 200

San Jose, CA 95134

Tel: +1-408-577-0488

Fax: +1-408-577-0492

AudioCodes Offices Worldwide

Beijing, Boston (MA), Chicago (IL), London

Mexico City, Paris, Raleigh (NC), Somerset (NJ), Tokyo

info@audiocodes.com

www.audiocodes.com