Release Notes

AudioCodes Media Gateways

Analog & Digital Media Gateways

Version 6.6

audiocodes

Table of Contents

Notice

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 accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: June-09-2025

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

WEEE EU Directive

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

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Document Name
MP-11x SIP Hardware Installation Manual
MP-124 SIP Hardware Installation Manual
MP-11x and MP-124 SIP User's Manual Ver. 6.6
SNMP User's Guide for SIP Enterprise Devices
Mediant 2000 SIP Installation Manual
Mediant 2000 SIP User’s Manual

Document Revision Record Table

LTRT	Feature
26911	■ Mediant 500 MSBR ■ Remote Trigger of Automatic Update or Reset using SIP NOTIFY ■ Increase in Maximum Record-Route Headers in INVITE / 200 OK ■ SRTP State Reset for Session Refresh upon New Key ■ TCP Keep-Alive per SIP Interface ■ Call Disconnect upon User-Defined Session Expiry ■ Accept CANCEL Requests Received after 200 OK ■ Reject SIP Requests with Different User in Request-URI and Previous Contact ■ Testing SIP Calls Filtering Syslog Messages and Debug Recordings ■ ENUM Domain Name as FQDN and NRENum Support ■ V.150.1 SDP Format Double Wink-Start Signaling and Polarity Reversal ■ Increase in Maximum SIP Calling Name Manipulation Rules ■ Simultaneous Negotiation of Fax (T.38) and Modem (V.150.1) Relay CED Tone ■ Different RTP Ports for Held and New Call by FXS Endpoint ■ Interworking User-to-User Header with Text Format to UUIE IA5 Characters in Q.931 Messages ■ New Format for re-INVITE for Call Hold ■ Disconnect IP-to-Tel Call upon Answer Machine Detection ■ Calling Name Retrieval from AD using LDAP Query ■ SAS Emergency upon OPTIONS Only Response Failure ■ Increase in Number of Maximum Transcoding Sessions ■ User Registration Time per IP Profile ■ Interworking DTMF Payload Type for RFC 2833 ■ Removing 'gop' parameter in SBC Authentication Challenge ■ Media (RTP) Normalization Increase in Maximum Number of SBC IP-to-IP Routing Rules ■ Increase in Maximum Number of Classification Rules ■ SIP Response Code for Unclassified Calls ■ Call Forking to Available Contacts Only ■ Call Forking of Specific Contact to all Contacts under AoR ■ Termination of REGISTER for Shared Lines ■ Interworking Call Hold and Retrieve Requests ■ Cloud Resilience Package Application ■ Multiple IP Interfaces per VLAN ■ DHCP Server Options / DHCP Client Option 121 ■ Monitoring IP Entity and HA Switchover upon Ping Failure ■ Redundant Device Display on Web Home Page of Active Unit ■ B-Channel Restart ■ FXS Line Testing ■ Zero Configuration using AudioCodes HTTPS Redirect Server ■ Automatic Update using Zero Configuration Certificate ■ Automatic Update using CLI Scripts ■ Automatic Update through WAN Interface ■ Configuration of Automatic Update using CLI ■ Web Access from Any Interface ■ Clear History Alarms Table ■ Quality of Service using MIBs ■ Information on Physical Configuration ■ New show Commands

LTRT	Feature
	■ Show VoIP DSP Status Commands ■ Auto-Configuration Server Discovery via DHCP ■ TR-104 Support
26912	■ Intrusion Detection System ■ Configurable User Information Table via CLI
26913	Mediant 2600 E-SBC
26915	ISO 8859 Character Set Type
26916	Update to Mediant 8xx DSP templates
26942	Constraints Version 6.60A.312.003 and 6.60A.314.004
26947	Constraints and New Features for Version 6.60A.317.001
26951	Resolved Constraints for Version 6.60A.319.003
26951	New Product variant MP-124 Rev. E
26961	Ver. 6.60A.322
26962	Channel capacity update for MP-124 Rev. E
26966	Ver. 6.60A.331
26966	Ver. 6.60A.323.005
26985	Ver. 6.60A.331.005
27093	Ver. 6.60A.336.004
27240	Ver. 6.60A.337
27245	Ver. 6.60A.340.001
27248	Ver. 6.60A.342.003
27271	Ver. 6.60A.347.002
27277	Known constraint added to Ver. 6.60A.347.002
27278	Ver. 6.60A.348
27341	Ver. 6.60A.349.001
27350	Ver. 6.60A.350.001
27354	Ver. 6.60A.352.002
27364	Ver. 6.60A.354
27367	Ver. 6.60A.355.004 Updated Hardware for MP-112 and MP-114 added to New Products section
27375	Ver. 6.60A.357.003
27377	Resolved constraint VI-156238 added to 6.60A.357.003.
27387	Ver. 6.60A.359.001
27443	Ver. 6.60A.360.004
27456	Ver. 6.60A.361
27467	Ver. 6.60A.361.002
27480	Ver. 6.60A.361.005

LTRT	Feature
27486	Ver. 6.60A.362.002
27490	Ver. 6.60A.363.001; products not supported in latest 6.6 removed
27507	Ver. 6.60A.363.003
27526	Ver. 6.60A.363.005
27528	Ver. 6.60A.364
27543	Ver. 6.60A.365
27556	Typo (BlindTransferOnOnHook)
27561	Ver. 6.60A.365.005
27567	Ver. 6.60A.366.002
27586	Ver. 6.60A.366.005
27634	Ver. 6.60A.367.001
27636	Typo
27639	Ver. 6.60A.367.005
27658	Ver. 6.60A.368.002
27663	Ver. 6.60A.368.003
27667	Ver. 6.60A.368.005
27678	Ver. 6.60A.369.001
27684	Ver. 6.60A.369.002
27738	Typo
27739	Ver. 6.60A.369.005
27745	Ver. 6.60A.370.002
27763	RADIUS security feature added to Ver. 6.60A.369.005.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This Release Notes describes the release of Version 6.6. This includes new products, and new hardware and software features.

- Some of the features mentioned in this document are available only if the relevant software License Key has been purchased from AudioCodes and is installed on the device. For a list of available License Keys that can be purchased, please contact your AudioCodes sales representative.
- Open-source software may have been added and/or amended. For further information, contact your AudioCodes sales representative.
- Updates to this document may be made due to significant information discovered after the release or too late in the release cycle to be otherwise included in this release documentation. You can check for an updated version on AudioCodes website at https://www.audiocodes.com/library/technical-documents.
- Release 6.6 no longer supports Mediant 500 MSBR, Mediant 800 Family Series, Mediant 1000B, Mediant 3000, Mediant 2600, Mediant 4000, Mediant Software. Release 6.8 and later should be used for these products.

1.1 Released Software Revision Record

The following table lists the software versions released in Version 6.6.

The latest software versions can be downloaded from AudioCodes' Services Portal (registered users only) at https://services.audiocodes.com.

Table 1: Released Software Revision Record

Software Version	Date
6.60A.370.002	January 2025
6.60A.369.005	September 2024
6.60A.369.002	August 2023
6.60A.369.001	July 2023
6.60A.368.005	May 2023
6.60A.368.003	May 2023
6.60A.368.002	April 2023
6.60A.367.005	November 2022
6.60A.367.001	October 2022
6.60A.366.005	February 2022
6.60A.366.002	October 21, 2021
6.60A.365.005	August 29, 2021
6.60A.365	April 13, 2021
6.60A.364	January 20, 2021
6.60A.363.005	January 5, 2021

Software Version	Date
6.60A.363.003	November 2020
6.60A.363.001	October 2020
6.60A.362.002	August 2020
6.60A.361.005	July 2020
6.60A.361.002	April 2020
6.60A.361	March 2020
6.60A.360.004	November 2019
6.60A.359.001	August 2019
6.60A.357.003	June 2019
6.60A.355.004	April 2019
6.60A.354	March 2019
6.60A.352.002	January 2019
6.60A.350.001	November 2018
6.60A.349.001	September 2018
6.60A.348	August 2018
6.60A.347.002	June 2018
6.60A.342.003	November 2017
6.60A.340.001	October 2017
6.60A.337	July 2017
6.60A.336.004	June 2017
6.60A.331.005	January 2017
6.60A.331	December 2016
6.60A.323.005	June 2016
6.60A.322	May 2016
6.60A.319.003	February 2016
6.60A.317.001	January 2016
6.60A.312.003	December 2015
6.60A.314.004	December 2015
General Availability (GA)	December 2012

1.2 Products Supported in Version 6.6

This section lists the products from the previous release that are also supported in Release 6.6 as well as any new hardware configurations supported on these products.

> Release 6.6 **no longer supports** Mediant 500 MSBR, Mediant 800 Family Series, Mediant 1000B, Mediant 3000, Mediant 2600, Mediant 4000, and Mediant Software. **Release 6.8 and later should be used for these products**.

1.2.1 MediaPack 1xx

This release supports the following existing hardware platforms:

- MP-11x combined FXS/FXO devices:
  - MP-114/FXS+FXO providing 2 FXS ports and 2 FXO ports
  - MP-118/FXS+FXO providing 4 FXS ports and 4 FXO ports
- MP-11x/FXO devices:
  - MP-118/FXO providing 8 FXO ports
  - MP-114/FXO providing 4 FXO ports
- MP-11x/FXS devices:
  - MP-118/FXS providing 8 FXS ports
  - MP-114/FXS providing 4 FXS ports
  - MP-112/FXS providing 2 FXS ports
- MP-124/FXS providing 24 FXS interfaces:
  - MP-124 Rev. E with AC or DC power
  - MP-124 Rev. D with AC or DC power

1.2.2 Mediant 2000

Mediant 2000 continues to be supported.

1.2.2.1 New Hardware

No new hardware has been introduced in this release for Mediant 2000.

1.2.2.2 Existing Hardware

This release supports the following existing hardware:

- Mediant 2000 1U-chassis, hosting a TP-1610 blade supporting up to 16 E1/T1 PRI spans

1.3 Product Naming Conventions

Throughout this document, unless specifically stated, the following terms are used to represent a family of AudioCodes products:

- **MP-1xx:**
  - MP-112
  - MP-114
  - MP-118
  - MP-124
- **MP-11x:**
  - MP-112
  - MP-114
  - MP-118

2 New Products

This section describes the new products and hardware introduced in Release 6.6 as well as the incumbent products supported in this release.

2.1 Updated Hardware for MP-112 and MP-114

MP-112 and MP-114 are now shipped with an updated hardware revision. This updated hardware revision is compatible with Software Version 6.60A.349.003 and later.

The updated hardware revision supports the same feature set as the previous hardware revision, except for three-way conferencing capacity:

- MP-112 supports a single 3-way conference call.
- MP-114 supports two 3-way conference calls. Each established conference call disables one of the FXS ports.

For more information, click here to read the Product Notice on AudioCodes website.

2.2 MP-124 Rev. E

This version introduces new hardware revision for MP-124 VoIP media gateway models that are based on AC power supply and running the SIP protocol (MP124/16S/AC/SIP and MP124/24S/AC/SIP).

The current hardware revision (Rev. D) has been replaced by a new hardware revision (Rev. E), offering the following enhancements and benefits:

- MP-124 Rev. E provides enhanced power surge protection for outdoor FXS cabling. MP-124 Rev. E with Gas Discharge Tube (GDT) for primary protection is ITU-T K.21 basic-compliant, versus MP-124D that requires primary Circa-lightning-protection for ITU-T K.21 basic-compliant.
- MP-124 Rev. E provides a standard RJ-45 connector for RS-232 interface (instead of a DB-9 connector).

MP-124 Rev. E is supported from SIP Software Version 6.60A.301 and later.

Note that even though the software functionality and configuration of these two hardware revisions—MP-124 Rev. D and MP-124 Rev. E—are identical, they use different software firmware files (.cmp):

- MP-124 Rev. E: MP124E_SIP_F6.60A.301.cmp
- MP-124 Rev. D: MP124_SIP_F6.60A.301.cmp

3 New Features, Known and Resolved Constraints

This section describes the new software features, known constraints, and resolved constraints of Release 6.6.

3.1 Version 6.60A.370.002

This version includes only resolved constraints.

3.1.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 2: Resolved Constraints in Version 6.60A.370.002

Incident	Description
157176	The device restarts because of low available memory (syslog sending “malloc size” messages for the SSH task). **Applicable Products:** MP-1xx
157198	If the SIP header Alert-Info contains the string “dr” and doesn’t specify a tone index, the device erroneously attempts to play a Distinctive Ringing tone. **Applicable Products:** MP-1xx

3.2 Version 6.60A.369.005

This version includes new features and resolved constraints.

3.2.1 New Features

3.2.1.1 Enhanced RADIUS Security with Message-Authenticator Attribute

The device now offers robust security for RADIUS-based user authentication, using RADIUS attribute 80 (Message-Authenticator). This attribute ensures the integrity of RADIUS packets, safeguarding against unauthorized access, for example, "man-in-the-middle" attacks.

This feature provides security for both incoming and outgoing RADIUS packets:

- **Outgoing RADIUS messages:** You can enable the device (Network Access Server / NAS) to include the Message-Authenticator attribute in all Access-Request RADIUS packets sent to the RADIUS server. This is applicable only to the Password Authentication Protocol (PAP) authentication method. This functionality is enabled by the following new parameter:

  Ini file: [RadiusPapRequireMsgAuthTx]

  Note: For RADIUS-based SIP message authentication, this parameter is not needed as SIP authentication uses the Digest protocol, which inherently includes the Message-Authenticator attribute.

- **Incoming RADIUS messages:** You can enable the device to require the presence of the Message-Authenticator attribute in all incoming Accept-Accept RADIUS messages from the RADIUS server. If the attribute is not present, the device rejects the message and denies user login. This is applicable to Digest and PAP authentication methods. This functionality is enabled by the following new parameter:

  Ini file: [RadiusRequireMsgAuthRx]

Applicable Application: Gateway.

Applicable Products: MP-1xx.

3.2.2 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 3: Resolved Constraints in Version 6.60A.369.005

Incident	Description
157173	Connectivity (over HTTP/S) to the device’s Web interface is lost (error message “Task WEBS is deleted abnormally”). **Applicable Products:** MP-124E
157175	RADUIS vulnerability (resolved by feature described above). **Applicable Products:** MP-1xx

3.3 Version 6.60A.369.002

This version includes only resolved constraints.

3.3.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 4: Resolved Constraints in Version 6.60A.369.002

Incident	Description
157076	The device resets when OVOC sends it an incremental ini file. **Applicable Products:** MP-1xx

3.4 Version 6.60A.369.001

This version includes only resolved constraints.

3.4.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 5: Resolved Constraints in Version 6.60A.369.001

Incident	Description
157056	The device doesn't support the HTTP response 302 (Moved Temporarily) for ini file download. **Applicable Products:** MP-1xx
157058	DHCP failure occurs because EAP-TLS doesn't end (DHCP should be delayed until after successful 802.1x). **Applicable Products:** MP-1xx

3.5 Version 6.60A.368.005

This version includes only resolved constraints.

3.5.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 6: Resolved Constraints in Version 6.60A.368.005

Incident	Description
157019	The device doesn't support HTTP Strict Transport Security (HSTS). **Applicable Products:** MP-1xx

3.6 Version 6.60A.368.003

This version includes only resolved constraints.

3.6.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 7: Resolved Constraints in Version 6.60A.368.003

Incident	Description
157026	Upon the receipt of a SIP 408 from the main proxy for a sent REGISTER message, the device doesn’t send a REGISTER message to the second proxy, resulting in alternative routing failure. **Applicable Products:** MP-1xx

3.7 Version 6.60A.368.002

This version includes only resolved constraints.

3.7.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 8: Resolved Constraints in Version 6.60A.368.002

Incident	Description
157020 157037	The device as an 802.1x supplicant doesn't support EAP-TLS. **Applicable Products:** MP-1xx

3.8 Version 6.60A.367.005

This version includes only resolved constraints.

3.8.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 9: Resolved Constraints in Version 6.60A.367.005

Incident	Description
156999	The device includes an extension suffix (e.g., 'ext=1234') in the SIP CONTACT header in REGISTER messages sent for the challenge (401/407). **Applicable Products:** MP-1xx

3.9 Version 6.60A.367.001

This version includes only resolved constraints.

3.9.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 10: Resolved Constraints in Version 6.60A.367.001

Incident	Description
156931	The device sends a SIP REGISTER message with a duplicated UUDI in the instance’s URN when the EnableGRUU parameter is configured to 1 (enabled). **Applicable Products:** MP-1xx

3.10 Version 6.60A.366.005

This version includes only resolved constraints.

3.10.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 11: Resolved Constraints in Version 6.60A.366.005

Incident	Description
156748 / 156901	The device fails to send an ini file to OVOC for backup when the ini file is configured with a URL (acSysUploadFileURI SNMP) that is 100 characters or more. As a result, ini file backup fails. **Applicable Products:** MP-1xx
156864	The device fails to upload a secured (encrypted) ini file from the HTTPS server (URL configured by the INIFileURL parameter), generating the error message "INI file is not textual - aborting INI load". As a result, the Auto-Update mechanism fails. **Applicable Products:** MP-1xx
156871	When the device is configured for media security (MediaSecurityBehaviour) to Preferable, it fails to handle a delayed offer re-INVITE, where ACK has both SRTP and RTP. As a result, the device places the call on hold and no voice occurs. **Applicable Products:** MP-1xx

3.11 Version 6.60A.366.002

This version includes only resolved constraints.

3.11.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 12: Resolved Constraints in Version 6.60A.366.002

Incident	Description
156809	The device does not modify the VLAN in the DHCP request after the network side has changed the VLAN over LLDP. As a result, the DHCP process fails. **Applicable Products:** MP-1xx
156844	The device sends a DHCP request twice (once on the boot stage and again on the .cmp stage) when the [DhcpHasLocalIpAddrDuringInit] parameter is set to 0. As a result, the DHCP process fails. **Applicable Products:** MP-1xx

3.12 Version 6.60A.365.005

This version includes only resolved constraints.

3.12.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 13: Resolved Constraints in Version 6.60A.365.005

Incident	Description
156768	The device fails to detect DTMF digits from the Tel side. **Applicable Products:** MP-124E
156788	Even though the device is configured for 802.1x using TLSv1.1 and TLSv1.2, it uses TLSv1.0 when it sends the Client Hello message to the server. **Applicable Products:** MP-11x
156830	The device fails to send a SIP REGISTER message after loading a .cmp file through the Automatic Update mechanism. **Applicable Products:** MP-11x

3.13 Version 6.60A.365

This version includes only resolved constraints.

3.13.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 14: Resolved Constraints in Version 6.60A.365

Incident	Description
156714	The device fails to load the .cmp file due to lack of memory. **Applicable Products:** MP-11x

3.14 Version 6.60A.364

This version includes only resolved constraints.

3.14.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 15: Resolved Constraints in Version 6.60A.364

Incident	Description
156708	The device doesn’t detect an HTTP response 200 without the "OK" string. **Applicable Products:** MP-1xx

3.15 Version 6.60A.363.005

This version includes only resolved constraints.

3.15.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 16: Resolved Constraints in Version 6.60A.363.005

Incident	Description
156667	The device can't change its username and password through SNMP, causing SNMP failure. **Applicable Products:** All
156700	A Gateway authentication failure occurs when the password contains the "&" character. **Applicable Products:** MP-1xx
156704	A Hunt Group failure occurs when the [TrunkGroupSettings_DedicatedConnectionMode] parameter in the Hunt Group Settings table is configured to [-1]. **Applicable Products:** MP-1xx

3.16 Version 6.60A.363.003

This version includes only resolved constraints.

3.16.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 17: Resolved Constraints in Version 6.60A.363.003

Incident	Description
156685	The device fails to send the Server Name Identity (SNI) field in the TLS Client Hello message when redirected to a different HTTPS server during the Auto Update process. **Applicable Products:** MP-1xx

3.17 Version 6.60A.363.001

This version includes only resolved constraints.

3.17.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 18: Resolved Constraints in Version F6.60A.363.001

Incident	Description
156646	The device displays the credentials (username and password) in the Syslog when the user updates the INIFileURL and CMPFileURL parameters through the Admin Page. **Applicable Products:** MP-1xx
156655	INI files are requested continuously upon Automatic Update in Client defaults over TFTP. **Applicable Products:** MP-1xx
156656	The device fails to resolve the DNS type NAPTR. **Applicable Products:** MP-1xx

3.18 Version 6.60A.362.002

This version includes only resolved constraints.

3.18.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 19: Resolved Constraints in Version 6.60A.362.002

Incident	Description
156590	The device's SNMP variable ipNetToMediaPhysAddress doesn't return the correct MAC address. **Applicable Products:** MP-1xx

Incident	Description
156591	The device doesn't send the Chassis ID (IP address) with Link Layer Discovery Protocol (LLDP). **Applicable Products:** MP-1xx

3.19 Version 6.60A.361.005

This version includes only resolved constraints.

3.19.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 20: Resolved Constraints in Version 6.60A.361.005

Incident	Description
156595	This version blocks the Ripple20 vulnerabilities that were discovered by the JSOF research lab on the TCP/IP software library developed by Treck, Inc. **Applicable Products:** MP-1xx; Mediant 2000

3.20 Version 6.60A.361.002

This version includes only resolved constraints.

3.20.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 21: Resolved Constraints in Version 6.60A.361.002

Incident	Description
156507	When using the INIFILEURL parameter for provisioning, credentials are displayed in clear text. **Applicable Products:** MP-11x

3.21 Version 6.60A.361

This version includes only resolved constraints.

3.21.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 22: Resolved Constraints in Version 6.60A.361

Incident	Description
156491 / 156509	The device doesn't support the Answer Machine Detector (AMD) feature. **Applicable Products:** MP-11x (New H/W Revision)

3.22 Version 6.60A.360.004

This version includes only new features and resolved constraints.

3.22.1 New Features

3.22.1.1 Routing of REGISTER Messages During SAS Emergency State

The SAS application can now be configured to route incoming SIP REGISTER messages received from UAs during Emergency state. The device uses the SAS IP-to-IP Routing table to determine the destination of the REGISTER messages. This feature is enabled by the new parameter, SASEmergencyModeRouteRegister.

Applicable Application: SAS.

Applicable Products: MP-1xx.

No Reply Time Saved for Deactivated Call Forward Rule

When an active call forwarding rule is deactivated ('Forward Type' field changed to **Deactivate**) in the Call Forward table, the configured value in the 'Time for No Reply Forward' field is maintained (and value in the 'Forward to Phone Number' field is deleted). Up until now, the 'Time for No Reply Forward' value reverted to default (30) when the rule was deactivated.

Applicable Application: Gateway.

Applicable Products: MP-1xx.

Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 23: Resolved Constraints in Version 6.60A.360.004

Incident	Description
156367 / 156384	When the device is configured with DNS names for registration in the Proxy Set, only one DNS gets resolved into an IP address. **Applicable Products:** MP-11x (new H/W revision)
156383	The 'Dedicated Connection Mode' parameter cannot be configured through the Web interface. **Applicable Products:** MP-11x
156411	Using multiple SSH connections on the device causes a memory leak. **Applicable Products:** MP-11x
156415	The device generates a software watchdog exception when using the INIFileURL parameter with specific values. For example: 'https://urldefense.proofpoint.com/v2/url?u=https-3A__acata.8x8.com_acodesata_&d=DwIGAg&c=--1RjWWBW4Kf6aBAaj53vPItwfT0BR1YjSDV46P5EvE&r=Qn3y4g5bs0aN5rjqx3zVFu-9BvqlaMOeTpC-al16Jh0&m=UXTLAoqLR9FZxOe5sryKOTI6SE-eWOxGpr1mcaMNNMc&s=FOU0TWCgoYD6M2uYN99e_9879-LYnn76akGREeAy_MI&e=<mac>.cfg' **Applicable Products:** MP-11x

3.23 Version 6.60A.359.001

This version includes only resolved constraints.

3.23.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 24: Resolved Constraints in Version 6.60A.359.001

Incident	Description
156097	The device can be configured only through ini file to use a dedicated TCP socket per FXS analog channel. Now, it can also be configured through the Web interface ('Dedicated Connection Mode' parameter has been added to the Hunt Group Settings table). **Applicable Products:** MP-1xx.
156126	When the device uses LLDP and DHCP, it doesn't assign the correct IP address to the device. **Applicable Products:** MP-1xx.
156136	The device doesn't raise an alarm for certificate expiration. **Applicable Products:** MP-1xx.
156185	RADIUS-based login attempt to the device fails because the Service-Type attribute is sent with the wrong length. **Applicable Products:** MP-1xx.
156265	The device's memory consumption is very high when many TLS connections are opened (causing software upgrade failure). **Applicable Products:** MP-1xx.
156268	The device's backup ini file from OVOC fails due to the ini file size. **Applicable Products:** MP-1xx.

3.24 Version 6.60A.357.003

This version includes only resolved constraints.

3.24.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 25: Resolved Constraints in Version 6.60A.357.003

Incident	Description
155837	When the device is configured to allow access (logged in) only to Web browsers using TLS Version 1.2, the Web interface allows access from TLS 1.0 and TLS 1.1 Web browsers. **Applicable Products:** Mediant 2000.
155959	The device generates continuous Syslog messages - "SWWD : Run Task GWAP Ticks 5 (5)". **Applicable Products:** MP-124 Rev. E.
156127	Incomplete measurements of the Local Metrics block appear in RTCP XR PUBLISH reports (should not appear). **Applicable Products:** Gateway.

Incident	Description
156132	The Remote Metrics block appears in RFC 6035 SIP PUBLISH when no RTCP XR is received (should not appear). **Applicable Products:** Gateway.
156238	In specific scenarios (involving number of characters in headers of SIP messages), a memory overflow occurs in one of the device's resources, causing the device to reset. **Applicable Products:** MP-1xx.
156185	Logging into the device through RADIUS fails because the device sends the Service-Type attribute to the RADIUS server with the wrong length. **Applicable Products:** MP-1xx.

3.25 Version 6.60A.355.004

This version includes only resolved constraints.

3.25.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 26: Resolved Constraints in Version 6.60A.355.004

Incident	Description
156054	The device fails to establish a T.38 fax session when the far side sends a short CNG tone. **Applicable Products:** MP-1xx
156128	For RTCP XR, the reported gap duration (GD) appears to wrap on calls that are longer than 65 seconds. **Applicable Products:** Gateway
156129	Silence suppression is not displayed as "On" in any packet capture where it is used. **Applicable Products:** Gateway
156131	MOS scores don't appear when the RTCP reporting interval is greater than the call duration for Local Metrics. **Applicable Products:** Gateway
156136	The device doesn't send an alarm for certificate expiration. **Applicable Products:** Gateway
156155	The device resets upon a CAS transfer. **Applicable Products:** Gateway

3.26 Version 6.60A.354

This version includes only new features and resolved constraints.

3.26.1 New Features

3.26.1.1 Dedicated TCP Socket for FXS Channel Signaling

The device can be configured to use a dedicated TCP socket for SIP traffic (REGISTER, re-REGISTER, SUBSCRIBE, and INVITE messages) for each FXS analog channel (endpoint). The dedicated TCP socket is the socket on which the endpoint successfully registers to the server.

Up until now, multiple endpoints used the same TCP socket. If SIP authentication failed for one endpoint with the server and the server "blacklisted" the TCP socket, it meant that the server blocked traffic from all the other endpoints that used this same socket.

The dedicated socket is used **only** for SIP requests from the Trunk Group (to which the endpoints belong) whose destination is the same as the destination where the endpoint registered (i.e., same Proxy Set and Serving IP Group). If the endpoint is not registered to the Serving IP Group over a TCP connection, calls from the endpoint to the Serving IP Group are rejected (and trigger an immediate registration attempt).

This feature is configured by the new ini file parameter, TrunkGroupSettings_DedicatedConnectionMode (0 is Reuse Connection; 1 - Connection per Endpoint), which has been added to the Trunk Group Settings table. When enabled, the table's 'Serving IP Group' must be configured and the 'Registration Mode' parameter must be configured to **Per Endpoint**.

Applicable Application: Gateway (FXS).

Applicable Products: MP-11x.

Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 27: Resolved Constraints in Version 6.60A.354

Incident	Description
151840	The Syslog messages contains "TPAPP_ErrorHandler" messages due to any specific timer being deleted twice. **Applicable Products:** Gateway.
155953	After the device is upgraded to Version 6.60A.350.001, it stops sending SIP REGISTER messages over TLS (i.e., registration failure). **Applicable Products:** MP-11x.
55983 / 156071	The device experiences DSP errors: "Max number of failures (type=3) was reached for Dsp 0. Dsp is refreshed". **Applicable Products:** MP-124 Rev. E.
156040	Calls of a short duration show erroneous Round-Trip Delay time statistics in SIP PUBLISH messages. **Applicable Products:** MP-11x.

3.27 Version 6.60A.352.002

This version includes only resolved constraints.

3.27.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 28: Resolved Constraints in Version 6.60A.352.002

Incident	Description
153495	When the device receives an RTP stream with duplicate packets (each packet appears twice), the voice towards the Tel side sounds robotic. **Applicable Products:** MP-124 Rev. E.
154510	Upgrading (.cmp file) the device through TR-069 fails with a memory error. **Applicable Products:** MP-1xx.
155796	One-way voice occurs due to incorrect translation of the ptime in SRTP. **Applicable Products:** MP-1xx.
155815	During periods of high traffic, the device loses connectivity with OVOC. **Applicable Products:** Gateway.
155858	Upgrading (.cmp file) the device fails due to a memory error. **Applicable Products:** MP-1xx.
155865	Newly generated certificates show an incorrect value for "Time to Expiration". **Applicable Products:** Gateway.
155873	Loading, using the Automatic Update mechanism, a partial ini file that contains configuration for the Web Users table, causes the device to enter a reset loop. **Applicable Products:** MP-1xx.
155957	The device repeatedly generates the following Syslog message: "Max number of failures (type=3) was reached for Dsp 0". **Applicable Products:** MP-1xx.

3.28 Version 6.60A.350.001

This version includes only resolved constraints.

3.28.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 29: Resolved Constraints in Version 6.60A.350.001

Incident	Description
155486	Delayed response from the DHCP server causes the device to abandon the Auto-Update mechanism. As a result, automatic provisioning fails. The constraint has been fixed by the new parameter, DhcpHasLocalIpAddrDuringInit. **Applicable Products:** MP-1xx.

3.29 Version 6.60A.349.001

This version includes new features and resolved constraints.

3.29.1 New Features

This section describes the new features introduced in this version.

3.29.1.1 Enhanced Blind Call Transfer

The device supports an additional blind transfer method for calls made on FXS interfaces. When this new feature is enabled and a call has been established, to perform a blind transfer, the FXS endpoint simply presses the phone's hook-flash button, dials the second number without a "#" at the end, and then on-hooks the phone within a user-defined interval (configured by TimeBetweenDigits) or before a match is found by DigitMapping. The device sends a SIP REFER message to establish the blind transfer call. If the user on-hooks the phone after the timeout expires, a new second call is established (INVITE message sent). The feature is enabled by the new parameter BlindTransferOnOnHook (by default, disabled).

Up until now (and still existing), blind transfer was activated by dialing the keypad sequence (configured by the KeyBlindTransfer parameter), followed by a transferee destination number. Once the key sequence is dialed, the current call is put on hold (using a re-INVITE message), a dial tone is played, and then the phone number collection starts. After the destination phone number is collected by the device, the device sends it to the transferee in a SIP REFER request in the Refer-To header.

Applicable Product: MP-1xx.

Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 30: Resolved Constraints in Version 6.60A.349.001

Incident	Description
155209	The device cannot be software upgraded (.cmp) using the SIP NOTIFY message. The device generates the error message, "Device does not have enough memory". **Applicable Products:** MP-11x.
155108	For the Automatic Update feature, when using a redirect server with more than one URL location, the device doesn’t reset as expected and automatic provisioning fails. **Applicable Products:** MP-1xx.
154417	When configuring the device to operate with TLS Version 1.2 only, the device can still be accessed (logged in) with TLS Version 1.1 (i.e., security leak). **Applicable Products:** MP-1xx.

3.30 Version 6.60A.348

This version includes only resolved constraints.

3.30.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 31: Resolved Constraints in Version 6.60A.348

Incident	Description
154251	If the device receives an HTTP 302 message from the Redirect server with a new location that is denoted with the "<MAC>" string, the device doesn't recognize the string correctly and replies with an HTTP GET request as is, without parsing the "<MAC>". As a result, automatic provisioning fails. **Applicable Products:** MP-1xx.
154340	The device cannot be upgraded to 6.60A.347.002 due to memory allocation issues with its' DSP. **Applicable Products:** MP-112.

3.31 Version 6.60A.347.002

This version includes known and resolved constraints.

3.31.1 Known Constraints

This section lists known constraints.

Table 32: Resolved Constraints in Version 6.60A.347.002

Incident	Description
154340	This version is **not** supported on MP-112. **Applicable Products:** MP-112.

3.31.2 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 33: Resolved Constraints in Version 6.60A.347.002

Incident	Description
153266	Configuring the device for Automatic Update (provisioning) through a redirect server, the process fails. **Applicable Products:** MP-1xx.
152473	When configuring the device for Automatic Update (provisioning) that includes loading a software file (.cmp), loading the file sometimes fails. **Applicable Products:** MP-1xx.

3.32 Version 6.60A.342.003

This version includes new features and resolved constraints.

3.32.1 New Features

This section describes the new features introduced in this version.

3.32.1.1 Proxy Set Homing and Successful Keep-Alive

This feature provides support for configuring the number of consecutive, successful keep-alive (using OPTIONS method) responses from the primary proxy that are required before the device switches to the proxy after it was offline. This is used when the Proxy Set is configured for homing (i.e., 'Proxy Redundancy Mode' parameter set to **Homing**). Up until now, the device immediately switched back to the primary proxy when it became available again.

To support the feature, the 'Main Proxy Success Detection Retries' (HomingSuccessDetectionRetries) parameter has been added to the Proxy Set table, with optional value of 1 to 300 (default 1).

Applicable Product: MP-1xx.

3.32.1.2 DHCP Option 160 for Automatic Provisioning

This feature provides support for DHCP Option 160, which the device, as a DHCP client, can use to download software (.cmp) and configuration (.ini) files from a provisioning server. Option 160 defines the location (URL address) of the provisioning server and optionally, the names of the required files and their folder location on the server.

Upon device reset or power up, the device sends a DHCP request to a DHCP server for networking parameters (e.g., IP address). The response from the DHCP server can include the networking information as well as Option 160.

The following syntax is supported for defining the URL and configuration/firmware filenames in DHCP Option 160:

- <protocol>://<server IP address or hostname>
- <protocol>://<server IP address or hostname>/<software filename>
- <protocol>://<server IP address or hostname>/;<configuration filename>
- <protocol>://<server IP address or hostname>/<software filename>;<configuration filename>

Where *protocol* can be HTTP, HTTPS, FTP or TFTP. As shown above, a URL can include both the software and configuration filenames. In this case, they must be separated by a semicolon (;) and without spaces.

If the URL does not specify a configuration filename or the file does not exist on the provisioning server, the device requests from the server a "default" configuration file whose name includes the device's product name and MAC address (<Product><MAC>.ini, for example, "MP114FXS00908f5b1035.ini"). If this "default" file also does not exist on the server, the device attempts to retrieve another "default" configuration file whose name includes only the device's product name (<Product>.ini, for example, "MP114FXS.ini"). The device makes up to three attempts to download the configuration file if a failure occurs (i.e., file not exist or any other failure reason). This applies to each of the configuration files, as mentioned previously.

If the URL specifies a software file, the device makes only one attempt to download the file (even if a failure occurs). If the URL does not specify a software file, the device does not make any attempt to download a software file.

Once the device downloads the file(s), it undergoes a reset to apply the configuration and/or software. In addition, once the file(s) has been downloaded, the device ignores all future DHCP

Option 160 messages. Only if the device is restored to factory defaults will it process Option 160 again (and download any required files).

To support the feature, the new parameter, DhcpOption160Support has been introduced, with optional values 0 to disable (default) and 1 to enable DHCP Option 160 handling. A device reset is required for the parameter to take effect.

Applicable Applications: Gateway.

Applicable Products: MP-1xx.

3.32.1.3 SAS Registration Manipulation Table

This feature provides support for configuring multiple SAS registration manipulation rules. Up until now, only a single manipulation rule could be configured. To support the feature, a new dedicated table has been introduced for manipulation – SAS Registration Manipulation table (SASRegistrationManipulation).

Applicable Applications: SAS.

Applicable Products: MP-1xx.

3.32.2 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 34: Resolved Constraints in Version 6.60A.342.003

Incident	Description
147495	The 802.1x username (802.1xUsername) cannot be 32 bits or longer (only up to 31). **Applicable Products:** MP-1xx.

3.33 Version 6.60A.340.001

This version includes new features and resolved constraints.

3.33.1 New Features

This section describes the new features introduced in this version.

3.33.1.1 Disabling Trap for Disabled Ports

This feature provides support for configuring the device to not send the SNMP trap acBoardControllerFailureAlarm if a telephony port is not configured ("disabled"). A disabled port is one that is not configured at all or configured but without a Trunk Group ID (i.e., Trunk Group ID is 0) in the Trunk Group table. The feature is enabled using the new parameter NoAlarmForDisabledPort.

Applicable Product: MP-1xx.

3.33.1.2 Caller ID Enhancement

This feature provides support for caller ID enhancement whereby if a display name is received from the IP side, it is used as the Tel source number. If no display name is received from the IP side, the Tel source number is not affected. The feature is configured by configuring the existing parameter UseDisplayNameAsSourceNumber to the new optional value, Preferred (2).

Applicable Product: MP-1xx.

3.33.1.3 SAS Manipulation Enhancement

This feature provides support for specifying the type of SIP messages (REGISTER and INVITE, REGISTER only, or INVITE only) to apply a configured number manipulation rule for the SAS application. The feature is supported by the new field, 'Rule Apply To' in the SAS Registration Manipulation table.

Applicable Product: MP-1xx.

3.33.2 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 35: Resolved Constraints in Version 6.60A.340.001

Incident	Description
146947	Configuration of lengthy digit map strings (e.g., truncated after 152 characters) cannot be done through the device's Web management interface. **Applicable Products:** MP-1xx.
146890	The device can handle only a single test call session. **Applicable Products:** MP-1xx.
136453	Ports are randomly stuck in unknown states and as a result, the FXS ports cannot be used. **Applicable Products:** MP-124E.
146298	The device does not send clear alarm notifications for all alarms to the EMS. Some of the alarms remained active on EMS. **Applicable Products:** MP-124.
144871	When trying to negotiate the DHE cipher suite with 2048 bits key, the device crashes (resets). **Applicable Products:** MP-1xx.
141998	During a NESUS scan, the device crashes (resets) on massive TLS connections. **Applicable Products:** MP-1xx.

3.34 Version 6.60A.337

This version includes only resolved constraints.

3.34.1 Resolved Constraints

This section lists constraints from previous releases that have now been resolved.

Table 36: Resolved Constraints in Version 6.60A.337

Incident	Description
143446	The device sends the Proxy-Authorization SIP header with "Cnonce" instead of "cnonce" and as a result, the proxy server rejects the INVITE (call) with a 403 Forbidden response. **Applicable Products:** All.
143529	Even if an user account is locked in the Account table, the device still sends a REGISTER for the account. **Applicable Products:** Gateway.
144921	Password of Web users cannot be configured (WebUsers table) using clear text (instead of encrypted) in the ini file and loaded to the device. **Applicable Products:** All.

3.35 Version 6.60A.336.004

This version includes new features and resolved constraints.

3.35.1 New Features

This section describes the new features introduced in this version.

3.35.1.1 Password Display in ini File

This feature provides support for configuring the display format of passwords in the ini file, using the new parameter INIPasswordsDisplayType:

- Obscured: The password characters are concealed and displayed as encoded. The password is displayed using the syntax, $1$<obscured password>, for example, $1$S3p+fno=.
- Hidden: the password is replaced with an asterisk (*).

Applicable Product: MP-1xx.

3.35.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 37: Resolved Constraints for Version 6.60A.336.004

Incident	Description
143446	For proxy authorization, the device sends "Cnonce" (RFC) instead of "nonce", but customer equipment rejects it. As a result, calls fail. **Applicable Products:** All.

Incident	Description
144313	When the AddNpiandTon2CallingNumber is configured to 1 (Yes), the device adds NPI and TON twice to the calling number on outgoing INVITEs as a result of REFER. As a result, call transfer fails. **Applicable Products:** Mediant 2000.
143529	When the device is locked as a Gateway and a single Account is unlocked, all users are registered, instead of only the unlocked Account users. **Applicable Products:** MP-1xx; Mediant 2000.
143310	A memory leak occurs during TLS connection creation, resulting in call failure. **Applicable Products:** All.
142124	When the device receives illegal characters in the calling number, it stops processing calls, resulting in call failure. **Applicable Products:** MP-1xx; Mediant 2000.
141198	MLPP preemption is not functioning on FXS endpoints. **Applicable Products:** Analog MP-1xx; Mediant 2000.
140977	Outgoing faxes using T.38 does not function. As a result, faxes fail. **Applicable Products:** MP-124E.
140814	When employing automatic update, there is no way to determine whether there is a new firmware file over HTTP(S) without loading it. **Applicable Products:** All.
140500	When using the Automatic Update mechanism and a new software file (.cmp) is downloaded and burned to the device, there is no option to reset the device without saving configuration to flash. **Applicable Products:** All.
140467	When enabling FIPS 140 and media security, the device enters into a restart loop. **Applicable Products:** All.

3.36 Version 6.60A.323.005

This version includes only resolved constraints.

3.36.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 38: Resolved Constraints for Version 6.60A.323.005

Incident	Description
135012	When loading a .cmp file through the automatic update process, the device downloads a .cmp file and then attempts erroneously to download another .cmp file, resulting in software upgrade failure. This is due to lack of device memory resources. **Applicable Products:** Gateway.

Incident	Description
134631	When the device requests an ini file during the automatic update process, it always sends the MAC address (in the ini file URL) in upper case letters. If the ini file is defined in lower case on the HTTP server, ini file download fails as the HTTP server adheres to case sensitivity. This has been resolved: If the ini file URL includes "<MAC>", the device sends the MAC address in upper case; if it includes "<mac>", it sends it in lower case. **Applicable Products:** Gateway.
134630	During the automatic update process, even though the AutoUpdateCmpFile parameter is configured to 0, the device erroneously attempts to download the .cmp file (which fails). **Applicable Products:** Gateway.
134542	When ISDN tunneling is enabled, the device attempts to re-negotiate the B-channel instead of using the B-channel on which the call was initially established. As a result, call failure occurs. **Applicable Products:** Gateway.
133962	When the device operates for over 620 days, one of the counters overflow and causes all PSTN timers to expire sooner than normal (e.g. 5 seconds instead of 50 seconds). As a result, calls are untimely disconnected. A workaround is to reset the device. **Applicable Products:** Gateway.
132481	When the device sends SIP PUBLISH messages for call segments (calls whose media parameters such as a coder has changed during the call), the SSRC for local and remote streams in the first PUBLISH is always "0xffffffff", resulting in incorrect quality report information. **Applicable Products:** Gateway.
133390	The device does not send RTP traffic if it has TX overruns (occurring, for example, if there are collisions on the Ethernet port). As a result, one-way voice occurs. **Applicable Products:** MP-1xx; Mediant 2000.

3.37 Version 6.60A.331.005

This version includes only resolved constraints.

3.37.1 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 39: Resolved Constraints for Version 6.60A.331.005

Incident	Description
139732	When the device tries to establish a TLS connection with the OCSP server using a chained certificate, the device crashes (resets). **Applicable Products:** All.
140287	The device stops registering with the proxy server if it receives a SIP 407 (with "stale=FALSE") response from the server when it sends a REGISTER message. This bug has been resolved by the new parameter IgnoreAuthorizationStale, which when enabled, the device re-sends the REGISTER message even it was previously rejected by a 407 with "stale=FALSE". **Applicable Products:** Gateway.

Incident	Description
139559	When the device is loaded with a Client Default ini file which contains DHCPEnable=1 and INIFileURL, the device stops the DHCP functionality. **Applicable Products:** All.
139594	When configuring the Admin password in the Web interface, by copying-and-pasting a password that is greater than 20 characters, the Web field erroneously accepts this long password, but when trying to log in, the Web interface cuts the password to 19 characters (the limit) and as a result, login is denied. A workaround is to make sure that the password is less than 20 characters. (The bug is fixed – Web field does not allow pasting passwords greater than 20 characters.) **Applicable Products:** All.

3.38 Version 6.60A.331

This version includes new features and resolved constraints.

3.38.1 New Features

This section describes the new features introduced in this version.

3.38.1.1 SNMP SysDescr OID for MP-124E

This feature provides support for the SNMP OID SysDescr for the MP-124E model.

Applicable Product: MP-124E.

3.38.2 Resolved Constraints

Constraints from previous versions that have now been resolved include the following:

Table 40: Resolved Constraints for Version 6.60A.331

Incident	Description
138486	SNMP V2 keep-alive messages cause the device to crash (and reset). **Applicable Products:** Gateway.
137891	Loading an ini file containing configuration of alternative routing in the IP-to-IP Routing table, causes the device to crash (and reset). **Applicable Products:** Gateway.
137673	If the device rejects an INVITE and then receives a subsequent INVITE with the same Call-ID and From values, the device rejects the call. **Applicable Products:** Gateway.

3.39 Version 6.60A.322

This version includes only new features.

3.39.1 New Features

This section describes the new features introduced in this version.

3.39.1.1 RTCP XR per Media Segment

This feature provides support for the device to send RTCP XR (in SIP PUBLISH messages) at the end of each media segment during a call session. A media segment is a change in media, for example, when the coder is changed or when the caller toggles between two called parties (using call hold/retrieve). The RTCP XR sent at the end of a media segment contains information only of that segment. For call hold, the device sends an RTCP XR each time the call is placed on hold and each time it is retrieved. In addition, the Start timestamp in the RTCP XR indicates the start of the media segment; the End timestamp indicates the time of the last sent periodic RTCP XR (typically, up to 5 seconds before reported segment ends.

The feature is configured by setting the existing parameter, RTCPXRReportMode to the new option, **End Call & End Segment**.

Applicable Products: Gateway.

3.39.1.2 Upgraded OpenSSL Library

This feature provides support for an upgraded OpenSSL library - from Version 0.9.8o to 1.0.2g - used by the device for cryptographic processing.

This version covers many security vulnerability fixes and new features. For more information, see https://www.openssl.org/news/openssl-1.0.1-notes.html and https://www.openssl.org/news/openssl-1.0.2-notes.html.

Applicable Products: Gateway.

3.40 Version 6.60A.319.003

This version includes only resolved constraints.

3.40.1 Resolved Constraints

Below are constraints from previous versions that have been resolved in this version:

1. When the device is configured to T.38 and initiates a fax call, if none of the sides switch to T.38 fax, the call fails.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateway.

2. The device is unable to connect secured SIP telephones and therefore, calls are sent by the device as not secured.

   The constraint has now been resolved.

   SR: 754731

   Applicable Products: All.

3. The device cannot be assign an ifA*lias* object (name) to the device's FXS ports and Ethernet ports through SNMP.

The constraint has now been resolved.

SR: 769613

Applicable Products: MP-1xx.

4. Voice mail messages cannot be deleted from a voice mail server. The scenario occurs when the device communicates with the server through a PRI QSIG connection to a router. After the user deletes a voice mail message, the router is unable to send MWI deactivates to the PBX and therefore, the device does not receive this information correctly.

   The constraint has now been resolved.

   SR: 769983

   Applicable Products: Digital Gateway.

5. The device sends incorrect voice quality reports as the synchronization source (SSRC) for LocalAddr and RemoteAddr fields in the first SIP PUBLISH message is wrong.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateway.

6. When routing is according to proxy server (Proxy Set) instead of the Tel-to-IP Routing table, blind call transfer fails. The workaround is to route according to the Tel-to-IP Routing table.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateway.

7. MOS scores reported by the device in SIP PUBLISH messages at the end of a call is calculated incorrectly if the voice codec changes during the call.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: All.

8. When SNMP is used to obtain a Certificate Signing Request (CSR) and the size of the contents of the CSR field is large, the device's SNMP deletes half of it and therefore, cannot obtain a new certificate. The workaround is to use the device's Web interface for CSR.

   The constraint has now been resolved.

   SR: 767141

   Applicable Products: All.

3.41 Version 6.60A.317.001

This version includes new features and resolved constraints.

3.41.1 New Features

This section describes the new features introduced in this version.

3.41.1.1 Enhanced FXS Channel Cut-Through in Off-Hook

This feature provides enhanced support for the FXS Channel Cut-Through feature, which allows phones connected to the device’s FXS ports to automatically receive IP calls even when in off-hook state (and no call is currently active). The feature is useful for paging calls, which provides a one-way voice path from the paging phone to the paged phones (FXS phones).

The enhanced feature is that during the off-hook state, the device does not play any tones (before or after the call).

This new feature also provides support for configuring the functionality per specific calls using IP Profiles with the new IP Profile parameter. Up until this release, Channel Cut-Through was enabled by the global parameter, CutThrough.

[TelProfile_IP2TelCutThroughCallBehavior]	Enables the Cut-Through feature. ■ [0] NO cut through, no paging = Disabled ■ [1] cutThrough = Channel Cut-Through enabled. When the IP side ends the call, the device can play a reorder tone to the Tel side for a user-defined duration (configured by the CutThroughTimeForReorderTone parameter). Once the tone stops playing, the FXS phone is ready to automatically answer another incoming IP call, while in off-hook state. ■ [2] cutThrough + paging = Channel Cut-Through enabled and no tones are played.

Applicable Products: Analog.

3.41.1.2 Simultaneous DTMF Transport in SIP INFO and RFC 2833

This feature provides support for simultaneously sending DTMF tones (signals) in SIP INFO messages (out-of-band) as well as in RTP media streams with a special payload type as defined by RFC 2833 (in-band). This is relevant when the FirstTxDTMFOption parameter is configured for RFC 2833 (4) and the new parameter, described below, is configured to an out-of-band DTMF transport format.

To support the feature, the following global parameter has been added:

[AdditionalOutOfBandDtmfFormat]	Enables the device to send DTMF in SIP messages, e.g., INFO (out-of-band) as well as in RTP media streams (in-band) according to RFC 2833 when the FirstTxDTMFOption parameter is configured to 4. ■ [0] unknown = (Default) DTMF is sent according to FirstTxDTMFOption. ■ [1] Nortel ■ [2] cisco ■ [3] threecom ■ [4] korea

Applicable Products: Analog.

3.41.1.3 Connection ("c=") Line Display in SDP Offer/Answer

This feature provides support for configuring how the device displays the Connection ("c=") line ("c=") in the SDP Offer/Answer model.

To support the feature, the following parameter has been added:

[GwSDPConnectionMode]	■ [0] = (Default) The Connection ("c=") line is displayed as follows: • Offer: In the session description only. • Answer: In each media ("m=") description. ■ [1] = For Offer and Answer, the Connection ("c=") line is displayed only in the session description; not in any media ("m=") descriptions ■ [2] = The Connection ("c=") line is displayed only in media ("m=") descriptions.

Applicable Products: Gateway.

3.41.2 Resolved Constraints

Below are constraints from previous versions that have been resolved in this version:

1. The device's up time display (on the Device Information page) returns to zero after approximately 497 days.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: All. A password (command shell) is required to load Customer coefficient files to the device.

   The constraint has now been resolved (password is not required).

   SR: 769681

   Applicable Products: MP-1xx.

3. When the device initially receives a re-INVITE for VBD and then a subsequent re-INVITE for T.38, it does not send T.38 No-Op packets. This causes the fax to fail.

   The constraint has now been resolved.

   SR: 769253

   Applicable Products: MP-1xx. The device uses an incorrect payload type for faxes when it is configured with10-msec ptime for G711 and G711 VBD coders. When the device switches to VBD mode (upon fax/modem detection), the VBD RTP packets are sent at 20-msec size.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: All.

3.42 Version 6.60A.314.004

This version includes new features and resolved constraints.

3.42.1 New Features

This section describes the new features introduced in this version.

3.42.1.1 RTCP XR Sent to IP Group

This feature provides support for sending RTCP XR (in SIP PUBLISH messages) to a specific IP Group for Gateway calls. Up until this release, the device could only be configured to send RTCP XR to an Event State Compositor (ESC) server, where the server's address was defined by the RTCPXREscIP parameter. Now, the administrator can specify an IP Group instead. In such cases, the RTCP XR is sent to the address configured for the Proxy Set associated with the IP Group.

publication-ip-group-id [PublicationIPGroupID]	Specifies the IP Group to where the RTCP XR must be sent. If the value is -1 (default) or 0, the RTCP XR is sent to the address as configured by the RTCPXREscIP parameter. The SIP Request-URI header of the PUBLISH message contains the value as configured for the IP Group Name (IPGroup_Name) and not the values of SEM server IP address and port. The From and To headers contain the telephone extension number of the Tel user that is connected to the device.

Applicable Products: MP-1xx; Mediant 2000.

3.42.2 Resolved Constraints

Below are constraints from previous versions that have been resolved in this version:

1. The performance monitoring MIB for Gateway calls, acPMSIPTel2IPTrunkGroupEstablishedCallsVal, which reports the number of currently established Tel-to-IP calls per Trunk Group, indicates an erroneous count for calls of 1 second or less duration. When such calls disconnect, the counter is not decreased accordingly, but continues to indicate as though they are still established.

   The constraint has now been resolved.

   SR: 769333

   Applicable Products: Mediant 2000.

2. When the device (Gateway application) is configured to send No-Op packets when switching to T.38, if it receives a re-INVITE to switch to VBD before receiving the T.38 re-INVITE, it does not send the T.38 No-Op packets.

   The constraint has now been resolved.

   SR: 769253

   Applicable Products: MP-1xx; Mediant 2000.

3. If the device receives a SIP message containing a User-to-User header field that has a string enclosed by quotation marks (allowed by the SIP standard), it rejects the message.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: All.

4. If the device is configured with multiple Proxy Sets (i.e., multiple proxy servers), after the device has been in operation for a long time, it stops sending keep-alive SIP OPTIONS messages to some of the servers. These servers are considered by the device as not in service.

   The constraint has now been resolved.

   SR: 767763

   Applicable Products: All. The device erroneously crashes (and resets) upon a rare exception.

   The constraint has now been resolved.

   SR: 767099

   Applicable Products: All.

6. For Tel-to-IP fax re-routing, the device does not add a SIP Diversion header. For example: If the Tel-to-IP call results in a call redirection, the device adds a Diversion header to the outgoing INVITE. However, if the device detects a fax signal, it disconnects the initial call and generates a new INVITE to another destination but erroneously without a Diversion header.

   The constraint has now been resolved.

   SR: 766717

   Applicable Products: MP-1xx; Mediant 2000.

7. When the device receives a call from the ISDN in overlap dialing mode, it erroneously overrides the number plan (NPI) and number type (TON) information elements with default values. This results in the device sending incorrect source and destination numbers in the outgoing INVITE. The workaround is to apply number manipulation rules.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 2000.

8. The device's Auto-Update mechanism using HTTP fails on boot-up when it is configured to work with DHCP and HTTP automatic update.

   The constraint has now been resolved.

   SR: 764397

   Applicable Products: All.

3.43 Version 6.60A.312.003

This version includes only resolved constraints.

3.43.1 Resolved Constraints

Below are constraints from previous versions that have been resolved in this version.

1. When the device is enabled for DHCP and it receives Option 120 from the DHCP server in the DHCP response, it automatically adds the SIP servers (from the Option 120) to Proxy Set ID #0 in the Proxy Sets table. To overcome the bug, a new parameter DHCP120OptionMode has been added, which when set to 0, instructs the device to ignore DHCP Option 120.

   The constraint has now been resolved.

   SR: 762543

   Applicable Products: All.

2. One-way voice occurs for FXO and FXS interfaces when the 3xxBehavior parameter is set to 1 / Redirect (uses the same call identifier in the new INVITE as the original call) and the UseDifferentRTPportAfterHold parameter is set to 1 / Enable.

   The constraint has now been resolved.

   SR: 749395

   Applicable Products: All.

3. The device process call forking incorrectly for Tel-to-IP calls in the following example scenario: 1) A calls B, 2) B transfers A to C, 3) the device detects call forking, 4) C transfers A to D and then 5) the device detects call forking again.

   The constraint has now been resolved.

   SR: 756607

   Applicable Products: MP-1xx.

4. When the device employs ISDN overlap dialing, the TimeBetweenDigits parameter erroneously resulted in the device starting the interval from the beginning of dialing and not resetting between digits. This resulted in call failure.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 2000.

3.44 Version GA

This section describes the GA version.

3.44.1 New Features

This section describes the new features introduced in the GA version.

3.44.1.1 SIP General Features

This subsection describes the new general SIP features.

3.44.1.1.1 Intrusion Detection System

This feature provides support for detecting malicious attacks on the device and for raising SNMP traps to notify when such attacks occur. If notifications of malicious activity is received, preventative action can be taken. This may include, for example, configuring a blacklist for the IP address from where the attack arrived.

There are many types of malicious attacks, the most common being:

- Denial of service (DoS) or Distributed Denial of Service (DDoS), which prevents a server from functioning correctly by directing a large amount of requests (sometimes meaningless and sometimes legitimate). DoS includes message payload tampering, message flow tampering, and message flooding.
- SPAM over Internet Telephony (SPIT) is unwanted, automatically dialed, pre-recorded phone calls using VoIP. It is similar to e-mail spam.
- Theft of Service (ToS) for example, by phreaking, which is a type of hacking that steals service (i.e., free calls) from a service provider, or uses a service while passing the cost to another person.

The IDS configuration is based on IDS Policies, where each policy can be configured with a set of IDS rules. Each rule defines a type of malicious attack to detect and the number of attacks during an interval (threshold) before an SNMP trap is sent. Each policy is then applied to a target under attack (SIP interface) and/or source of attack (Proxy Set and/or subnet address).

To support this feature, the following parameters were added:

Web: Intrusion Detection System (IDS) CLI: enable-ids **[EnableIDS]**	Enables the IDS feature. - [0] Disable (default) - [1] Enable **Note:** For this parameter to take effect, a device reset is required.
CLI: ids-clear-period **[IDSAlarmClearPeriod]**	Defines the interval (in seconds) after which an IDS alarm is cleared from the Active Alarms table if no thresholds are crossed during this time. However, this "quiet" period must be at least twice the Threshold Window value. For example, if IDSAlarmClearPeriod is set to 20 sec and the Threshold Window is set to 15 sec, the IDSAlarmClearPeriod parameter is ignored and the alarm is cleared only after 30 seconds (2 x 15 sec). The valid value is 0 to 86400. The default is 300.
Web: IDS Policy Table **[IDSPolicy]**	Defines IDS Policies. The format of the ini file parameter is: [IDSPolicy] FORMAT IDSPolicy_Index = IDSPolicy_Name,

	IDSPolicy_Description; [\IDSPolicy] For more information, see the User's Manual.
Web: IDS Rule Table **[IDSRule]**	Defines rules for the IDS Policies. The format of the ini file parameter is: [IDSRule] FORMAT IDSRule_Index = IDSRule_Policy, IDSRule_RuleID, IDSRule_Reason, IDSRule_ThresholdScope, IDSRule_ThresholdWindow, IDSRule_MinorAlarmThreshold, IDSRule_MajorAlarmThreshold, IDSRule_CriticalAlarmThreshold; [\IDSRule] For more information, see the User's Manual.
Web: IDS Match Table **[IDSMatch]**	Defines target rules per IDS Policy. The format of the ini file parameter is: [IDSMatch] FORMAT IDSMatch_Index = IDSMatch_SIPInterface, IDSMatch_ProxySet, IDSMatch_Subnet, IDSMatch_Policy; [\IDSMatch] For more information, see the User's Manual.

Applicable Products: Mediant 2000.

3.44.1.1.2 Configurable User Information Table via CLI

This feature provides support for configuring the User Info / Registration database through CLI. Up until now, this database could be configured only in an external User Info file (text based) which was then loaded to the device. Once loaded, it could only be modified by loading a new User info file. This new feature now enables adding, editing, deleting, and searching users in this database, through CLI.

This database is used for the following applications:

- Gateway application: maps PBX extensions connected to the device to "global" IP numbers, and registers each PBX user to an external registrar server

To support this feature, the following new CLI tables have been added:

- Gateway application:

  ```
  gw-user-info
  ```

  Includes the following parameters:

  - **pbx-ext:** PBX extension (e.g., 405)
  - **global-phone-num:** Global phone number (e.g., 405)
  - **display-name:** Display name (e.g., Ext405)
  - **username:** Username (e.g., user405)
  - **password:** Password (hidden for security)
  - **status:** Registration status ("registered" or "not-registered")

The following commands can be used:

- To view all database entries, use the **`display`** command, as shown in the example below:

  ```
  (sip-def-proxy-and-reg)# user-info gw-user-info display
  ---- gw-user-info-0 ----
    pbx-ext (405)
    global-phone-num (405)
  ```

```
  display-name (Ext405)
  username (user405)
  password (0aGzoKfh5uI=)
  status (not-resgistered)
---- gw-user-info-1 ----
  pbx-ext (406)
  global-phone-num (406)
  display-name (Ext406)
  username (user406)
  password (0KCwoaDg5eA=)
  status (not-resgistered)
```

- To view a specific entry, enter the database record entry number and **display** command:

```
(sip-def-proxy-and-reg)# user-info gw-user-info 1
(gw-user-info-1)# display
  pbx-ext (406)
  global-phone-num (406)
  display-name (Ext406)
  username (user406)
  password (0KCwoaDg5eA=)
  status (not-resgistered)
```

- To add and/or define a user, use the **set** command, as shown in the example below:

```
(sip-def-proxy-and-reg)# user-info gw-user-info 1
(gw-user-info-1)# set username user406b
```

- To apply your changes, you must enter the **exit** or **activate** command per user addition or modification (not per parameter)

```
(gw-user-info-1)# <activate | exit>
```

- To search a user (by pbx-ext for Gateway), use the **find** command, as shown in the example below:

```
sip-def-proxy-and-reg)# user-info find <PBX-EXT e.g., 300 |
Local-User, e.g., JohnDoe>
300: Found at index 3 in GW user info table, not registered
```

  The search locates the table index belonging to the searched user.

- To delete a user, use the **no** command, as shown in the example below:

```
(sip-def-proxy-and-reg)# no user-info gw-user-info <database
index entry, e.g., 1)
```

Note: If you load a User Info file to the device, all previous database entries are removed and replaced with the users in the loaded User Info file.

Applicable Products: All.

3.44.1.1.3 Remote Trigger of Automatic Update or Reset using SIP NOTIFY

This feature provides support for remotely triggering the Automatic Update feature (if configured) or a device reset, using a SIP NOTIFY message with an Event header set to one of the following proprietary values:

- Event: check-sync;reboot=false: Activates the Automatic Update mechanism, if configured (i.e., in the loaded ini file). The NOTIFY message with this Event header value is shown below:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
```

```
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=false
```

- Event: check-sync;reboot=true: Triggers a device reset.

To support this feature, the following new parameter has been added:

SIP Remote Reset CLI: sip-remote-reset [EnableSIPRemoteReset]	Enables a specific device action upon the receipt of a SIP NOTIFY request, where the action depends on the value received in the Event header: ■ 'check-sync;reboot=false': triggers the regular Automatic Update feature (if Automatic update has been enabled on the device). ■ 'check-sync;reboot=true': triggers a device reset. The valid values: ■ [0] Disable (default) ■ [1] Enable Notes: ■ This feature does not trigger the automatic update mechanism based on the Zero Configuration feature. ■ The Event header value is proprietary to AudioCodes.

Applicable Products: All.

3.44.1.1.4 Increase in Maximum Record-Route Headers in INVITE / 200 OK

This feature provides support for an increase in the maximum number of supported SIP Record-Route headers to 20 that can be received in SIP INVITE requests or 200 OK responses. If the device receives an INVITE containing more than 20 Record-Route headers, it responds with a 513 Message Too Large response, indicating that the message is too large for processing.

Applicable Products: All.

3.44.1.1.5 SRTP State Reset for Session Refresh upon New Key

This feature provides support for synchronizing the Secure Real-time Transport Protocol (SRTP) state between the device and a server (e.g., Microsoft Lync Server 2010) that resets the SRTP roll-over counter (ROC) when a new SRTP key is generated upon a SIP session expire. This feature ensures that the ROC, which is one of the parameters used in the SRTP encryption/decryption process of the SRTP packets, is synchronized on both sides for transmit and receive packets.

When this feature is enabled and a session expires (according to the Session-Expires SIP header), causing a session refresh through a re-INVITE, the device or the server generates a new key and the device resets the ROC index (and other SRTP fields), as done by the server. Thus, the SRTP between the device and the server is synchronized.

If this feature is disabled and the device operates with a server that resets the ROC upon a re-key generation, one-way voice may occur.

To support this feature, the following new parameter has been added:

CLI: srtp-state-behavior-mode [ResetSRTPStateUponRekey]	Enables the resetting of the SRTP state (such as ROC) when a new session key is generated due to a session expires. ■ [0] Disable (default) = ROC is not reset.

	■ [1] Enable = ROC index used on the device side is reset and thereby, synchronized with the ROC on the server side (e.g., Lync) whenever a new session key is generated.
IP Profile Table	This feature can also be configured for an IP Profile, using the following parameter: IpProfile_SRTPStateBehaviorMode: ■ [0] Default ■ [1] Lync

Applicable Products: All.

3.44.1.1.6 TCP Keep-Alive per SIP Interface

This feature provides support for TCP keep-alive with a remote SIP entity (UAS or UAC) per SIP interface. A TCP keep-alive packet is an ACK (acknowledge) flag with the sequence number set to one less than the current sequence number for the connection. A host receiving one of these ACKs responds with an ACK for the current sequence number.

TCP keep-alive can be used, for example, to keep a NAT entry open for clients located behind a NAT server or simply to check that the connection to a remote network entity is available.

To support this feature, the following new parameters have been added:

SIP Interface Table - TCP Keepalive Enable [SIPInterface_TCPKeepAliveEnable]	Enables the TCP Keep-Alive feature per SIP Interface: ■ [0] No (default) ■ [1] Yes
TCP Keep Alive Idle Time [TCPKeepAliveTime]	Defines the interval (in sec) between the last data packet sent and the first keep-alive probe to send. The valid value is 10 to 65,000. The default is 60. Note: Simple ACKs such as keep-alives are not considered data packets.
TCP Keep Alive Interval Time [TCPKeepAliveInterval]	Defines the interval (in sec) between consecutive keep-alive probes, regardless of what the connection has exchanged in the meantime. The valid value is 10 to 65,000. The default is 10.
TCP Keep Alive Retry Number [TCPKeepAliveRetry]	Defines the number of unacknowledged keep-alive probes to send before considering the connection down. The valid value is 1 to 100. The default is 5.

Applicable Products: All.

3.44.1.1.7 Call Disconnect upon User-Defined Session Expiry

This feature provides support for configuring a session expiration time that if reached, the device disconnects the call (by sending a SIP BYE). SIP UAs periodically send re-INVITE or UPDATE requests, referred to as session refresh requests to keep the session alive. The session ends when no session refresh is sent within this interval (conveyed in the Session-Expires header). With this feature, the session expiration time is either one-third (1/3) of the Session-Expires header value, or the value configured by the new parameter associated with this feature (see below); the one that has the minimum time is used.

To support this feature, the following new parameter has been added:

Session Expires Disconnect Time CLI: session-exp-disconnect-time [SessionExpiresDisconnectTime]	Defines the minimum interval for session expires. The session is disconnected if the refresher did not send a refresh request before one third of the session expires time, or before the time defined by this parameter (minimum of them). The valid range is 0 to 32 (in seconds). The default is 32.

Applicable Products: All.

3.44.1.1.8 Accept CANCEL Requests Received after 200 OK

This feature provides support for enabling the device to accept or reject a SIP CANCEL request that is received after the receipt of a 200 OK during an established call. Normally, if a CANCEL is received after a 200 OK, the UA ignores the CANCEL and sends a 200 OK, maintaining call connection. With this new feature, the device can accept such a CANCEL request by responding with a SIP 200 OK and subsequently terminating the call.

To support this feature, the following new parameter has been added:

Reject Cancel after Connect CLI: reject-cancel-after-connect [RejectCancelAfterConnect]	Determines whether to accept or reject a CANCEL request received after a 200 OK during an established call session. ■ [0] = (Default) Accepts CANCEL by sending 200 OK and terminating session. ■ [1] = Rejects CANCEL by sending SIP 481 Call/Transaction Does Not Exist, and maintains call session.

Applicable Products: All.

3.44.1.1.9 Reject SIP Requests with Different User in Request-URI and Previous Contact

This feature provides support for rejecting SIP requests (for example, ACK, BYE, or re-INVITE) whose user part in the Request-URI is different from the user part received in the Contact header of the last sent SIP request.

To support this feature, the following new parameter has been added:

Verify Received RequestURI CLI: verify-rcvd-requri [VerifyReceevedRequestUri]	Enables verifying that the user part in the Request-URI is the same as the user received in the last sent Contact. ■ [0] Disable (default) = Even if the user is different, the device accepts the SIP request. ■ [1] Enable = If the user is different, the device rejects the SIP request (BYE is responded with 481; re-INVITE is responded by 404; ACK is ignored).

Applicable Products: All.

3.44.1.1.10 Testing SIP Calls

This feature provides support for testing the SIP signaling (setup and registration) of calls and media (DTMF signals) between a simulated phone on the device and a remote endpoint. These tests involve incoming and outgoing calls. Test calls can be dialed automatically at a user-defined interval or manually when required. The simulated phone and remote endpoints are defined as SIP URIs (user@host). The remote destination can be defined as an IP Group, IP address, or according to an Outbound IP Routing rule. The test endpoint can also be configured as the caller or called party.

The advantage of this feature is that it can remotely verify SIP message flow without the end customer being involved in the debug process. It also enhances the debug capabilities of the device.

When a SIP test call is initiated, the device generates a SIP INVITE toward the remote endpoint (e.g., a SIP proxy server). It simulates the SIP call setup process, managing SIP 1xx responses and completing the SIP transaction with a 200 OK.

The device's Web interface displays statistics of the test call scenario, such as total number of calls established, total number of failed call attempts, and the current duration of the test call.

To support this feature, the following new parameters have been added under a new folder in the Web navigation pane (**Configuration** tab > **System** menu > **Test Call**):

Test Call ID CLI: testcall-id [TestCallID]	Defines the prefix number of the simulated test endpoint. All incoming calls with this called (destination) prefix number is identified as a test call and sent to the simulated endpoint. This can be any string. The default is not configured.
Test Call Table CLI: test-endpoint [Test_Call]	Defines the local and remote test endpoints that you want to test. [Test_Call] FORMAT Test_Call_Index = Test_Call_EndpointURI, Test_Call_CalledURI, Test_Call_RouteBy, Test_Call_IPGroupID, Test_Call_DestAddress, Test_Call_DestTransportType, Test_Call_SRD, Test_Call_ApplicationType, Test_Call_AutoRegister, Test_Call_UserName, Test_Call_Password, Test_Call_CallParty, Test_Call_MaxChannels, Test_Call_CallDuration, Test_Call_CallsPerSecond, Test_Call_TestMode, Test_Call_TestDuration, Test_Call_Play, Test_Call_ScheduleInterval; [\Test_Call] Where: ■ EndpointURI = Endpoint's URI (string; default is empty) ■ CalledURI = Called URI (string; default is empty). ■ RouteBy = Type of routing method: • [0] GW Tel2IP = (Default) Calls are matched by (or routed to) an SRD and Application type (defined in the SRD and Application Type parameters below). • [1] IP Group = Calls are matched by (or routed to) an IP Group ID. • [2] Dest Address = Calls are matched by (or routed to) an SRD and application type. ■ IPGroupID = IP Group ID (default is empty) ■ DestType = Destination type: • [0] Tel2IP (default) • [1] IP Group • [2] IP address ■ DestAddress = Destination address (string; default is empty). ■ DestTransportType = Destination transport type: • [-1] Not configured (default) • [0] UDP • [1] TCP • [2] TLS ■ SRD = SRD ID (default is 0). ■ ApplicationType = Application type: • [0] GW & IP2IP (default) ■ AutoRegister = Enables automatic registration: • [0] Disable (default) • [1] Enable ■ UserName = Authentication username (string; default is empty) ■ Password = Authentication password (string; default is empty

	■ CallParty = Defines the call party: • [0] Caller (default) • [1] Called ■ MaxChannels = Maximum number of concurrent channels for the session. ■ CallDuration = Call duration (in seconds). ■ CallsPerSecond = Number of calls per second. ■ TestMode = Defines the test session mode: • [0] Once = (Default) The test runs until the lowest value between the following is reached: - Maximum channels is reached for the test session, configured by 'Maximum Channels for Session'. - Call duration ('Call Duration') multiplied by calls per second ('Calls per Second'). - Test duration expires, configured by 'Test Duration'. • [1] Continuous = The test runs until the configured test duration is reached. If it reaches the maximum channels configured for the test session (in the 'Maximum Channels for Session'), it waits until the configured call duration of a currently established tested call expires before making the next test call. In this way, the test session stays within the configured maximum channels. ■ TestDuration = Test duration (in minutes). ■ Play = Enables play of DTMF: • [0] Disable (default) • [1] DTMF ■ ScheduleInterval = Schedule interval (in minutes); default is 0.
Test Call DTMF String CLI: testcall-dtmf-string [TestCallDtmfString]	Defines the DTMF tone that is played for answered test calls (incoming and outgoing). This applies to all test calls. The DTMF string can be up to 15 strings. The default is "3212333". An empty string means that no DTMF is played. **Note:** To generate DTMF tones, DSP resources are required.

The Test Call Table in the Web interface provides the following commands in the 'Action' drop-down list to initiate and stop test calls of a selected test call table entry:

- **Dial:** initiates (dials) the test call
- **Drop Call:** stops the initiated test call
- **Restart:** drops all active calls of a selected test, and then starts a new test session

In addition, the CLI `debug test-call ip` command has been extended with the following commands:

```
dial from * to * dest-address * sip-interface *
set dest-address * sip-interface *
```

Where:

- `dest-address` sets the host name/address and optional port
- `sip-interface` sets the SIP Interface to which the call must be routed
- `set sip-interfaces` sets a comma-separated list of SIP Interfaces to listen on

The `set calling/called-number` commands were renamed `set calling/called`.

The table is accessed from:

```
# (config-system) test-call test-endpoint <index>
```

Parameters are accessed from:

```
# (config-system) test-call set testcall-id
```

Applicable Products: All.

3.44.1.1.11 Filtering Syslog Messages and Debug Recordings

This feature provides support for filtering Syslog and debug recording (DR) messages sent by the device to a Syslog server or packet capturing application (such as Wireshark), respectively. The benefit of this feature is that it can reduce CPU consumption and minimize negative impact on VoIP performance.

The Syslog / DR filtering feature supports the configuration of up to 30 filtering rules that can be based on one of the following filtering criteria (*type*):

- Any – no filtering (all are sent)
- Specific Trunk Group (applicable only to the Gateway/IP-to-IP application)
- Specific Trunk (applicable only to the Gateway application)
- Specific Trunk/B-channel (applicable only to the Gateway application)
- Specific FXS and FXO port (applicable only to the Gateway application)
- Specific Tel-to-IP routing rule listed in the Outbound IP Routing table (applicable only to the Gateway/IP-to-IP application)
- Specific IP-to-Tel routing rule listed in the Inbound IP Routing table (applicable only to the Gateway/IP-to-IP application)
- Specific IP Group
- Specific SRD
- Specific IP-to-IP routing rule listed in the IP-to-IP Routing table (applicable only to the SAS application)
- Specific user, defined by username or user@host
- IP trace - records any IP stream, for example, HTTP (that isn’t associated with media RTP/RTCP), according to destination and/or source IP address or port and Layer-4 protocol (UDP, TCP or any other IP type as defined by http://www.iana.com). When this option is selected, only the 'Value' field is applicable, supporting the following Wireshark-like expression fields:
  - ip.src / ip.dst: source and destination IP address
  - ip.addr: up to two IP addresses can be entered
  - ip.proto: IP protocol type (PDU) - enum (e.g., 1 is ICMP, 6 is TCP, 17 is UDP)
  - udp / tcp / icmp / sip / ldap / http / https: single expressions of protocol type
  - udp.port / tcp.port: transport layer
  - udp.srcport / tcp.srcport: transport layer for source port
  - udp.dstport / tcp.dstport: transport layer for destination port
  - and / && / == / < / >: between expressions

Each filtering criteria can be configured with a range. For example, you can filter Syslog messages for IP Groups 1 through 4. For each filter criteria, you can enable or disable Syslog messages as well as enable or disable DR.

DR can be filtered using the following criteria:

- None (default)
- Signaling – contains all information related to signaling such as SIP signaling messages, Syslog, and CDR
- Signaling and media (RTP/RTCP/T.38)

- Signaling, media, and PCM - voice signals from and to TDM
- PSTN (ISDN and CAS) traces - applicable only for Trunk-related filters

The Syslog debug level is affected by the setting of the existing parameter, DebugLevel.

To support this feature, the following new table and parameters have been added:

Logging Filters [LoggingFilters]	[LoggingFilters] FORMAT LoggingFilters_Index = LoggingFilters_Type, LoggingFilters_Value, LoggingFilters_Syslog, LoggingFilters_CaptureType; [\LoggingFilters] Where: ■ Type = Defines the filter criteria: • [0] Unknown • [1] Any • [2] Trunk ID • [3] Trunk Group ID • [4] B-channel • [5] FXS / FXO • [6] Tel to IP • [7] IP to Tel • [8] IP Group • [9] SRD • [10] Classification • [11] IP to IP Routing • [12] User • [13] IP Trace ■ Value = Defines the value for the selected Filtering Type. This can be a single value, a range separated by a dash or comma, 'Any' (except for Trunks and FXO/FXS which can be module/port or port), or Wireshark-like expressions for IP traces ■ Syslog = Enables Syslog messages: • [0] Disable (Default) • [1] Enable ■ CaptureType = Enables debug recording: • [0] None (Default) • [1] Signaling • [2] Signaling and Media • [3] Signaling, Media PCM • [4] PSTN trace

Applicable Products: All.

3.44.1.1.12 ENUM Domain Name as FQDN and NRENum Support

This feature provides the following support:

- Configuring the ENUM domain name as any FQDN (e.g., e164.customer.net). Up until this release, the ENUM domain name could be configured only as an e164.arpa domain name (e.g., 3.0.1.9.5.8.9.1.6.3.e164.arpa).

- Support for the NRENum.net (www.nrenum.net) ENUM service (in addition to the already supported e164.arpa ENUM service). NRENum.net is an ENUM service for academia that uses a private dialing plan. NRENum.net provides countries, where the Golden ENUM Tree is unavailable, with the possibility to publish ENUM data. The NRENum.net tree is queried by the participating partners if no ENUM data is found in the Golden Tree. Countries that already have access to the Golden Tree cannot get a delegation in NRENum.net. As soon as the Golden Tree is available in a country, e164.arpa is used and the delegation in NRENum.net is then revoked

To support this feature, the following existing parameter is used:

CLI: enum-service-domain [EnumService]	Defines the ENUM service for translating telephone numbers to IP addresses or domain names (FQDN). For example, e164.arpa, e164.customer.net, or NRENum.net. The valid value is a string of up to 50 characters. The default is "e164.arpa". Note: ENUM-based routing is configured in the Outbound IP Routing table using the "ENUM" string value as the destination address to denote this parameter's value.

Applicable Products: MP-1xx.

3.44.1.1.13 Debug Recording Destination Configuration and Activation

This feature provides support for configuring the capturing server (target) for debug recordings and activating debug recording, using the *ini* file and Web interface.

To support this feature, the following new parameters have been added:

Debug Recording Destination IP **[DebugRecordingDestIP]**	Defines the IP address of the server for capturing debug recording.
Destination Port **[DebugRecordingDestPort]**	Defines the port of the server for capturing debug recording. The default is 925.
Debug Recording Status **[DebugRecordingStatus]**	Starts or stops the Debug Recording tool. ■ [0] Stop (Default) ■ [1] Start

Applicable Products: All.

3.44.1.1.14 New CDR Fields for Call Termination Reasons

This feature provides support for indicating the reason for call termination in Call Detail Records (CDR). This includes support for SIP and PSTN call termination reasons.

To support this feature, the following new CDR fields have been added:

- SipTermReason – SIP termination reason. Possible values can include the SIP methods BYE or CANCEL, or SIP response codes such as 404.
- SipTermDesc – Description of SIP termination reason:
  - SIP reason header if exists, for example: SIP ;cause=200 ;text="Call completed elsewhere".
  - If no SIP Reason header exists, the description is taken from the reason text if exists, of the SIP response code, for example, "417 Unknown Resource-Priority".
  - If no reason text exists in the SIP response code, the description is taken from an internal SIP response mapping mechanism. For example, if the device receives a SIP response "422", it sends in the CDR "422 Session Interval Too Small method" as the description.

- PstnTermReason – Q.850 protocol termination reason. Possible values are 0-127.

Applicable Products: All.

3.44.1.1.15 Unique Session ID per Call Session for Syslog and DR

This feature provides support for automatically assigning (randomly) a unique session identifier (session-id / SID) number per call in the CDR of sent Syslog messages and debug recording packets.

- Gateway application: A call session is considered either as a Tel-to-IP leg or an IP-to-Tel leg, where each leg is assigned a unique SID.

Note that forked legs or alternative legs share the same SID.

The benefit of this feature is that it enables the user to filter the information (such as SIP, Syslog, and media) according to a specific SID.

Applicable Products: All.

3.44.1.1.16 CDR Filtering of Debug Recordings with Wireshark Plugin

This feature provides support for filtering CDRs of debug recording packets received on the Wireshark packet analyzer, based on various attributes such as IP Group and Trunk Group.

To support this feature, a new AudioCodes proprietary plugin, *cdr.dtd* has been introduced for Wireshark. The plugin file is located in the same directory as Wireshark. This plugin provides proprietary Filter attributes in the Wireshark 'Filter' field, selected by typing "cdr." and then choosing the desired attribute from the displayed list.

Applicable Products: All.

3.44.1.1.17 Local LDAP Cache for LDAP Query Results

This feature provides support for storing recent LDAP queries and responses in the device's local cache. The cache is used for subsequent queries, and/or in case of LDAP server failure.

The benefits of this feature include the following:

- Improves routing decision performance using local cache for subsequent LDAP queries
- Reduces number of queries performed on an LDAP server and corresponding bandwidth consumption
- Provides partial survivability in case of intermittent LDAP server failure (or network isolation)

To support this feature, the following new parameters have been added:

LDAP Cache Service CLI: cache [LDAPCacheEnable]	Enables the LDAP cache service. • [0] Disable (default) • [1] Enable **Note:** For this parameter to take effect, a device reset is required.
LDAP Cache Entry Timeout CLI: entry-timeout [LDAPCacheEntryTimeout]	Defines the duration (in minutes) that an entry in the LDAP cache is valid. The default is 1200.
LDAP Cache Entry Removal Timeout CLI: entry-removal-timemout [LDAPCacheEntryRemovalTimeout]	Defines the duration (in hours) after which the LDAP entry is removed from the cache. The default is 0.

In addition to the above parameters, the Web interface provides the following cache-related buttons:

- LDAP Refresh Cache By Key – refreshes a saved LDAP entry response of an LDAP search key. If a request with the specified key exists in the cache, the request is resent to the LDAP server
- LDAP Clear All Cache – removes all LDAP entries in the cache

Applicable Products: Mediant 2000.

3.44.1.1.18 LDAP Query of Multiple Subtrees (DNs)

This feature provides support for performing LDAP Active Directory database queries in up to three different AD subtrees or distinguished names (DNs). This search can be done in parallel or sequentially where the search is done on the second DN if the first DN search fails.

To support this feature, the following new parameters have been added:

LDAP Search DNs [LDAPSearchDNs]	Defines up to three DNs to search in the LDAP AD database. The format of this parameter is as follows: [LdapSearchDNs] FORMAT LdapSearchDNs_Index = LdapSearchDNs_Base_Path; [\LdapSearchDNs] For example: LdapSearchDNs 0 = "OU=QA,DC=abc,DC=local"; LdapSearchDNs 1 = "OU=RD,DC=abc,DC=local"; Where the DN path is defined by ou (organizational unit) and dc (domain component) in this example..
CLI: search-dns-in-parallel [LDAPSearchDNsinParallel]	Defines the LDAP query search method in the AD database if multiple search DNs are configured (see LDAPSearchDNs). ▪ [0] Sequential ▪ [1] Parallel (Default)

Applicable Products: Mediant 2000.

3.44.1.1.19 Multiple IP Addresses for LDAP Server using FQDN

This feature provides support for using multiple IP addresses from a DNS query when the LDAP server address is configured as an FQDN. Up until this release, if an FQDN was configured, the device used only the first IP address received from the DNS query. With this feature, if there is no connection to the LDAP server or the connection to the LDAP server fails, the device attempts to connect to the LDAP server using the next IP address in the DNS query list. Note that LDAP server can also be configured with an IP address (in dotted-decimal notation) instead.

To support this feature, the following existing parameter has been modified:

Web: LDAP Server IP [LDAPServerIP]	Defines the LDAP server's address as an IP address (in dotted-decimal notation, e.g., 192.10.1.255) or as an FQDN. If an FQDN is used, the device attempts to connect to the LDAP server according to the IP address list received in the DNS query. If no connection to the LDAP server or the connection to the LDAP server fails, the device attempts to connect to the LDAP server using the next IP address in the DNS query list. The default is 0.0.0.0

Applicable Products: Mediant 2000.

3.44.1.1.20 Deriving Call IP Destination from Dial Plan File

This feature provides support for using a specified dial plan in a loaded Dial Plan file for determining the IP destination of IP calls. This enables the mapping of called numbers to dotted-decimal notation IP addresses or FQDNs (up to 15 characters).

This feature is configured by specifying the required Dial Plan index (0 to 7) of the Dial Plan file as the destination address in the IP routing tables.

- For the Gateway/IP-to-IP application (Tel-to-IP calls), the 'Destination Address' field in the Outbound IP Routing table is used to specify the Dial Plan index instead of the IP address. The entered value is a string (case-sensitive) in the format "DialPlan<index>", where "DialPlan0" denotes [PLAN1] in the Dial Plan file, "DialPlan1" denotes [PLAN2], and so on.

In the Dial Plan file, the syntax of the Dial Plan index for this feature is as follows:

```
<destination / called prefix number>,0,<IP destination>
```

The second parameter, "0" is ignored. Below shows an example of a Dial Plan for routing to an IP destination:

```
[ PLAN6 ]
200,0,10.33.8.52
201,0,10.33.8.52
300,0,itsp.com
```

Applicable Products: All.

3.44.1.1.21 Increase in Maximum Number of Coder Groups

This feature provides support for an increase in the maximum number of Coder Groups from 4 to 10 that can be configured. The Coder Groups are configured in the Coder Group Settings table.

Additional indices, CodersGroup5 through CodersGroup9 have been added to the Coder Group Settings table to support this feature:

Coder Group Settings CLI: config voip > coders-and-profiles coders-group [CodersGroup0], [CodersGroup1], [CodersGroup2], [CodersGroup3], [CodersGroup4], [CodersGroup5], [CodersGroup6], [CodersGroup7], [CodersGroup8],],[CodersGroup9]	Defines the device's coders. Up to 10 groups of coders can be defined, where each group can include up to 10 coders.

Applicable Products: Mediant 2000.

3.44.1.1.22 Proxy IP Address as Host Name in REGISTER Requests

This feature provides support for using the proxy server's IP address (in dotted-decimal notation) as the host name in SIP From and To headers in REGISTER requests.

A new parameter, 'Use Proxy IP as Host' has been added to support this feature:

Web: Use Proxy IP as Host CLI: use-proxy-ip-as-host [UseProxyIPasHost]	■ [0] Disable (default) ■ [1] Enable

If this feature is disabled and the device registers to an IP Group (i.e., proxy server), it uses the string configured by the ProxyName parameter as the host name in the REGISTER's Request-URI, and uses the string configured by the IP Group table parameter, SIPGroupName as the host name in the To and From headers. If the IP Group is configured with a Proxy Set that has several IP addresses, the REGISTER messages sent to these proxies are sent with the same host name.

Note that even if this new feature is disabled, if the ProxyName parameter is not configured, the host name in the REGISTER Request-URI is set to the proxy's IP address.

Applicable Products: All.

3.44.1.1.23 SIP Header Manipulations using Regular Expressions

This feature provides support for configuring SIP header manipulation rules using regular expressions (regex). Regex is a special text string pattern matching engine, which is used to define the condition that must exist in order to use a specific manipulation rule. If the SIP header matches the regex pattern, then the "action" of the manipulation rule is applied to the SIP message. Executing a regex pattern also creates sub-expressions. The sub-expressions are referenced using $1, $2, $3, and so on (until $13).

This feature provides the following main benefits:

- The device does not need to know the SIP header name or structure.
- The sub-expressions can be used in the manipulation action. All that is required is to set the action (for example, add, modify, etc.) and then reference the sub-expression you want to use as the value.

Applicable Products: Mediant 2000.

3.44.1.1.24 Manipulation based on Source/Destination Address of SIP Message

This feature provides support for configuring manipulating rules whose condition or action value is the source or destination address of the SIP message. The following manipulation syntax is used for this feature:

- param.message.address.src.port: source port of the message.
- param.message.address.dst.port: destination port of the message.
- param.message.address.src.ip: source ip address of the message.
- param.message.address.dst.ip: destination ip address of the message.
- param.message.address.src.transporttype: source transport type of the message.
- param.message.address.dst.transporttype: Destination transport type of the message.

Applicable Products: All.

3.44.1.1.25 Manipulation of Port and IP Address in SDP

This feature provides support for manipulating the port and IP address located in the SDP body in outgoing SIP messages. The following manipulation syntax is used to indicate the port and IP address in the SDP body:

- "sdp.port": First audio active media port number (i.e., port number greater than 0) in the "m=" field of the SDP body.
- "sdp.ip": IP address of the first active media (port greater than 0). The IP address is taken from the media "c=" field (the "c=" field below the "m=" field) of the SDP body. Note that if the "m=" field doesn't contain a "c=" field, then the IP address is taken from the global "c=" field (the "c=" field at the top of the SDP).

This manipulation capability can be used, for example, to copy the port and IP address specified in the SDP body to a customized SIP header (e.g., Custom-RTP-Address/Port) in the outgoing INVITE message, as follows:

Message Type	Action Subject	Action Type	Action Value
invite.request	header.custom-rtp-address	Add	param.message.sdp.ip
invite.request	header.custom-rtp-port	Add	param.message.sdp.port

Applicable Products: All.

3.44.1.1.26 Empty Prefix as Matching Criteria for Routing and Manipulation

This feature provides support for matching routing and/or manipulation rules for incoming IP calls that do not have a user part in the Request-URI, or for incoming Tel calls that do not have a called or calling number.

To support this feature, the dollar "$" sign is used to denote an "empty" prefix for such incoming calls. This is used in the routing and manipulation tables for the following matching criteria:

- Source and Destination Phone Prefix
- Source and Destination Username
- Source and Destination Calling Name Prefix

Applicable Products: All.

3.44.1.1.27 TLS Mutual Authentication per SIP Interface

This feature provides support for enabling TLS mutual authentication per SIP Interface. Up until this release, TLS mutual authentication could only be configured globally for all SIP calls, using the SIPSRequireClientCertificate parameter.

A new field, 'TLS Mutual Authentication' has been added to the SIP Interface table to support this feature:

Web: TLS Mutual Authentication [SIPInterface_TLSMutualAuthentication]	▪ [-1] = (Default) The SIPSRequireClientCertificate global parameter setting is applied. ▪ [0] Disable = Device does not request the client certificate for TLS connection. ▪ [1] Enable = Device requires receipt and verification of the client certificate to establish the TLS connection.

Applicable Products: Mediant 2000.

3.44.1.1.28 Re-using TCP/TLS Connections without "alias" Requirement

This feature provides support for re-using TCP (or TLS) connections without requiring the receipt of the "alias" parameter in the SIP Via header. Up until this release, TCP/TLS connection re-use was supported only if this parameter was present in the Via header of the first received INVITE message.

TCP/TLS connection re-use enables the device to use the same TCP/TLS connection for multiple SIP requests / responses for a specific SIP UA (according to RFC 5923). The benefits of this feature include less CPU and memory usage (because of fewer opened TCP connections) and reduced network congestion.

To support this feature, the following new parameter has been added:

Web: Fake TCP alias CLI: fake-tcp-alias [FakeTCPalias]	Enables the re-use of the same TCP/TLS connection for sessions with the same user, even if the "alias" parameter is not present in the SIP Via header of the first INVITE. ■ [0] Disable = (Default) TCP/TLS connection reuse is done only if the "alias" parameter is present in the Via header of the first INVITE. ■ [1] Enable Note: To enable TCP/TLS connection re-use, use the EnableTCPConnectionReuse parameter.

Applicable Products: All.

3.44.1.1.29 Same Defaults for IP / Tel Profiles and Global Parameters

This feature assigns a default value of parameters in the IP Profile and Tel Profile tables that is the same as the default value of their corresponding "global" parameter.

Applicable Products: All.

3.44.1.1.30 Increase in Maximum Number of SIP Message Manipulation Rules

This feature provides support for an increase in the maximum number of SIP message manipulation rules from 80 to 100 that can be configured in the Message Manipulation table.

Applicable Products: Mediant 2000.

3.44.1.1.31 Failed Registration Request Handling

This feature provides support for handling failed registration requests. If the device receives a second SIP 401/407 in response to a REGISTER request, with the Authentication header containing the value "stale=false", the device does not retry the registration process (i.e., does not send another REGISTER message). The "stale=false" indicates a failed username/password negotiation.

Applicable Products: All.

3.44.1.1.32 Registration Expiry Time from Original Contact

This feature provides support for obtaining the registration expiration time, upon receipt of SIP 200 OK, from the same contact as that sent in the REGISTER request. Therefore, even if the 200 OK may contain numerous contacts, only the original one will be used. If no contacts meet this condition and the Expires header is not present, the first contact will be selected.

Applicable Products: All.

3.44.1.1.33 Request Rejection if IP Address Mismatch between Via and From Header

This feature provides support for rejecting initial requests in which the top-most Via header contains an IP address that is different than the source IP address received in the From header. These requests are rejected without sending a response. An IP address mismatch is typically observed if the user agent is located behind NAT. In such network topologies, this feature would not be used.

To support this feature, the following new parameter has been added:

[VerifyRecievedVia]	Enables the device to reject initial requests in which the top-most Via header contains an IP address that is different than the source IP address received in the From header. These requests are rejected without sending a response.

	■ [0] Disable (default) = SIP request is not rejected, as this IP address mismatch indicates that the UA is behind NAT. ■ [1] Enable = SIP request is rejected.

Applicable Products: All.

3.44.1.2 SIP Gateway / IP-to-IP Features

This subsection describes the new SIP features related to the Gateway / IP-to-IP application.

> This section is applicable only to devices that support the Gateway and IP-to-IP applications.

3.44.1.2.1 V.150.1 SDP Format

This feature provides support for sending an INVITE’s SDP offer in a format according to USA Department of Defense (DoD) UCR 2008 and the ITU-T V.150.1 Annex E specification (RFC 3407) in order to negotiate V.150 modem relay using the same port as RTP, as shown below:

```
a=cdsc:1 audio udpsprt 114\r\n
a=cpar:a=sprtmap:114 v150mr/8000\r\n
a=cpar:a=fmtp:114
mr=1;mg=0;CDSCselect=1;mrmods=1,3;jmdelay=no;versn=1.1\r\n\
```

To determine the payload type for the outgoing SDP offer, a new parameter has been added (see below). This parameter enables support of "NoAudio", whereby RTP is not sent and the device adds an audio media only for the Modem Relay purpose. This is also in accordance to DOD UCR 2008 specification: "The AS-SIP signaling appliance MUST advertise the 'NoAudio' payload type to interoperate with a “Modem Relay-Preferred” endpoint that immediately transitions to the Modem Relay state without first transmitting voice information in the Audio state."

To support this feature, the following new parameter has been added:

[NoAudioPayloadType]	Determines the payload type of the outgoing SDP offer. The valid value range is 96 to 127 (dynamic payload type). The default is 0 (i.e. NoAudio is not supported). For example, if set to 120, the following is added to the INVITE SDP: `a=rtpmap:120 NoAudio/8000\r\n` Note: For incoming SDP offers, NoAudio is always supported.

Applicable Products: All.

3.44.1.2.2 Double Wink-Start Signaling and Polarity Reversal

This feature provides support for Direct Inward Dialing (DID) using additional wink-start signaling options Double-Wink Signaling and Double Polarity. These wink-signaling options are typically used for signaling between an E-911 switch and the PSAP. Up until this release, the device supported only single-wink signaling for E-911 lines.

To support this feature, the new options, [2] and [3] have been added to the existing parameter, EnableDIDWink.

Web/EMS: Enable DID Wink CLI: did-wink-enbl [EnableDIDWink]	Enables Direct Inward Dialing (DID) using Wink-Start signaling, typically used for signaling between an E-911 switch and the PSAP. ■ [0] Disable (default)

	■ [1] Single = The device can be used for connection to EIA/TIA-464B DID Loop Start lines. Both FXO (detection) and FXS (generation) are supported: • The FXO interface dials DTMF (or MF) digits upon detection of a Wink signal, instead of a dial tone. • The FXS interface generates a Wink signal upon detection of an off-hook state, instead of playing a dial tone. Example: (Wink) KP I(I) xxx-xxxx ST (Off Hook) Where: • I = one or two information digits • x = ANI Note: The FXO interface generates such MF digits when the Enable911PSAP parameter is set to 1. ■ [2] Double Wink = Double-wink signaling. The FXS interface generates the first wink upon detection of an off-hook state in the line. The second wink is generated after a user-defined interval (configured by the TimeBetweenDIDWinks parameter), after which the DTMF/MF digits are collected by the device. Digits that arrive between the first and second wink are ignored as they contain the same number. Example: (Wink) KP 911 ST (Wink) KP I(I) xxx-xxxx ST (Off Hook). ■ [3] Wink and Polarity = The FXS interface generates the first wink after it detects an off-hook state. A polarity change from normal to reversed is generated after a user-defined time (configured by the TimeBetweenDIDWinks parameter). DTMF/MF digits are collected only after this polarity change. Digits that arrive between the first wink and the polarity change are ignored as they always contain the same number. In this mode, the FXS interface does not generate a polarity change to normal if the Tel-to-IP call is answered by an IP party. Polarity reverts to normal when the call is released. Example: (Wink) KP 911 ST (Polarity) KP I(I) xxx-xxxx ST (Off Hook) Notes: ■ Options [2] and [3] are applicable only to FXS interfaces. ■ The EnableReversalPolarity and PolarityReversalType parameters must be set to [1] for FXS interfaces. ■ See also the Enable911PSAP parameter. ■ This parameter can also be configured in a Tel Profile.
[TimeBetweenDIDWinks]	Defines the interval (in msec) for wink signaling: ■ Double-wink signaling [2]: interval between the first and second wink ■ Wink and Polarity signaling [3]: interval between wink and polarity change The default value is 100 to 2000. The default is 1000. Note: See the EnableDIDWink parameter for configuring the wink signaling type.

Applicable Products: MP-1xx.

3.44.1.2.3 Increase in Maximum SIP Calling Name Manipulation Rules

This feature provides support for an increase, from 20 to 120, in the maximum number of SIP calling name manipulation rules for IP-to-Tel and Tel-to-IP calls. These rules are configured in the SIP Calling Name Manipulations IP2Tel table and SIP Calling Name Manipulations Tel2IP table, respectively.

Applicable Products: Mediant 2000.

3.44.1.2.4 Different RTP Ports for Held and New Call by FXS Endpoint

This feature provides support for using different RTP ports between the two calls involved in a three-way conference made by an FXS endpoint. In this scenario, the device establishes the first call and puts it on hold (by pressing the phone's flash-hook button) and then establishes a second call using a different RTP port. Up until this release (and when this feature is disabled), when the FXS endpoint placed the first call on hold and then made a new call, the outgoing INVITE request contained the same RTP port that was used for the first call. If the user initiated a three-way conference call, the device sent a re-INVITE to change this local port.

To support this feature, the following new parameter has been added:

Use Different RTP port After Hold CLI: use-different-rtp-port-after-hold [UseDifferentRTPportAfterHold]	Enables the use of a different RTP port when an FXS endpoint makes a new call, after the first call is put on hold, for three-way conferencing. ■ [0] Disable = First and second calls use the same RTP port in the outgoing INVITE request. If a three-way conference is then made, the device sends a re-INVITE to the held call to retrieve the call and to change the RTP port to a different port number. Example: The first call is made on port 6000 and placed on hold. The second call is made, also on port 6000. The device sends a re-INVITE to the held call to retrieve it and changes the port to 6010. ■ [1] Enable = First and second calls use different RTP ports in the outgoing INVITE request. If a three-way conference is then made, the device sends a re-INVITE to the held call to retrieve it, but the port of the held call remains unchanged. Notes: ■ When this feature is enabled and only one RTP port is available, only one call can be made by the FXS endpoint, as there is no free RTP port for a second call. ■ When this feature is enabled and you are using the Call Forking feature, every forked call is sent with a different RTP port. As the device can fork a call to up to 10 destinations, the device requires at least 10 free RTP ports.

Applicable Products: MP-1xx.

3.44.1.2.5 Interworking User-to-User Header with Text Format to UUIE IA5 Characters in Q.931 Messages

This feature provides support for interworking the SIP User-to-User header containing text format and the User-to-User information element (UUIE) with hexadecimal (IA5) characters in the Q.931 message. This feature is applicable to IP-to-Tel and Tel-to-IP calls.

To support this feature, a new optional value has been added to the existing parameter, UserToUserHeaderFormat:

[UserToUserHeaderFormat]	Defines the format of the SIP User-to-User header in INVITE messages for interworking with the ISDN User to User (UU) IE data to SIP. This applies to Tel-to-IP and IP-to-Tel calls.
	▪ [0] = (Default) Format: X-UserToUser.
	▪ [1] = Format: User-to-User with Protocol Discriminator (pd) attribute. For example:
	`User-to-User=30303734353137343136353353b313233343b3834;pd=4`
	This format is according to IETF Internet-Draft draft-johnston-sipping-cc-uui-04.
	▪ [2] = Format: User-to-User with encoding=hex at the end and pd embedded as the first byte. For example:
	`User-to-User=0430303734353137343136353353b313233343b3834; encoding=hex`
	Where "04" at the beginning of this message is the pd.
	This format is according to IETF Internet-Draft draft-johnston-sipping-cc-uui-03.
	▪ [3] = Interworks the SIP User-to-User header containing text format to ISDN UUIE in hexadecimal format, and vice versa. For example:
	SIP Header in text format:
	`User-to-User=01800213027b712a;NULL;4582166;`
	Translated to hexadecimal in the ISDN UUIE:
	`30313830303231333032376237313261 3b4e554c4c3b343538323136363b`
	The Protocol Discriminator (pd) used in UUIE is "04" (IUA characters).

Applicable Products: Mediant 2000.

3.44.1.2.6 New Format for re-INVITE for Call Hold

This feature provides support for configuring the device to send a re-INVITE for call hold with the SDP 'c=' field containing 'a=inactive' and the original IP address. The original IP address is typically the address of the party that sends the re-INVITE message.

To support this feature, a new option, [2] has been added to the existing parameter, HoldFormat:

Web/EMS: Hold Format CLI: hold-format [HoldFormat]	Determines the format of the SDP in the sent re-INVITE hold request. ▪ [0] 0.0.0.0 = (Default) The SDP "c=" field contains the IP address "0.0.0.0" and the "a=inactive" attribute. ▪ [1] Send Only = The SDP "c=" field contains the device's IP address and the "a=sendonly" attribute. ▪ [2] x.y.z.t = The SDP "c=" field contains the device's IP address and the "a=inactive" attribute. Notes: ▪ The device does not send any RTP packets when it is in hold state (for both hold formats). ▪ For digital interfaces: This parameter is applicable only to QSIG and Euro ISDN protocols.

Applicable Products: MP-1xx; Mediant 2000.

3.44.1.2.7 Disconnect IP-to-Tel Call upon Answer Machine Detection

This feature provides support for configuring the device to disconnect an IP-to-Tel call upon detection of an answering machine on the Tel side. In such a scenario, the device sends a SIP BYE message upon answering machine detection (AMD). Note that this feature does not need the receipt of an X-Detect header in the incoming INVITE to activate the AMD.

To support this feature, the following new parameters have been added:

AMD mode CLI: amd-mode [AMDmode]	Enables the device to disconnect the IP-to-Tel call upon answering machine detection (AMD). ■ [0] = (Default) Device does not disconnect call upon detection of answering machine. ■ [1] = Device disconnects call upon detection of answering machine.
IP Profile Table – AMD Mode [IpProfile_AmdMode]	Same description as above, but per IP Profile.

Applicable Products: Mediant 2000.

3.44.1.2.8 Calling Name Retrieval from AD using LDAP Query

This feature provides support for retrieving the calling name (display name) from Microsoft Active Directory (AD) for Tel-to-IP calls that are received without a calling name. The device queries the AD based on the Calling Number search key and searches for the calling name attribute configured by the new parameter, MSLDAPDisplayNameAttrName (e.g., “displayName”). The device uses the resultant calling name for the Display Name parameter in the SIP From header of the sent INVITE message.

To support this feature, the following new keywords are supported in the Calling Name Manipulation Table for Tel -> IP Calls table for the 'Prefix/Suffix to Add' fields and can be combined with other characters:

- $LDAP-PBX - starts LDAP query using MSLDAPPBXAttrName parameter as the search key
- $LDAP-MOBILE - starts LDAP query using MSLDAPMobileAttrName parameter as the search key

If the source (calling) number of the Tel-to-IP call matches the PBX / MOBILE (e.g., "telephoneNumber" and "mobile") number in the AD server, the device uses the resultant Display Name instead of the keyword(s).

For example, assume the following configuration in the Calling Name Manipulation Table for Tel -> IP Calls:

- 'Source Prefix' field is set to "4"
- 'Prefix to Add' field is set to "$LDAP-PBX Office",

If the calling number is 4046 and the resultant LDAP query display name is "John Doe", the device sends the INVITE message with the following From header:

```
From: John Doe <sip:4064@company.com>
```

To support this feature, the following new parameter has been added:

CLI: ldap-display-nm-attr [MSLDAPDisplayNameAttributeName]	Defines the attribute name that represents the Calling Name in the AD for LDAP queries based on calling number.

	The valid value is a string of up to 49 characters. The default is "displayName".

Notes:

- Calling Name Manipulation Table for Tel -> IP Calls table uses the numbers before manipulation as inputs.
- LDAP query uses the calling number after source number manipulation as the search key value.

Applicable Products: Mediant 2000.

3.44.1.2.9 Call Preemption per Trunk

This feature provides support for configuring call preemption per trunk. Call preemption modes include Multilevel Precedence and Preemption (MLPP) or Emergency (preemption of IP-to-Tel E9-1-1 emergency calls). Up until this release, call preemption could be set to MLPP or Emergency for all trunks only, using the global parameter, CallPriorityMode.

To support this feature, the following new parameter been added to the Tel Profile table:

Call Priority Mode [TelProfile_CallPriorityMode]	▪ [0] Disable (default) ▪ [1] MLPP ▪ [2] Emergency

To configure call preemption per trunk, this Tel Profile configured with call preemption (enabled or disabled) can then be assigned to specific trunks in the Trunk Group table.

Notes:

- For trunks configured with call preemption, all must be configured to [1] or all configured to [2]. In other words, the device cannot have some trunks set to [1] and some to [2].
- The global parameter must be set to the same value as that of the Tel Profile parameter; otherwise, the Tel Profile parameter will not be applied.
- If you configure call preemption using the global parameter and a new Tel Profile is subsequently added, the TelProfile_CallPriorityMode parameter automatically acquires the same setting as well.

Applicable Products: MP-11x; Mediant 2000.

3.44.1.2.10 Interworking MLPP Network Identity between ISDN and SIP

This feature provides support for automatically interworking between Multilevel Precedence and Preemption (MLPP) network identity of ISDN Q.931 and SIP messages. This feature interworks the network identity (NI) digits in the ISDN Precedence Information Element (IE) to the network domain subfield of the INVITE's Resource-Priority header, and vice versa.

The SIP Resource-Priority header contains two fields - namespace and priority. The namespace is subdivided into two subfields - network-domain and precedence-domain. Below is an example of a Resource-Priority header whose network-domain subfield is "uc", r-priority field is "priority" (2), and precedence-domain subfield is "000000":

```
Resource-Priority: uc-000000.2
```

The MLPP Q.931 Setup message contains the Precedence IE. The NI digits are presented by four nibbles found in octets 5 and 6. Up until this release, the NI digits where disregarded and the device used the value "uc" in the SIP network-domain subfield, regardless of the received NI digits.

With this feature, the device checks the NI digits according to the translation table of the Department of Defense (DoD) Unified Capabilities (UC) Requirements (UCR 2008, Changes 3) document:

NI Digits in ISDN Precedence Level IE	Network Domain in SIP Resource-Priority Header
0000	uc
0001	cuc
0002	dod
0003	nato

Notes:

- If the received NI digits in the ISDN message are not listed in the translation table, the device sets the network-domain to "uc" in the outgoing SIP message.
- If the received network-domain value in the SIP message is not listed in the translation table, the device sets the NI digits to "0000" in the outgoing ISDN message.

Applicable Products: Mediant 2000.

3.44.1.2.11 MLPP Namespace "cuc" Option for Resource-Priority Header

This feature provides support for configuring the MLPP Namespace to "cuc" in the SIP Resource-Priority header. This is used only if the received ISDN message does not contain a Precedence IE.

To support this feature, a new option, [7] 'CUC' has been added to the existing parameter, MLPPDefaultNamespace:

MLPP Default Namespace CLI: mlpp-dflt-namespace [MLPPDefaultNamespace]	Determines the namespace used for MLPP calls that are received from the ISDN side without a Precedence IE and destined for the Application server. This value is used in the Resource-Priority header of the outgoing SIP INVITE request. ■ [1] DSN (default) ■ [2] DOD ■ [3] DRSN ■ [5] UC ■ [7] CUC **Note:** If the ISDN message contains a Precedence IE, the device automatically interworks the "network identity" (NI) digits in the IE to the network domain subfield in the Resource-Priority header, as follows: Precedence IE — Resource-Priority Header 0000 — uc 0001 — cuc 0002 — dod 0003 — nato

Applicable Products: Mediant 2000.

3.44.1.2.12 User-Defined MLPP Network Domains

This feature provides support for configuring up to 32 user-defined MLPP network domain names (namespaces). This value is used in the AS-SIP Resource-Priority header of the outgoing SIP INVITE request. This feature is used in combination with the MLPPDefaultNamespace parameter (which can be set to 'DSN', 'DOD', 'DRSN', 'UC', or 'CUC' network domains) or "point" to a user-defined network domain configured using the new parameter table, ResourcePriorityNetworkDomains:

[ResourcePriorityNetworkDomains]	Defines MLPP network domain names.
	The domain name is a string that can contain up to 10 characters.
	FORMAT ResourcePriorityNetworkDomains_Index = ResourcePriorityNetworkDomains_Name;
	ResourcePriorityNetworkDomains 1 = dsn;
	ResourcePriorityNetworkDomains 2 = dod;
	ResourcePriorityNetworkDomains 3 = drsn;
	ResourcePriorityNetworkDomains 5 = uc;
	ResourcePriorityNetworkDomains 7 = cuc;
	[\ResourcePriorityNetworkDomains]
	■ **Notes:**
	■ Indices 1, 2, 3, 5, and 7 cannot be modified and are defined for DSN, DOD, DRSN, UC, and CUC, respectively.
	■ If the MLPPDefaultNamespace parameter is set to -1, interworking from PSTN NI digits is done automatically.

Applicable Products: Mediant 2000.

3.44.1.2.13 SIP Resource-Priority Header to ISDN PRI Mapping in MLPP

This feature provides support for mapping the Resource-Priority field of the SIP Resource-Priority header to the ISDN PRI Precedence Level (priority level) field, for the MLPP application (typically implemented by the USA DoD). By default, this feature does the translation as follows:

- If the network-domain field in the Resource-Priority header is "uc", then the device sets the Precedence Level field in the ISDN PRI Precedence Level IE according to Table 5.3.2.12-4 (Mapping of RPH r-priority Field to PRI Precedence Level Value):

MLPP Precedence Level	PRI Precedence Level	SIP Resource-Priority Header Field
Routine	4	0
Priority	3	2
Immediate	2	4
Flash	1	6
Flash Override	0	8

- If the network-domain field in the Resource-Priority header is any value other than "uc", then the device sets the Precedence Level field to "0 1 0 0" (i.e., "routine").

Up until this release, the priority level translation was done only for RPNDs configured in the ResourcePriorityNetworkDomains table. For all other RPNDs, the priority level was automatically set to "routine".

To support this feature, a new field, EnableIp2TelInterworking has been added to the ResourcePriorityNetworkDomains table. By default, this field is enabled only for the "uc" entry.

[ResourcePriorityNetworkDomains]	Defines MLPP network domain names. The domain name is a string that can contain up to 10 characters. FORMAT ResourcePriorityNetworkDomains_Index = ResourcePriorityNetworkDomains_Name,

	ResourcePriorityNetworkDomains_EnableIp2TelInterworking ; ResourcePriorityNetworkDomains 1 = dsn, 0; ResourcePriorityNetworkDomains 2 = dod, 0; ResourcePriorityNetworkDomains 3 = drsn, 0; ResourcePriorityNetworkDomains 5 = uc, 1; ResourcePriorityNetworkDomains 7 = cuc, 0; [\ResourcePriorityNetworkDomains] ■ **Notes:** ■ Indices 1, 2, 3, 5, and 7 cannot be modified and are defined for DSN, DOD, DRSN, UC, and CUC, respectively. ■ If the MLPPDefaultNamespace parameter is set to -1, interworking from PSTN NI digits is done automatically.

Applicable Products: Mediant 2000.

3.44.1.2.14 Call Routing and Manipulation based on Location of Emergency Calls in Lync

This feature provides support for routing or SIP header / number manipulation of emergency calls made from Microsoft® Lync™ Server 2010 clients, based on the geographical location of the caller.

To enable this feature, the device supports manipulation of the original destination number (i.e., 911) received from E-911 remote branch callers to the destination number of an emergency provider relevant to the geographical area in which the remote branch office is located. The device identifies these callers by their ELIN numbers, contained in the PIDF-LO XML body of the received SIP INVITE message. The ELIN number is associated with the precise location (e.g., civic address and building floor level) of the E-911 caller.

To configure such manipulation, the ELIN number is used as the source prefix in the Destination Phone Number Manipulation Table for Tel -> IP Calls table. To identify this source prefix as belonging to E-911 ELIN numbers, the "ELIN" string is used and added as a prefix to the number, for example, "ELIN1234567890". For example, assume an E-9-1-1 call is received for destination 911@company.com and the ELIN number is 1234567890; to create the new destination, 15509115000@company.com, the destination number can be manipulated using the manipulation table by adding prefix 1550 and suffix 5000.

To enable this feature, a new option, [2] has been added to the existing E911Gateway parameter:

[E911Gateway]	Enables Enhanced 9-1-1 support for ELIN handling in the Microsoft Lync Server 2010 environment. ■ [0] = Disable (default) ■ [1] = Enable ■ [2] = Location based manipulations

Applicable Products: Mediant 2000.

3.44.1.2.15 Rejecting Emergency INVITE Messages with SIP 503 Response

This feature provides support for issuing a SIP 503 response code when it rejects incoming INVITE messages whose Priority headers are set to "emergency". The device rejects this message with a SIP 503 response, regardless of the rejection reason.

When a Lync 2010 client makes an emergency call, the call is routed through the Microsoft Mediation Server to the ELIN Gateway, which forwards it to the PSTN. In some scenarios, the call may not be established due to either the PSTN (for example, the destination is busy or not found) or ELIN Gateway (for example, lack of resources or an internal error). In such cases, the Mediation Server requires that the ELIN Gateway "reject" the call with the SIP release cause code 503 "Service

Unavailable" instead of the designated release call. Such a release cause code enables the Mediation Server to issue a failover to another entity (for example, another ELIN Gateway), instead of retrying the call or returning the release call to the user.

To support this feature, the following new parameter has been added:

Emergency Special Release Cause CLI: emrg-spcl-rel-cse [EmergencySpecialReleaseCause]	■ [0] Disable = (Default) The original release cause is sent ■ [1] Enable = SIP 503 response is sent

Applicable Products: Mediant 2000.

3.44.1.2.16 Re-routing Tel-to-IP Calls to Fax Destinations

This feature provides support for re-routing Tel-to-IP calls that are identified as fax calls. The re-routing can be delayed until a fax CNG tone is detected or until a user-defined timeout expires. Once detected as a fax call, the device re-routes the call to a specific destination (IP Group or a fax server) according to the matching rules configured in the Outbound IP Routing table.

To support this feature, the following new parameters have been added:

[FaxReroutingMode]	Determines the re-routing of Tel-to-IP calls that are identified as fax calls. If a CNG tone is detected on the Tel side of a Tel-to-IP call, the prefix string "FAX" is appended to the destination number before routing and manipulation. A value of "FAX" entered as the destination number in the Outbound IP Routing table is then used to route the call, and the destination number manipulation mechanism is used to remove the "FAX" prefix, if required. Note that the "FAX" prefix string in routing and manipulation tables is case-sensitive. If the initial INVITE used to establish the voice call (not fax) was already sent, a CANCEL (if not connected yet) or a BYE (if already connected) is sent to release the voice call. ■ [0] Disable (default) ■ [1] Rerouting without Delay ■ [2] Progress and Delay = Incoming ISDN calls are delayed until a CNG tone detection or timeout, set by the FaxReroutingDelay parameter. If the EnableComfortTone parameter is set to 1, a Q.931 Progress message with Protocol Discriminator set to 1 is sent to the PSTN and a comfort tone is played accordingly to the PSTN. When the timeout expires, the device sends an INVITE to a specific IP Group or to a fax server, according to the Outbound IP Routing table rules. This option is applicable only to ISDN. ■ [3] Connect and Delay = Incoming ISDN calls are delayed until a CNG tone detection or timeout, set by the FaxReroutingDelay parameter. A Q.931 Connect message is sent to the PSTN. If the EnableComfortTone parameter is set to 1, a comfort tone is played to the PSTN. When the timeout expires, the device sends an INVITE to a specific IP Group or to a fax server according to the Outbound IP Routing table rules. This option is applicable only to ISDN. **Note:** This parameter replaces the EnableFaxRerouting parameter. For backward compatibility, the EnableFaxRerouting parameter set to 1 is equivalent to the FaxReroutingMode parameter set to 1.

[FaxReroutingDelay]	Defines the maximum time interval (in seconds) that the device waits for CNG detection before re-routing calls identified as fax calls to fax destinations (terminating fax machine). The valid value range is 1-10. The default is 5.

Applicable Products: Mediant 2000.

3.44.1.2.17 T.38 Fax Relay upon re-INVITE with T.38 and Audio in SDP

This feature provides support for enabling the device to activate T.38 fax relay upon receipt of a re-INVITE with T.38 and audio media in the SDP. Up until this release, fax relay was activated upon receipt of a re-INVITE with only T.38 in the SDP. This is used for fax machines (connected to the device) located behind NAT. To enable fax transmission from the WAN, the device opens pinholes in the NAT by sending No-Op ("no-signal") packets upon activation of the fax relay.

To support this feature, a new option, [2] Immediate Start on Fax and Voice has been added to the existing 'T38 Fax Session Immediate Start' parameter:

T38 Fax Session Immediate Start CLI: t38-sess-imm-strt [T38FaxSessionImmediateStart]	Enables fax transmission of T.38 "no-signal" packets to the terminating fax machine. ■ [0] Disable (default) ■ [1] Immediate Start on Fax ■ [2] Immediate Start on Fax and Voice This is used for transmission from fax machines (connected to the device) located inside a NAT. Generally, the firewall blocks T.38 (and other) packets received from the WAN, unless the device behind NAT sends at least one IP packet from the LAN to the WAN through the firewall. If the firewall blocks T.38 packets sent from the termination IP fax, the fax fails. To overcome this, the device sends No-Op ("no-signal") packets to open a pinhole in the NAT for the answering fax machine. The originating fax does not wait for an answer, but immediately starts sending T.38 packets to the terminating fax machine. **Note:** To enable No-Op packet transmission, use the NoOpEnable and NoOpInterval parameters.

Applicable Products: MP-11x; Mediant 2000.

3.44.1.2.18 Call Detail Records for IP-to-IP Application

This feature provides unique Call Detail Records (CDR) for calls pertaining to the IP-to-IP application. For these calls, the device sends CDRs with the *EPTyp* field set to "IP2IP". The CDR also contains a unique Session ID for each IP-to-IP call session (i.e., both legs of the call). This Session ID is displayed in the *SessionId* CDR field.

Applicable Products: Mediant 2000.

3.44.1.2.19 SIP 183 for Early Media of IP-to-IP Calls

This feature provides support for sending a SIP 183 with SDP response immediately upon receipt of an INVITE request for IP-to-IP calls. This feature is useful when interworking with SIP servers that require a stream of early media to keep sessions open (i.e., when a 180 response is insufficient to keep sessions open). Up until this release, this feature was applicable only to the Gateway application (i.e., ISDN interfaces).

This feature can also be configured per IP Profile, thereby allowing early media to be configured for specific calls.

To support this feature, the following existing parameter is used:

Enable Early 183 CLI: early-183 [EnableEarly183]	Enables the device to send SIP 183 responses with SDP to the IP side immediately upon receipt of INVITE messages (for IP-to-Tel and IP-to-IP calls). ■ [0] Disable (default) ■ [1] Enable • For IP-to-Tel calls: By sending the 183 response, the device opens an RTP channel before receiving the "progress" tone from the ISDN side. The device sends RTP packets immediately upon receipt of an ISDN Progress, Alerting with Progress indicator, or Connect message according to the initial negotiation without sending the 183 response again, thereby saving response time. Therefore, this avoids early media clipping. • For IP-to-IP calls: Sending the 183 response enables SIP servers requiring a stream of early media to keep sessions open. **Note:** To enable this feature, set the EnableEarlyMedia parameter to 1.
Enable Early 183 [IpProfile_EnableEarly183]	The description is the same as that of the global parameter above.

Applicable Products: Mediant 2000.

3.44.1.2.20 Manipulation of SIP REGISTER Messages

This feature provides support for manipulating REGISTER messages for the Gateway/IP-to-IP applications. This feature is applicable only for outbound manipulation of REGISTER messages. Up until this release, manipulation was supported only for INVITE messages. SIP message manipulation is configured in the existing Message Manipulations table.

Applicable Products: Mediant 2000.

3.44.1.2.21 Host Name as Match Criteria for Number Manipulation Rules

This feature provides enhanced support for number manipulation of IP-to-Tel calls. This feature enables the use of the source and/or destination host name prefix as criteria for matching incoming SIP INVITE messages to a desired manipulation rule. This feature is supported in the following IP-to-Tel manipulation tables:

- Destination Phone Number Manipulation Table for IP > Tel Calls
- Source Phone Number Manipulation Table for IP > Tel Calls
- Redirect Number IP > Tel
- Calling Name Manipulations IP2Tel

Two new fields have been added to these manipulation tables to support this feature:

- 'Source Host Prefix'
- 'Destination Host Prefix'

The source host part of the incoming SIP dialog is typically located in the From URI, and the destination host part is typically located in the Request-URI.

Applicable Products: MP-11x; Mediant 2000.

3.44.1.2.22 Destination Number Manipulation Rules per Destination IP Group

This feature provides support for configuring destination phone number manipulation rules per destination IP Group, for Tel-to-IP and IP-to-IP calls. For example, if a Tel-to-IP call is routed to a specific IP Group (according to the Outbound IP Routing table) a specific Tel-to-IP number manipulation rule can be assigned to this IP Group.

To support this feature, a new field, 'Destination IP Group ID' (DestIPGroupID) has been added to the Destination Phone Number Manipulation Table for Tel > IP Calls (NumberMapTel2IP) table to specify the destination IP Group to which the manipulation rule is applied.

Applicable Products: MP-11x; Mediant 2000.

3.44.1.2.23 Increase in Number of Destination Number Manipulation Rules

This feature provides support for an increase in the maximum number of destination number manipulation rules that can be configured. This applies to the following tables:

- Destination Phone Number Manipulation Table for Tel-to-IP Calls (NumberMapTel2IP ini file parameter) - up to 120 entries
- Destination Phone Number Manipulation Table for IP-to-Tel Calls (NumberMapIP2Tel ini file parameter) - up to 120 entries

Applicable Products: MP-11x; Mediant 2000.

3.44.1.2.24 Forcing Device to Send Local Date / Time to PBX

This feature provides support for always sending the device's local date and time (obtained from its internal clock) to PBXs in ISDN Q.931 Connect messages (Date / Time Information Element). This is done regardless of whether or not the incoming SIP 200 OK contains the Date header. If the SIP 200 OK includes the Date header, the device ignores its values.

To support this feature, a new option, [2] 'Always Send Local Date and Time' has been added to the following parameter:

Send Local Time To ISDN Connect [SendLocalTimeToISDNConnect]	Determines the device's handling of the date and time sent in the ISDN Connect message (Date / Time Information Element) upon receipt of SIP 200 OK messages. This feature is applicable only to Tel-to-IP calls. ▪ [0] Disable = (Default) If the SIP 200 OK includes the Date header, the device sends its value in the ISDN Connect Date / Time IE. If the 200 OK does not include this header, it does not add the Date / Time IE to the sent ISDN Connect message. ▪ [1] Enable = If the SIP 200 OK includes the Date header, the device sends its value (i.e. date and time) in the ISDN Connect Date / Time IE. If the 200 OK does not include this header, the device uses its internal, local date and time for the Date / Time IE, which it adds to the sent ISDN Connect message. ▪ [2] Always Send Local Date and Time = Device always sends its local date and time (obtained from its internal clock) to PBXs in ISDN Q.931 Connect messages (Date / Time IE). This is regardless of whether or not the incoming SIP 200 OK includes the Date header. If the SIP 200 OK includes the Date header, the device ignores its value. **Notes:** ▪ This feature is applicable only to Tel-to-IP calls.

	■ For IP-to-Tel calls, only if the incoming ISDN Connect message includes the Date / Time IE does the device add the Date header to the sent SIP 200 OK message.

Applicable Products: Mediant 2000.

3.44.1.2.25 Routing SIP Calls to Specific E1/T1 Trunks

This feature provides support for routing incoming SIP calls to specific E1/T1 trunks. Up until this release, IP calls could be routed only to specified Trunk Groups. The specified trunk can belong to a Trunk Group that is also used in other IP-to-Tel routing rules.

To support this feature, a new field, 'Trunk ID' has been added to the Inbound IP Routing table:

Inbound IP Routing Table [PstnPrefix]	Defines the IP-to-PSTN routing rules. [PstnPrefix] FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, PstnPrefix_TrunkGroupId, PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId, PstnPrefix_SrcIPGroupID, PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix, PstnPrefix_TrunkId; [/PstnPrefix] **Notes:** ■ If both 'Trunk Group ID' and 'Trunk ID' fields are configured in the table, the routing is done according to the Trunk Group ID field. ■ The method for selecting the trunk's channel to which the IP call is sent is configured by the global parameter, ChannelSelectMode.

Applicable Products: Mediant 2000.

3.44.1.2.26 Euro ISDN and QSIG to SIP Redirected Number Manipulation

This feature provides support for using special strings to manipulate the Diverted-to and Diverting numbers received in the incoming Call Redirection Facility message, which is interworked to outgoing SIP 302 response. This is applicable for IP-to-Tel calls.

The incoming redirection Facility message includes, among other parameters, the Diverted-to number and Diverting number. The Diverted-to number (i.e., the new destination) is mapped to the user part in the Contact header of the SIP 302 response. The Diverting number is mapped to the user part in the Diversion header of the SIP 302 response.

This feature enables the manipulation of these two numbers, using the existing Redirect Number Tel -> IP manipulation table. To support this, the following special strings can now be used in this table using the 'Destination prefix' field:

- "RN" - used in the rule to manipulate the Redirected number (i.e., originally called number or Diverted-to number).
- "DN" - used in the rule to manipulate the Diverted-to number (i.e., the new called number or destination). This manipulation is done on the user part in the Contact header of the SIP 302 response.

For example, assume the following required manipulation:

- Manipulate Redirected number 6001 (originally called number) to 6005
- Manipulate Diverted-to number 8002 (the new called number or destination) to 8005

The configuration in the Redirect Number Tel -> IP manipulation table is as follows:

Parameter	Rule 1	Rule 2
Destination Prefix	RN	DN
Redirect Prefix	6	8
Stripped Digits From Right	1	1
Suffix to Add	5	5
Number of Digits to Leave	5	-

After the above manipulation is done, the device sends the following outgoing SIP 302 response:

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/TLS 10.33.45.68;branch=z9hG4bKac54132643;alias
From: "MP118 1" <sip:8001@10.33.45.68>;tag=1c54119560
To: <sip:6001@10.33.45.69;user=phone>;tag=1c664560944
Call-ID: 541189832710201115142@10.33.45.68
CSeq: 1 INVITE
Contact: <sip:8005@10.33.45.68;user=phone>
Supported: em,timer,replaces,path,early-session,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
Diversion: <tel:6005>;reason=unknown;counter=1
Server: Audiocodes-Sip-Gateway-IPmedia 260_UN/v.6.20A.043.001
Reason: SIP ;cause=302 ;text="302 Moved Temporarily"
Content-Length: 0
```

Applicable Products: Mediant 2000.

3.44.1.2.27 IP-to-Tel Routing based on Source SRD

This feature provides support for routing received SIP INVITE messages to specific Trunk Groups, based on source SRD from which the INVITE arrived.

To support this feature, a new field, 'Source SRD ID' has been added to the Inbound IP Routing Table:

Inbound IP Routing Table [PstnPrefix]	Defines the IP-to-PSTN routing rules. [PstnPrefix] FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, PstnPrefix_TrunkGroupId, PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId, PstnPrefix_SrcIPGroupID, PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix, PstnPrefix_TrunkId, PstnPrefix_SrcSRDID; [/PstnPrefix] **Note:** When the incoming INVITE matches the SRD in the routing rule, if the Source IP Group ID is defined and its SRD is different, the incoming SIP call is rejected. If the Source IP Group ID is not defined, the SRD's default IP Group is used. If there is no valid source IP Group, the call is rejected.

Applicable Products: Mediant 2000.

3.44.1.2.28 Interworking User Information from REFER to Q.931 Setup

This feature provides support for interworking user-to-user information (UUI) received in incoming SIP REFER messages to User-to-User information element (IE) in ISDN Q.931 Setup messages. Up until this release, the following SIP-to-ISDN UUI interworking was supported:

- INVITE to Setup
- 200 OK to Connect
- INFO to User Information
- 18x to Alerting
- BYE to Disconnect

To support this feature, the existing parameter, 'Enable User-to-User IE for IP to Tel' is used:

Enable User-to-User IE for IP to Tel CLI: uui-ie-for-ip2tel [EnableUUIIP2Tel]	Enables interworking of SIP user-to-user information (UUI) to User-to-User IE in ISDN Q.931 messages. ■ [0] Disable (default) = Received UUI is not sent in ISDN message. ■ [1] Enable = Device interworks UUI from SIP to ISDN. The device supports the following SIP-to-ISDN interworking of UUI: • SIP INVITE to Q.931 Setup • SIP REFER to Q.931 Setup • SIP 200 OK to Q.931 Connect • SIP INFO to Q.931 User Information • SIP 18x to Q.931 Alerting • SIP BYE to Q.931 Disconnect Notes: ■ The interworking of ISDN User-to-User IE to SIP INFO is applicable only to the Euro ISDN, QSIG, and 4ESS PRI variants. ■ To interwork the UUIE header from SIP-to-ISDN messages with the 4ESS ISDN variant, the ISDNGeneralCCBehavior parameter must be set to 16384.

Applicable Products: Mediant 2000.

3.44.1.2.29 Special Dial Tone to FXS Phones when Call Forward Activated

This feature provides support for playing a special dial tone to FXS phones that are activated with call forwarding. This special tone is a stutter dial tone (Tone Type = 15) as defined in the CPT file and is played whenever the phone goes off-hook.

The special dial tone is used as a result of the device receiving a SIP NOTIFY message from a third-party softswitch providing the call forwarding service with the following SIP Alert-Info header:

```
Alert-Info: <http://127.0.0.1/Tono-Espec-Invitacion>;lpi-
aviso=Desvio-Inmediato
```

The FXS phone user, connected to the device, activates the call forwarding service by dialing a special number (e.g., *21*xxxxx) and as a result, the device sends a regular SIP INVITE message to the softswitch. The softswitch later notifies of the activation of the forwarding service by sending an unsolicited NOTIFY message with the Alert-Info header, as mentioned above.

When the call forwarding service is de-activated, for example, by dialing #21# and sending an INVITE with this number, the softswitch sends another SIP NOTIFY message with the following Alert-Info header:

```
Alert-Info: <http://127.0.0.1/ Tono-Normal-Invitacion>; Aviso =
Desvió-Inmediato
```

From this point on, the device plays a normal dial tone to the FXS phone when it goes off-hook.

Applicable Products: MP-1xx.

3.44.1.2.30 Denial of Collect Calls per Tel Profile

This feature provides support for configuring the Denial of Collect Calls feature per Tel Profile and thereby enabling this feature for specific calls. Denial of Collect Calls rejects (or disconnects) incoming Tel (FXO) to IP collect calls and signals this denial to the PSTN. Up until this release, it could only be enabled for all calls or per FXO port, using the global parameter, EnableFXODoubleAnswer.

A new field, TelProfile_EnableFXODoubleAnswer has been added to the Tel Profile table to support this feature.

This feature also provides support for Denial of Collect Calls when automatic dialing is enabled. The FXO line does not answer the incoming call (ringing) until a SIP 200 OK is received from the remote destination. When a 200 OK is received, a double answer is sent from the FXO line.

Applicable Products: MP-11x.

3.44.1.2.31 Configurable Name for Trunk Group

This feature provides support for configuring a name for each Trunk Group. This name is used to represent the Trunk Group in the *tgrp* parameter of sent SIP INVITE messages (according to RFC 4904), instead of using the Trunk Group decimal number.

For example:

```
sip:+16305550100;tgrp=TG-1;trunk-context=+1-
630@isp.example.net;user=phone
```

To support this feature, a new field, 'Trunk Group Name' has been added to the Trunk Group Settings table:

Trunk Group Name [TrunkGroupSettings_TrunkGroupName]	Defines a name for the Trunk Group. The valid value can be a string of up to 20 characters. By default, no name is configured. Note: If this parameter is not configured, the Trunk Group decimal number is used instead in the SIP *tgrp* parameter.

This feature is enabled by any of the following existing parameters:

- UseSIPtgrp
- UseBroadsoftDTG

Applicable Products: MP-11x; Mediant 2000.

3.44.1.2.32 Connected Number Subaddress Added to Connect Message

This feature provides support for adding the connected number subaddress to the ISDN Q.931 Connect message (i.e. the message sent when a call is answered). This feature is supported only for E1 EURO ISDN, QSIG, and NTT protocols. The subaddress may be an additional information in a phone number for identifying extensions (i.e., the same number may have several extensions). This feature also supports the mapping of the 'isub' parameter value contained in the SIP P-Asserted-Identity header (RFC 4715) of the received 200 OK response to the connected number subaddress in the Q.931 Connect message. To support the P-Asserted-Identity header (which contains the 'isub' parameter), the ini file parameter, AssertedIdMode must be set to 1.

Applicable Products: Mediant 2000.

3.44.1.2.33 Minimum Call Duration for Disconnecting PSTN Calls

This feature provides support for keeping the PSTN call open for a user-defined duration (in seconds) if the established call was terminated before this duration expired. If the IP side terminates the call before this designated timeout, the device terminates the call towards the IP side, but delays the termination towards the PSTN side until the user-defined timeout expires. This feature is applicable to IP-to-Tel and Tel-to-IP calls, and for ISDN and CAS protocols.

For example: assume the minimum call duration is set to 10 seconds and an IP phone hangs up a call that it had with a BRI phone after 2 seconds. As the call duration is below that of the configured minimum duration, the device does not disconnect the call from the Tel side. It sends a 200 OK immediately upon receipt of the BYE to disconnect from the IP phone. The call is disconnected from the Tel side only when the current call duration is greater than or equals the configured minimum call duration.

To support this feature, the following new parameter has been added:

CLI: configure voip > sip advanced-settings > set mn-call-duration [MinCallDuration]	Defines the minimum call duration. The valid value range is 0 to 10 seconds, where 0 (default) disables the feature.

Applicable Products: Mediant 2000.

3.44.1.2.34 Increased Timeout for Call Disconnect upon LOS / LOF

This feature provides support for configuring longer timeout duration - from 80 to 3,600 seconds - activated once an E1/T1 trunk "Red" (LOS / LOF) alarm is raised. If this timeout expires and the alarm is still raised, the device disconnects the SIP call by sending a SIP BYE message. If the alarm is cleared before this timeout elapses, the call is not terminated and continues as normal.

To support this feature, the existing parameter, TrunkAlarmCallDisconnectTimeout is used.

Applicable Products: Mediant 2000.

3.44.1.2.35 Interworking SIP REFER Messages for IP-to-IP Application

This feature provides support for interworking incoming mid-call SIP REFER messages to outgoing REFER messages. This is supported for blind and consultation call transfers.

Up until this release, if the IP-to-IP application received a SIP REFER message, it sent an INVITE to the refer-to destination with or without the Replaces header. This new feature forwards REFER and all relevant SIP messages from / to the transferor through the IP-to-IP application during call transfer. In addition, for consultation transfer, the REFER message contains a 'replaces' parameter in the Refer-To header. In this case, the outgoing REFER also contains a 'replaces' parameter in the Refer-To header.

To support this feature, the following new parameter has been added:

Web: IP2IP Transfer Mode CLI: ip2ip-transfer-mode [IP2IPTransfermode]	Determines the interworking of SIP REFER messages for calls pertaining to the IP-to-IP application. ■ [0] Refer Termination = (Default) Device sends an INVITE to the "refer-to" destination with or without the Replaces header. ■ [1] Refer Interworking = Device sends the REFER and all relevant SIP messages from / to the transferor, to the target destination.

Applicable Products: Mediant 2000.

3.44.1.2.36 New Behavior for Hook-Flash Key Sequence "Flash + 1"

This feature provides support for a new hook-flash key sequence "Flash + 1" behavior for FXS interfaces. This hook-flash key sequence does the following:

- When the device handles two calls (an active and a held call) and "Flash+1" is dialed, it sends a SIP BYE message to the active call and the previously held call becomes the active call.
- When there is an active call and there is an incoming waiting call, if "Flash+1" is dialed, the active call is disconnected and the waiting call is received.

To support this feature, the existing parameter, FlashKeysSequenceStyle set to [2] is used:

Flash Keys Sequence Style CLI: flash-key-seq-style [FlashKeysSequenceStyle]	Determines the hook-flash key sequence for FXS interfaces. ■ [0] 0 = Flash hook (default) - only the phone's Flash button is used, according to the following scenarios: • During an existing call, if the user presses the Flash button, the call is put on hold; a dial tone is heard and the user is able to initiate a second call. Once the second call is established, on-hooking transfers the first (held) call to the second call. • During an existing call, if a call comes in (call waiting), pressing the Flash button places the active call on hold and answers the waiting call; pressing Flash again toggles between these two calls. ■ [1] 1 = Sequence of Flash hook and digit: • Flash + 1: holds a call or toggles between two existing calls • Flash + 2: makes a call transfer. • Flash + 3: makes a three-way conference call (if the Three-Way Conference feature is enabled, i.e., the parameter Enable3WayConference is set to 1 and the parameter 3WayConferenceMode is set to 2). ■ [2] 2 = Sequence of Flash Hook and digit: • Flash Hook only: places a call on hold. • **Flash + 1:** see Feature Description above. • Flash + 2: places a call on hold and answers a call-waiting call, or toggles between active and on-hold calls. • Flash + 3: makes a three-way conference call (if the Enable3WayConference parameter is set to 1 and the 3WayConferenceMode parameter is set to 2, and the device houses the MPM modules). Note that the settings of the ConferenceCode parameter are ignored. • Flash + 4: makes a call transfer.

Applicable Products: MP-1xx.

3.44.1.2.37 SIP re-INVITE with "a=sendonly" Handled as "a=inactive"

This feature provides support for enabling the device to handle re-INVITE messages received with the "a=sendonly" attribute in the SDP, in the same way as if an "a=inactive" was received in the SDP. When enabled, the device plays a held tone to the Tel phone and responds with a 200 OK containing the "a=recvonly" attribute in the SDP.

To support this feature, the following new parameter has been added:

SIP Hold Behavior [SIPHoldBehavior]	■ [0] Disable (default) ■ [1] Enable

Applicable Products: MP-1xx.

3.44.1.2.38 Early Answer Timeout per Call

This feature provides support for configuring Early Answer Timeout per specific calls. This is done by configuring Early Answer Timeout for an IP Profile.

To support this feature, the global parameter, EarlyAnswerTimeout has now been added to the IP Profile table:

[IPProfile_EarlyAnswerTimeout]	Defines the duration (in seconds) that the device waits for an ISDN Connect message from the called party (Tel side), started from when it sends a Setup message. If this timer expires, the call is answered by sending a SIP 200 OK message (to the IP side). The valid range is 0 to 2400. The default is 0 (i.e., disabled).

Applicable Products: Mediant 2000.

3.44.1.2.39 Coder Negotiation Priority between Local or Remote Coder List

This feature provides support for assigning a higher priority to the device's coder list when negotiating the coder in the incoming SDP offer with the remote User Agent (UA). Up until this release, the priority of coder negotiation was according to the remote UA's coder list offer.

To support this feature, the following new parameter has been added:

Coder Priority Negotiation [CoderPriorityNegotiation]	Defines the priority for coder negotiation in the incoming SDP offer, between the device's or remote UA's coder list. ■ [0] = (Default) Coder negotiation is given higher priority to the remote UA's list of supported coders. ■ [1] = Coder negotiation is given higher priority to the device's (local) supported coders list.

Applicable Products: MP-1xx; Mediant 2000.

3.44.1.2.40 Re-Negotiation of Coders in re-INVITE for Unheld Calls

This feature provides support for re-negotiating the coder for a call that was previously put on-hold and which is now made un-hold. Up until this release, the device used the same coder as was negotiated before the call was put on-hold, for the call when made un-hold. Now, in the re-INVITE for retrieving the on-hold call, all the supported coders are sent in the SDP negotiation with the call in order to re-negotiate the coder to use. This feature is useful, for example, where party B, established with party A using G.711 coder is put on-hold, transferred to party C who uses G.729 coder, and then made un-hold. In such a scenario and without this feature support, the call would fail due to incompatible coders. Implementing this new feature, party B re-negotiates the coder support with party C.

To support this feature, the following new parameter has been added:

Send All Coders on Retrieve CLI: send-all-cdrs-on-rtrv [SendAllCodersOnRetrieve]	Defines coder negotiation in the re-INVITE for retrieving on-hold calls. ■ [0] Disable = (Default) Sends only initially chosen coder from when call was first established, in the re-INVITE. ■ [1] Enable = Sends all supported coders in the SDP of the re-INVITE for re-negotiating the coder.

Applicable Products: MP-1xx; Mediant 2000.

3.44.1.2.41 Performance Monitoring for All Trunks Busy (ATB)

This feature provides support for performance monitoring of busy Trunk Groups. This feature may be useful, for example, to regulators who wish to ensure availability of channels for urgent calls (such as emergency calls) and to verify that at no time all trunks toward a specific connection are busy. If channel availability is limited, the customer may resolve this by, for example, increasing the number of channels and/or trunks in the Trunk Group.

This feature is supported by the addition of the following new SNMP MIBs:

- **gwTrunkGroupUtilization (Trunk Group Utilization):** Indicates the number of channels that are currently in use (busy) per Trunk Group. The device also supports the configuration (SNMP) of a busy channel threshold per Trunk Group, which when exceeded, sends an alarm. For example, if the device has 240 channels and the threshold is set to 106, if the number of concurrent busy channels exceeds 106, this threshold alarm is sent. Note that if a trunk is in LOF state, this MIB counts only the channels that are used.
- **gwTrunkGroupAllTrunksBusy (All Trunks Busy):** This MIB counts the total duration (in seconds) for which all channels of a specific Trunk Group were concurrently busy during each performance monitoring collection time interval (typically, 15 minutes). Note that trunks that are out of service or not configured (set to NONE) are considered "busy" in this calculation. For example, if Trunk Group ID #3 has 200 channels and all these were concurrently busy for 60 seconds, then the All Trunks Busy MIB will display "60" for this Trunk Group. At the time when all trunks are in busy state, the Trunk Group Utilization MIB will display "200".

To support this feature:

- A Trunk Group must be configured for the trunks, which is done in the Trunk Group Settings table.
- The ID number of the Trunk Group must be set to the same number as the table row index in which the Trunk Group is configured. For example, Trunk Group ID #17 must be configured in table row index 17.
- The Trunk Group must be set to any ID number between 1 and 19 (inclusive) only.

Note: Disabled trunks are not considered busy trunks and thus, are ignored in the calculation of these performance monitoring MIBs.

Applicable Products: Mediant 2000.

3.44.1.2.42 ISO 8859 Character Set Type

This feature provides support for configuring the ISO 8859 character set type (languages) for representing the alphanumeric string of the calling name (caller ID) in the forwarded message, for IP-to-Tel and Tel-to-IP calls.

To support this feature, the following new parameter has been added:

CLI: iso8859-charset [ISO8859CharacterSet]	Defines the ISO 8859 character set type (languages) for representing the alphanumeric string of the calling name (caller ID) in the forwarded message, for IP-to-Tel and Tel-to-IP calls. ■ [0] No Accented = Proprietary method where incoming INVITE messages with any accented characters (e.g., á, é, í, ó, and ü), which are represented in a 2-byte unicode character, are translated to Latin-only, which are normal one-byte ASCII characters (a, e, i, o, and u, respectively). ■ [1] Western European (Default) ■ [2] Central European ■ [3] South European ■ [4] North European

	■ [5] Cyrillic ■ [6] Arabic ■ [7] Hebrew ■ [8] Turkish

Applicable Products: Mediant 2000.

3.44.1.3 SIP Stand-Alone Survivability (SAS) Features

This subsection describes the new SIP Stand-Alone Survivability (SAS) application features.

3.44.1.3.1 SAS Emergency upon OPTIONS Only Response Failure

This feature provides support for entering SAS Emergency mode when communication with the proxy server fails due to no response received from sent SIP OPTIONS messages only. Up until this release, the device entered SAS Emergency mode when no response was received from sent SIP OPTIONS, INVITE, or REGISTER messages.

Using only OPTIONS messages may be useful in certain scenarios in order to avoid SAS entering Emergency mode even though the proxy is up. For example, in scenarios where many IP phones register through SAS to a proxy (softswitch), there could be a chance that the softswitch doesn't respond (for whatever reason) to a register of one of the IP phones and erroneously triggers SAS to enter Emergency mode even though the softswitch is up.

To support this feature, the following new parameter has been added:

SAS Entering Emergency Mode CLI: sas-enter-emg-mode [SASEnteringEmergencyMode]	Defines the SIP messages for which if no response is received from the proxy, triggers SAS Emergency mode. ■ [0] = (Default) SAS enters Emergency mode only if no response is received from sent SIP OPTIONS. ■ [1] = SAS enters Emergency mode if no response is received from sent SIP OPTIONS, INVITE, or REGISTER messages.

Applicable Products: All.

3.44.1.3.2 Re-using TCP Connections for SAS

This feature provides support for re-using TCP connections in the SAS application. Thus, the device can use the same TCP connection for multiple SIP requests / responses for a specific SIP UA.

For example, assume the following:

- User A sends a REGISTER message to SAS with transport=TCP.
- User B sends an INVITE message to A using SAS.

In this scenario, the device's SAS application forwards the INVITE request using the TCP connection that User A initially opened with the REGISTER message.

To support this feature, the following new parameter has been added:

SAS Connection Reuse CLI: sas-connection-reuse [SASConnectionReuse]	Enables the re-use of the same TCP connection for sessions with the same user in the SAS application. ■ [0] Disable ■ [1] Enable (default)

Applicable Products: All.

3.44.1.4 Media Features

This subsection describes the new media features.

3.44.1.4.1 CDR and Syslog Field for Automatic Machine Detection

This feature provides support for sending information relating to the Automatic Machine Detection (AMD) feature in Call Detail Records (CDR) and Syslog messages. AMD is used to detect whether a human voice, a fax machine, silence, or beeps have answered the call on the remote side. This feature is applicable only to the Gateway application.

To support this feature, the following new fields have been added:

- CDR:
  - AMD – this field can acquire one of the following values:
    - V voice
    - A answer machine
    - S silence
    - U unknown
  - % success that correctly detected answering type (probability)
- Syslog:
  - AMDSignal – this field can acquire one of the following values:
    - V voice
    - A answer machine
    - S silence
    - U unknown
  - AMDDecisionProbability – probability success that correctly detects answering type

  Below is an example of such a Syslog message with AMD information:

```
CallMachine:EVENT_DETECTED_EV - AMDSignal = <type - V/A/S/U>,
AMDDecisionProbability = <percentage> %
```

  If there is no AMD detection, the AMDSignal field is shown empty (i.e. AMDSignal =).

Applicable Products: Mediant 2000.

3.44.1.5 Networking Features

This subsection describes the new networking features.

3.44.1.5.1 Network Time Protocol Server Address by DNS

This feature provides support for defining the Network Time Protocol (NTP) server address using a fully-qualified domain name (FQDN). In previous releases, the NTP server address could only be defined as an IP address in dotted-decimal notation. The advantage of an FQDN is that multiple IP addresses can be resolved from the DNS server, providing NTP server redundancy.

To support this feature, the following existing parameters are used:

NTP Server IP Address CLI: primary-server [NTPServerIP]	Defines the NTP server's address as an FQDN or an IP address in dotted-decimal notation. The default IP address is 0.0.0.0 (i.e., internal NTP client is disabled).

NTP Secondary Server IP [NTPSecondaryServerIP]	Defines the second NTP server's address as an FQDN or an IP address in dotted-decimal notation. This NTP is used for redundancy; if the primary NTP server fails, then this NTP server is used. The default IP address is 0.0.0.0 (i.e., internal NTP client is disabled).

Applicable Products: All.

3.44.1.5.2 Disabling ICMP Redirect Messages

This feature provides support for disabling the handling of ICMP Redirect messages.

To support this feature, the following new parameter has been added:

[DisableICMPRedirects]	Determines whether the device accepts or ignores ICMP Redirect messages. ■ [0] = (Default) ICMP Redirect messages are handled by the device. ■ [1] = ICMP Redirect messages are ignored.

Applicable Products: MP-1xx; Mediant 2000.

3.44.1.6 Quality of Experience Features

This subsection describes the new Quality of Experience (QoE) features.

3.44.1.6.1 Bandwidth Management per Media Realm

This feature provides support for limiting bandwidth usage per Media Realm. It also enables the configuration of specific actions that the device performs if the bandwidth utilization of a Media Realm exceeds a user-defined threshold.

This feature defines the following states for bandwidth utilization:

- Normal
- High
- Critical

The bandwidth threshold, defined in bytes per second, and hysteresis for each state can be configured, as well as the corresponding action that the device must perform upon transitions between bandwidth states. Up to two thresholds can be configured, one for each state transition, that is, Normal-High state change and High-Critical state change. The desired action upon exceeding a user-defined threshold can be one of the following:

- Report only: If a threshold is crossed, the device generates an appropriate alarm. The alarm is cleared when the bandwidth utilization returns to normal.
- No more calls: No additional calls are allowed on the Media Realm.

To support this feature, the following new table has been added:

Bandwidth Management Table [BWManagement]	Defines bandwidth management rules per Media Realm. [BWManagement] FORMAT BWManagement_Index = BWManagement_MediaRealmIndex, BWManagement_ThresholdIndex, BWManagement_RuleAction, BWManagement_Threshold, BWManagement_Hysteresis; [\BWManagement]

	Where: ■ MediaRealmIndex: Related Media Realm ■ ThresholdIndex: Index of bandwidth threshold rule: • [0] High Threshold Rule. • [1] Critical Threshold Rule ■ RuleAction: • [0] Report Only (default) • [1] No more calls ■ Threshold: Bandwidth threshold in Bps ■ Hysteresis: Fluctuation (change) from threshold value at which the device executes the action

Applicable Products: Mediant 2000.

3.44.1.6.2 New Voice Quality Parameters for Reporting to SEM

This feature provides support for monitoring status changes of additional voice quality parameters during a call. The device reports these changes to the SEM when user-defined thresholds are crossed.

The following additional voice quality parameters can now be monitored:

- Remote MOS
- Remote Delay
- Remote Jitter
- Remote Packet Loss
- Residual Echo Return Loss (RERL)
- Remote RERL

To support this feature, the following parameter has been added to configure the direction of the monitoring in the Quality Of Experience table.

Direction [QOERules_Direction]	Defines the monitoring direction. ■ [0] Device Side ■ [1] Remote Side

Applicable Products: Mediant 2000.

3.44.1.7 PSTN Features

This subsection describes the new PSTN features.

3.44.1.7.1 B-Channel Restart

This feature provides support for restarting a specific B-channel belonging to an ISDN or CAS trunk. This feature may be useful for troubleshooting specific voice channels. To support this feature, the new SNMP MIB variable, acTrunkISDNCommonRestartBChannel has been added.

Notes:

- If a voice call is currently in progress on the B-channel, it is disconnected when the B-channel is restarted.
- B-channel restart can only be done if the D-channel of the trunk to which it belongs is synchronized (Layer 2).
- B-channel restart does not affect the B-channel's configuration.

Applicable Products: Mediant 2000.

3.44.1.7.2 Manual D-Channel Switchover

This feature provides support for manual switchover between active and standby D-channels belonging to the same NFAS group. To perform this switchover, the **Switch Activity** button on the new NFAS Group & D-channel Status page is used. This is done per selected NFAS group. If the switchover cannot be done due to, for example, alarms or unsuitable states, this button becomes unavailable (grayed out).

This feature is supported only for T1 ISDN protocols supporting NFAS, and only if the NFAS group is configured with two D-channels.

Applicable Products: Mediant 2000.

3.44.1.8 Infrastructure Features

This subsection describes the new infrastructure features.

3.44.1.8.1 FXS Line Testing

This feature provides support for testing an FXS port or phone number regarding line status and electrical measurements:

- Line status:
    - Hook status – on-hook (0) or off-hook (1)
    - Message Waiting Indication (MWI) – off (0) or on (1)
    - Ring – off (0) or on (1)
    - Reversal polarity – off (0) or on (1)
- Line electrical measurements:
    - Line current reading (mA)
    - Line voltage reading (V):
    - Line resistance reading (Ohm) – relevant only when the phone is in off-hook state

To support this feature, the following CLI command has been added:

```
LineTesting Port <port number) <test type>
```

or

```
LineTesting Phone <phone number) <test type>
```

Where *test type* can be one of the following values:

- 0 for line status
- 1 for line measurements

Applicable Products: MP-124.

3.44.1.8.2 New Format for Configuring Daylight Saving Time Period

This feature provides support for a new format option to define the Daylight Saving Time (DST) period. This period can now be defined in the format, mm:day/week:hh:mm, where,

- *mm* denotes month (e.g., 4)
- *day* denotes day of week (e.g., fri)
- *week* denotes week of month (e.g., 3)
- *hh* denotes hour (e.g., 23)
- *mm* denotes minutes (e.g., 0)

For example, "4:Fri/3:23:0" denotes Friday, the third week of April, at 11 P.M. The week field can be 1-5, where *5* denotes the last occurrence of the specified day in the specified month. For example, "4:Fri/5:23:0" denotes the last Friday of April, at 11 P.M.

Applicable Products: All.

3.44.1.9 General Management Features

This subsection describes the new general management features.

3.44.1.10 Web Management Features

This subsection describes the new Web interface features.

3.44.1.10.1 Clear History Alarms Table

This feature provides support for clearing all the alarms in the Alarms History table. To support this feature, a **Delete History Table** button has been added to the Alarms History page (Status & Diagnostics tab > System Status menu > Carrier-Grade Alarms > Alarms History). This feature is also supported by CLI (clear alarms-history) and SNMP.

Applicable Products: All.

3.44.1.10.2 Mozilla Firefox Web Browser Support

This feature provides support for running the device's Web-based management interface on Mozilla Firefox Web browser, versions 5 through 7.

Applicable Products: All.

3.44.1.10.3 New Web "Master" User Level

This feature provides support for an additional Web user privilege level – "Master User" (numerical representation in RADIUS is 220). The first Master user can only be created by the Security Administrator level user. Once created, only the Master user can add, modify, or delete other Master users. Master users have higher security privileges than the Security Administrator user; they can even delete the Security Administrator user.

Up until this release, three Web user levels were supported:

- Security Administrator – full read / write privileges for all Web pages (including security and adding lower-level Web users)
- Administrator – read / write privileges for all pages, except security-related pages
- User Monitor – read-only privileges (and no access to security-related pages)

Applicable Products: All.

3.44.1.10.4 Enhanced Management of Web Users

This feature provides support for enhanced management of Web users by introducing a new table to facilitate the creation, modification, and removal of Web users. This new table, Web Users Table, is accessed from the existing Web User Accounts page (**Configuration** tab > **System** menu > **Web User Accounts**).

Up to 10 different Web users can be added to the table, with the following user levels:

- Master User
- Security Administrator
- Admin

- Monitor

In addition to username and password, each user can be defined with the following attributes:

- Session limit – number of users that can be logged in simultaneously
- Session timeout – duration the user can be logged in
- Block duration – if a user is blocked to Web access due to exceeding number of user-defined failed login attempts, the user is unblocked after this timeout (or by the security administrator)

The Web login password must be at least eight characters, containing at least two uppercase, two lowercase, two numbers, and two special characters. It must also be at least four characters different than the previous password.

Applicable Products: All.

3.44.1.10.5 New Table Design Format

The following Web configuration tables have been re-designed into a new table format to facilitate configuration:

- Power Over Ethernet Settings
- SNMPv3 Users
- Firewall Settings
- IP Security Proposals Table
- IP Security Associations Table
- Physical Ports Table
- Internal DNS Table
- Internal SRV Table
- DSP Templates
- SIP Interface Table
- IP Group Table
- NAT Translation Table
- Destination Phone Number Manipulation Table for IP -> Tel Calls
- Destination Phone Number Manipulation Table for Tel -> IP Calls
- Source Phone Number Manipulation Table for IP -> Tel Calls
- Source Phone Number Manipulation Table for Tel -> IP Calls
- Redirect Number Tel -> IP
- Redirect Number IP -> Tel
- Forward On Busy Trunk Destination
- Tone Index Table
- Admission Control
- Condition Table
- Message Manipulations
- IP to IP Inbound Manipulation
- IP to IP Outbound Manipulation

Applicable Products: All (according to relevant page).

3.44.1.10.6 New Web Login Screen for Enhanced Security

This feature provides support for a new Web login screen. This login screen uses form-based authentication, thereby improving the security level of the device's Web-based management system.

Applicable Products: All.

3.44.1.10.7 Status Display of D-Channels and NFAS Groups

This feature provides support for displaying the status of D-channels and NFAS groups:

- D-channels: A D-channel alarm (if raised) is now indicated using the color-coded **D-Channel Alarm** icon (orange). This is displayed in the Home page and in the NFAS Group & D-Channel Status page.
- NFAS: An NFAS alarm (if raised) is now indicated using a new color-coded **NFAS Alarm** icon (dark orange). This is displayed in the Home page and in the NFAS Group & D-Channel Status page. The NFAS Group & D-Channel Status page also displays NFAS groups and their status.

Applicable Products: Mediant 2000.

3.44.1.10.8 Loopback Creation for DS1 Lines

This feature provides support for creating (and removing) loopback for DS1 lines. A new button – **Create Loopback** (and **Remove Loopback**) – was added to the Trunk Settings page to support this feature.

Applicable Products: Mediant 2000.

3.44.1.10.9 B-Channel Out-of-Service & Maintenance Alarm

This feature provides support for displaying the following B-channel status, using new color-coded icons in the Trunks & Channels Status page:

- Maintenance (orange) – The B-channel indicated by this alarm has been intentionally taken out of service due to maintenance
- Out of Service (red) - The B-channel indicated by this alarm has gone out of service

Note: This feature is not enabled by default. To enable it, please contact your AudioCodes sales representative.

Applicable Products: Mediant 2000.

3.44.1.10.10 Relocation of Message Policy & Message Manipulations Tables

The Message Policy and Message Manipulations tables are now located under the **SIP Definitions** folder in the Navigation pane.

Applicable Products: Mediant 2000.

3.44.1.10.11 SS7-Related Web Pages Removed

The SS7-related Web pages have been removed from the Web interface. This was done due to discontinuing support for SS7.

Applicable Products: All.

3.44.1.10.12 Hotline Duration Configurable in Web

This feature provides support for configuring the Hotline duration per hotline port for automatic dialing, in the Automatic Dialing page. Up until this release, hotline duration per port could only be configured using the ini file.

Applicable Products: MP-1xx.

3.44.1.11 SNMP Features

This subsection describes the new Simple Network Management Protocol (SNMP) features.

3.44.1.11.1 Encrypted Traps per SNMPv3 User

This feature provides support for associating a trap destination with a specific SNMPv3 user. This enables sending encrypted and authenticated traps to an SNMPv3 destination. By default, traps are sent unencrypted using SNMPv2.

A new field, 'Trap User' has been added to the SNMP Trap Destinations table to support this feature. This field lists the SNMP v3 users defined for traps (Trap Group) in the SNMPv3 Users table.

Applicable Products: All.

3.44.1.11.2 Restarting B-Channels

This feature provides support for restarting a B-channel. A new SNMP parameter, acTrunkISDNCommonRestartBChannel has been added to support this feature.

Applicable Products: Mediant 2000.

3.44.1.11.3 SNMP Trap for TLS Server Certificate Expiry

This feature provides support for a new SNMP trap, acCertificateExpiryNotifiaction that is sent at a user-defined number of days before the installed TLS server certificate expires. The device checks the expiry state of the certificate periodically at a user-defined interval.

To support this feature, the following new parameters have been added:

TLS Expiry Check Start CLI: expiry-check-start [TLSExpiryCheckStart]	Defines the number of days before the installed TLS server certificate will expire that the device must first send a trap to notify of this. The valid value is 0 to 3650. The default is 60.
TLS Expiry Check Period CLI: expiry-check-period [TLSExpiryCheckPeriod]	Defines the interval (in days) between device checks of the TLS server certificate expiry. The valid value is 1 to 3650. The default is 7 (i.e., checks the certificate every 7 days).

Applicable Products: MP-1xx.

3.44.2 Known Constraints

This section lists known constraints discovered in the GA version.

3.44.2.1 SIP Constraints

This release includes the following known SIP constraints for the specified products:

1. To configure IP-to-IP inbound manipulation for SAS, the IP-to-IP Inbound Manipulation table of the SBC application must be used. This table is available in the Web interface only if the SBC application is enabled and if the device is installed with the SBC Feature Key.

   Applicable Products: MP-1xx; Mediant 2000.

2. For the Tel-to-IP Call Forking feature (supported by the Gateway application), if a domain name is used as the destination in the Outbound IP Routing table, the maximum number of resolved IP addresses supported by the device's internal DNS that the call can be forked to is three (even if four IP addresses are defined for the domain name).

   Applicable Products: MP-1xx; Mediant 2000.

3. The AT&T toll free out-of-band blind transfer for trunks configured with the 4ESS ISDN protocol can only be configured using *ini* file parameters.

   Applicable Products: Mediant 2000.

4. For the IP-to-IP application, since the back-to-back user agent (B2BUA) mode is based on full termination at each leg, some SIP requests, headers and URI parameters and message bodies are omitted or changed while traversing the device. Responses to requests within a SIP dialog are always sent independently at each leg, regardless of the other leg’s response.

   - The following SIP Methods are omitted by the IP-to-IP application:
     - MESSAGE
     - PUBLISH
     - SUBSCRIBE
     - NOTIFY
     - Out-of-dialog REFER
     - Any other proprietary Method
   - The following SIP message components are omitted by the IP-to-IP application:
     - Message body (other than SDP)
     - Specific parameters in the SIP headers handled by the device (such as To, From, P-Asserted, Diversion, Remote Party ID, and Contact)
     - Specific parameters in the SDP – these parameters may affect the RTP flow at each leg independently

   Applicable Products: Mediant 2000.

3.44.2.2 Media Constraints

This release includes the following known media (voice, RTP and RTCP) constraints:

1. The device does not support the sending of RFC 2198 RTP redundancy packets as an operation if the configured packet loss threshold is exceeded; this is configured in the Quality Of Experience Web page.

   Applicable Products: All.

2. The Transparent coder (RFC 4040) poses the following limitations:

   - The coder can be used only when using physical terminations
   - No detection of IBS (e.g., DTMF)
   - Generation of IBS is only toward the network
   - No fax/modem detection or generation (i.e., no support for T.38 and Bypass)

   A workaround for this constraint is to use the G.711 coder instead.

   Applicable Products: MP-1xx; Mediant 2000.

3. The RFC 2198 Redundancy mode with RFC 2833 is not supported (i.e., if a complete DTMF digit is lost, it is not reconstructed). The current RFC 2833 implementation supports redundancy for lost inter-digit information. Since the channel can construct the entire digit from a single RFC 2833 end packet, the probability of such inter-digit information loss is very low.

   Applicable Products: MP-1xx; Mediant 2000.

4. The duration resolution of the On and Off time digits when dialing to the network using RFC 2833 relay is dependent on the basic frame size of the coder being used.

   Applicable Products: MP-1xx; Mediant 2000.

5. The Calling Tone (CNG) detector must be set to Transparent mode to detect a fax CNG tone received from the PSTN, using the Call Progress Tone detector.

   Applicable Products: MP-1xx; Mediant 2000.

6. EVRC Interleaving according to RFC 3558 is supported only on the receiving side. Supporting this mode on the transmitting side is not mandatory according to this RFC.

   Applicable Products: MP-1xx; Mediant 2000.

3.44.2.3 PSTN Constraints

This release includes the following known PSTN constraints:

1. After changing the trunk configurations from the initial factory default (i.e., trunks are of Protocol Type 'None'), a device reset is required (i.e., the change cannot be made on-the-fly).

   Applicable Products: Mediant 2000.

2. When configuring the framing method to 'Extended Super Frame' (0) or 'Super Frame' (1), the framing method is converted to another framing method. The correct value that is updated in the device is displayed in the Web interface:

   - For E1: 'Extended Super Frame' (0) and 'Super Frame' (1) are converted to 'E1 FRAMING MFF CRC4 EXT' (c).
   - For T1: 'Extended Super Frame' (0) is converted to 'T1 FRAMING ESF CRC6' (D). In addition, 'Super Frame' (1) is converted to 'T1 FRAMING F12' (B).

   Applicable Products: Mediant 2000.

3.44.2.4 Networking Constraints

This release includes the following known networking constraints:

1. In certain cases, when the Spanning-Tree algorithm is enabled on the external Ethernet switch port that is connected to the device, the external switch blocks all traffic from entering and leaving the device for some time after the device is reset. This may result in the loss of important packets such as BootP and TFTP requests, which in turn, may cause a failure in device start-up. A possible workaround is to set the *ini* file parameter BootPRetries to 5, causing the device to issue 20 BootP requests for 60 seconds. Another workaround is to disable the spanning tree on the port of the external switch that is connected to the device.

   Applicable Products: MP-1xx; Mediant 2000.

2. Configuring the device to auto-negotiate mode while the opposite port is set manually to full-duplex (either 10BaseT or 100BaseTX) is invalid. It is also invalid to set the device to one of the manual modes while the opposite port is configured differently. The user is encouraged to always prefer full-duplex connections over half-duplex and 100BaseTX over 10BaseT (due to the larger bandwidth).

   Applicable Products: All.

3. Debug Recording:

- Only one IP target is allowed.
- Maximum of 50 trace rules are allowed simultaneously.
- Maximum of 5 media stream recordings are allowed simultaneously.

Applicable Products: All.

3.44.2.5 Infrastructure Constraints

This release includes the following known infrastructure constraints:

1. The FSX Line Testing does not function on ports 2 and 3.

   Applicable Products: MP-124.

2. The following parameters do not return to their default values when attempting to restore them to defaults using the Web interface or SNMP, or when loading a new *ini* file using BootP/TFTP:

   - VLANMode
   - VLANNativeVLANID
   - RoutingTableDestinationsColumn
   - RoutingTableDestinationPrefixLensColumn
   - RoutingTableInterfacesColumn
   - RoutingTableGatewaysColumn
   - RoutingTableHopsCountColumn
   - RoutingTableDestinationMasksColumn
   - EnableDHCPLeaseRenewal
   - RoutingTableDestinationMasksColumn
   - IPSecMode
   - CASProtocolEnable
   - EnableSecureStartup
   - UseRProductName
   - LogoWidth
   - WebLogoText
   - UseWeblogo
   - UseProductName

   Applicable Products: All.

3. Files loaded to the device must not contain spaces in their file name. Including spaces in the file name prevents the file from being saved to the device's flash memory.

   Applicable Products: All.

3.44.2.6 Web Constraints

This release includes the following known Web constraints:

1. Internet Explorer's "Session Timeout" window is not displayed correctly.

   Applicable Products: All.

2. An unnecessary scroll bar appears on many of the Web pages when using 1280 x 1024 screen resolution.

   Applicable Products: All.

3. The Web interface is not displayed correctly when using the Firefox 4 Web browser. A workaround is to refresh the page using the Ctrl-and-F5 key combination.

Applicable Products: All.

4. When configuring a Media Realm in the SIP Media Realm table, if the user enters a value in the 'Port Range End' field (which should be read-only, but is erroneously read-write), this value is ignored and the Web interface assigns a value to this field based on the 'Number Of Media Session Legs' field and the 'Port Range First' field.

   Applicable Products: Mediant 2000.

5. When using the Software Upgrade Wizard, if the Voice Prompt (VP) file is loaded and the **Next** button is clicked while the progress bar is displayed, the file is not loaded to the device. Despite this failure, the user receives a message that the file has been successfully downloaded.

   Applicable Products: MP-1xx; Mediant 2000.

6. On the Software Upgrade Wizard page, the software upgrade process must be completed prior to clicking the **Back** button. Clicking the **Back** button before the wizard completes causes a display distortion.

   Applicable Products: All.

7. On the IP Interface Status page (under the **Status & Diagnostics** menu), the IP addresses may not be fully displayed if the address is greater than 25 characters.

   Applicable Products: All.

8. When using the Trunk Scroll Bar on the Trunk Settings page, some trunks may not be displayed on the Trunks panel when scrolling fast.

   Applicable Products: Mediant 2000.

9. The Web Search feature may produce incorrect search results. For example, a search result for the TLS version parameter directs the user to the incorrect page instead of the Security Settings page under the System menu.

   Applicable Products: All.

10. The fax counters, 'Attempted Fax Calls Counter' and 'Successful Fax Calls Counter' in the Status & Diagnostics page do not function correctly.

    Applicable Products: MP-1xx; Mediant 2000.

3.44.2.7 SNMP Constraints

This release includes the following known Simple Network Management Protocol (SNMP) constraints:

1. The following parameters in Media Provisioning do not change as expected: Gain Slope, Comfort Noise Generation, Tone Detector, MF R1 Enable, MF R2 Forward Enable, MF R2 Backward Enable, DTMF Enable, User Define Tone Enable, RTCP Encryption Disable Tx, RTP Authentication Disable Tx, Packet MKI Size, and T38 Version.

   Applicable Products: All.

2. When defining or deleting SNMPv3 users, the v3 trap user must not be the first to be defined or the last to be deleted. If there are no non-default v2c users, this results in a loss of SNMP contact with the device.

   Applicable Products: MP-1xx; Mediant 2000.

3.44.3 Resolved Constraints

This section lists constraints from previous releases that have been resolved in Version GA.

3.44.3.1 SIP Resolved Constraints

The following SIP constraints from the previous release have been resolved:

1. The SIP Calling Name Manipulations table can only be configured using the *ini* file parameter.

   Applicable Products: All.

2. The device does not support configuration of DNS servers (primary and secondary) per IP network interface, even though this appears in the Web interface's Multiple Interface table.

   Applicable Products: All.

3.44.3.2 Infrastructure Resolved Constraints

The following infrastructure constraints from the previous release have been resolved:

1. The Multiple Interface table does not return to default values when attempting to restore it to defaults using the Web or SNMP interfaces, or when loading a new *ini* file using BootP/TFTP.

   Applicable Products: All.

3.44.3.3 Web Resolved Constraints

The following Web constraints from the previous release have been resolved:

1. When entering negative values in the 'NTP Update Interval' field, the Web interface does not display an error message to indicate that this is not a valid value.

   Applicable Products: All.

2. In the Multiple Interface table, the 'Primary DNS Server IP Address' and 'Secondary DNS Server IP Address' fields are not applicable.

   Applicable Products: MP-1xx; Mediant 2000.

3. The Quality of Experience (QoE) feature is not supported through the Web interface.

   Applicable Products: Mediant 2000.

4. If an existing Web configuration table row is being edited and the user navigates to another configuration table page without clicking **Apply** and the user returns to the page, the edited row is removed entirely from the table and the Web no longer displays it. The user must ensure to click the **Apply** button after editing a row before navigating away from the page.

   Applicable Products: All.

5. In some Web pages, the **Submit** button is displayed for users with read-only permissions. For these users, it should not be displayed.

   Applicable Products: All.

6. The SNMPUsers_AuthKey and SNMPUsers_PrivKey parameter values are displayed in the Syslog when enabling "Activity Types to Report via 'Activity Log' Messages". This should be hidden.

   Applicable Products: MP-1xx; Mediant 2000.

7. The number of entries in the NFS table must not exceed four; otherwise, the device "crashes" after the next reset.

   Applicable Products: MP-1xx; Mediant 2000.

8. Changing the RADIUS state from Online to Offline and vice versa does not function correctly. The RADIUS enable/disable is an offline feature. As such, when changing it through the Web interface, the message should indicate that the effect will take place after a reset. However, trying to do so causes a prompt for user/password to appear, and it must be the administrator.

   Applicable Products: MP-1xx; Mediant 2000.

4 DSP Firmware Templates and Channel Capacity

This section lists the supported DSP firmware templates and capacity per product for Release 6.6.

- Installation and use of voice coders is subject to obtaining the appropriate license and royalty payments.
- The number of channels refers to the maximum channel capacity of the device.
- For additional DSP templates, contact your AudioCodes representative.

4.1 Maximum Registered Users and IP-to-IP Sessions

The table below lists the capacity per device for the following:

- Maximum number of users that can be registered in the device's registration database.
- Maximum number of call sessions for the IP-to-IP application when transcoding is implemented.

The capacity figures listed in the table below are accurate at the time of publication of this document. However, these figures may change due to a later software update. For the latest figures, please contact your AudioCodes representative.

Table 41: Maximum Registered Users and Call Sessions

Product	Registered Users SAS/IP-to-IP	IP-to-IP Mode Codec Transcoding
MediaPack 1xx	25	-
Mediant 2000	250	120

4.2 MediaPack 1xx

The table below lists the maximum supported channel capacity.

4.2.1 MP-11x

Table 42: Maximum Channel Capacity for MP-11x

	DSP Template			
	0 (**Default**)		1	
	Maximum Channels			
Model	Default (no SRTP	SRTP Enabled	Default (no SRTP	SRTP Enabled
MP-112 FXS/FXO	2	2	2	2
MP-114 FXS/FXO	4	3	3	3
MP-118 FXS/FXO	8	6	6	6
Voice Coder				
G.711 A/Mu-law PCM	√	√	√	√
G.726 ADPCM	√	√	√	√
G.727 ADPCM	√	√	√	√
G.723.1	√	√	√	√
G.729 A, B	√	√	√	√
EG.711	√	√	-	-
G.722	-	-	√	√

4.2.2 MP-124 Rev. E

Table 43: Maximum Channel Capacity for MP-124 Rev. E

Voice Coder	Maximum Channels	
	Default (no SRTP)	SRTP Enabled
G.711 A/Mu-law PCM	24	17
G.726 ADPCM	24	17
G.723.1	24	17
G.729 A, B	24	17
G.722	21	16

4.2.3 MP-124 Rev. D

Table 44: Maximum Channel Capacity for MP-124 Rev. D

	DSP Template			
	0		1	
	Maximum Channels			
	Default (no SRTP	SRTP Enabled	Default (no SRTP	SRTP Enabled
	24	18	18	18
Voice Coder				
G.711 A/Mu-law PCM	√	√	√	√
G.726 ADPCM	√	√	√	√
G.727 ADPCM	√	√	√	√
G.723.1	√	√	√	√
G.729 A, B	√	√	√	√
EG.711	√	√	-	-
G.722	-	-	√	√

4.3 Mediant 2000

The table below lists the supported channel capacity per DSP firmware template:

> DSP Templates 1 and 2 are not supported on reduced hardware assemblies (i.e., one or two trunks).

Table 45: DSP Firmware Templates for Mediant 2000

	DSP Template			
	0	**1**	**2**	**5**
	Number of Channels			
Default Setting	480	320	240	240
With 128 ms EC	400	320	240	240
With SRTP	400	-	160	240
With IPM Detectors	400	320	240	240
With IPM Detectors & SRTP	320	-	160	240
Voice Coder				
Transparent	✓	✓	✓	✓
G.711 A/µ-law PCM	✓	✓	✓	✓
G.727	✓	✓	✓	✓
G.726 ADPCM	✓	✓	✓	✓
G.723.1	✓	-	-	-
G.729 A, B	✓	✓	✓	-
GSM FR	✓	✓	-	-
MS GSM	✓	✓	-	-
EVRC	-	-	✓	-
QCELP	-	-	✓	-
AMR	-	✓	-	-
GSM EFR	-	✓	-	-
iLBC	-	-	-	✓

5 Supported SIP Standards

5.1 Supported RFCs

The table below lists the supported RFCs.

Table 46: Supported RFCs

RFC	Description	Gateway
RFC 2327	SDP	Yes
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication	Yes
RFC 2782	A DNS RR for specifying the location of services	Yes
RFC 2833	Telephone event	Yes
RFC 3261	SIP	Yes
RFC 3262	Reliability of Provisional Responses	Yes
RFC 3263	Locating SIP Servers	Yes
RFC 3264	Offer/Answer Model	Yes
RFC 3265	(SIP)-Specific Event Notification	Yes
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)	Yes
RFC 3311	UPDATE Method	Yes
RFC 3323	Privacy Mechanism	Yes
RFC 3325	Private Extensions to the SIP for Asserted Identity within Trusted Networks	Yes
RFC 3326	Reason header	Yes
RFC 3327	Extension Header Field for Registering Non-Adjacent Contacts	Yes
RFC 3361	DHCP Option for SIP Servers	Yes
RFC 3372	SIP-T	Yes
RFC 3389	RTP Payload for Comfort Noise	Yes
RFC 3420	Internet Media Type message/sipfrag	Yes
RFC 3455	P-Associated-URI	Yes
RFC 3489	STUN - Simple Traversal of UDP	Yes
RFC 3550	RTP: A Transport Protocol for Real-Time Applications	Yes
RFC 3515	Refer Method	Yes
RFC 3578	Interworking of ISDN overlap signalling to SIP	Yes
RFC 3581	Symmetric Response Routing - rport	Yes
RFC 3605	RTCP attribute in SDP	Yes

RFC	Description	Gateway
RFC 3608	SIP Extension Header Field for Service Route Discovery During Registration	Yes
RFC 3611	RTCP-XR	Yes
RFC 3665	SIP Basic Call Flow Examples	Yes
RFC 3666	SIP to PSTN Call Flows	Yes
RFC 3680	A SIP Event Package for Registration (IMS)	Yes
RFC 3711	The Secure Real-time Transport Protocol (SRTP)	Yes
RFC 3725	Third Party Call Control	Yes
RFC 3824	Using E.164 numbers with SIP (ENUM)	Yes
RFC 3842	MWI	Yes
RFC 3891	"Replaces" Header	Yes
RFC 3892	The SIP Referred-By Mechanism	Yes
RFC 3903	SIP Extension for Event State Publication	Yes
RFC 3911	The SIP Join Header	Partial
RFC 3959	The Early Disposition Type for SIP	Yes
RFC 3960	Early Media and Ringing Tone Generation in SIP	Partial
RFC 3966	The tel URI for Telephone Numbers	Yes
RFC 4028	Session Timers in the Session Initiation Protocol	Yes
RFC 4040	RTP payload format for a 64 kbit/s transparent call - Clearmode	Yes
RFC 4117	Transcoding Services Invocation	Yes
RFC 4235	Dialog Event Package	Partial
RFC 4240	Basic Network Media Services with SIP - NetAnn	Yes
RFC 4244	An Extension to SIP for Request History Information	Yes
RFC 4320	Actions Addressing Identified Issues with SIP Non-INVITE Transaction	Yes
RFC 4321	Problems Identified Associated with SIP Non-INVITE Transaction	Yes
RFC 4411	Extending SIP Reason Header for Preemption Events	Yes
RFC 4412	Communications Resource Priority for SIP	Yes
RFC 4458	SIP URIs for Applications such as Voicemail and Interactive Voice Response	Yes
RFC 4475	SIP Torture Test Messages	Yes
RFC 4497 or ISO/IEC 17343	Interworking between SIP and QSIG	Yes
RFC 4568	SDP Security Descriptions for Media Streams for SRTP	Yes
RFC 4715	Interworking of ISDN Sub Address to sip isub parameter	Yes

RFC	Description	Gateway
RFC 4730	A SIP Event Package for Key Press Stimulus (KPML)	Partial
RFC 4733	RTP Payload for DTMF Digits	Yes
RFC 4904	Representing trunk groups in tel/sip URIs	Yes
RFC 4961	Symmetric RTP and RTCP for NAT	Yes
RFC 5022	Media Server Control Markup Language (MSCML)	Yes
RFC 5079	Rejecting Anonymous Requests in SIP	Yes
RFC 5627	Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP	Yes
RFC 5628	Registration Event Package Extension for GRUU	Yes
RFC 5806	Diversion Header, same as draft-levy-sip-diversion-08	Yes
RFC 6035	SIP Package for Voice Quality Reporting Event, using sip PUBLISH	Yes
ECMA-355, ISO/IEC 22535	QSIG tunneling	Yes
draft-ietf-sip-privacy-04.txt	SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header	Yes
draft-levy-sip-diversion-08	Diversion Indication in SIP	Yes
draft-ietf-sipping-cc-transfer-05	Call Transfer	Yes
draft-ietf-sipping-realtimefax-01	SIP Support for Real-time Fax: Call Flow Examples	Yes
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection	Yes
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol	Yes
draft-ietf-sip-connect-reuse-06	Connection Reuse in SIP	Yes
draft-johnston-sipping-cc-uui-04	Transporting User to User Information for Call Centers using SIP	Yes
draft-mahy-iptel-cpc-06	The Calling Party's Category tel URI Parameter	Yes

5.2 SIP Message Compliancy

The SIP device complies with RFC 3261, as shown in the following subsections.

5.2.1 SIP Functions

The device supports the following SIP Functions:

Table 47: Supported SIP Functions

Function	Comments
User Agent Client (UAC)	-
User Agent Server (UAS)	-
Proxy Server	The device supports working with third-party Proxy Servers such as Nortel CS1K/CS2K, Avaya, Microsoft OCS, Alcatel, 3Com, BroadSoft, Snom, Cisco and many others
Redirect Server	The device supports working with third-party Redirection servers
Registrar Server	The device supports working with third-party Registration servers

5.2.2 SIP Methods

The device supports the following SIP Methods:

Table 48: Supported SIP Methods

Method	Comments
INVITE	-
ACK	-
BYE	-
CANCEL	-
REGISTER	Send only for Gateway/IP-to-IP application
REFER	Inside and outside of a dialog
NOTIFY	-
INFO	-
OPTIONS	-
PRACK	-
UPDATE	-
PUBLISH	Send only
SUBSCRIBE	-

5.2.3 SIP Headers

The device supports the following SIP Headers:

> The following SIP headers are not supported:
> - Encryption
> - Organization

- Accept
- Accept–Encoding
- Alert-Info

- Allow
- Also
- Asserted-Identity
- Authorization
- Call-ID
- Call-Info
- Contact
- Content-Disposition
- Content-Encoding
- Content-Length
- Content-Type
- Cseq
- Date
- Diversion
- Expires
- Fax
- From
- History-Info
- Join
- Max-Forwards
- Messages-Waiting
- MIN-SE
- P-Associated-URI
- P-Asserted-Identity
- P-Charging-Vector
- P-Preferred-Identity
- Priority
- Proxy- Authenticate
- Proxy- Authorization
- Proxy- Require
- Prack
- Reason
- Record- Route
- Refer-To
- Referred-By
- Replaces
- Require
- Remote-Party-ID
- Response- Key
- Retry-After
- Route
- Rseq

- Session-Expires
- Server
- Service-Route
- SIP-If-Match
- Subject
- Supported
- Target-Dialog
- Timestamp
- To
- Unsupported
- User- Agent
- Via
- Voicemail
- Warning
- WWW- Authenticate

5.2.4 SDP Fields

The device supports the following SDP fields:

Table 49: Supported SDP Fields

SDP Field	Name
v=	Protocol version number
o=	Owner/creator and session identifier
a=	Attribute information
c=	Connection information
d=	Digit
m=	Media name and transport address
s=	Session information
t=	Time alive header
b=	Bandwidth header
u=	URI description header
e=	Email address header
i=	Session info header
p=	Phone number header
y=	Year

5.2.5 SIP Responses

The device supports the following SIP responses:

- 1xx Response - Information Responses

- 2xx Response - Successful Responses
- 3xx Response - Redirection Responses
- 4xx Response - Client Failure Responses
- 5xx Response - Server Failure Responses
- 6xx Response - Global Responses

5.2.5.1 1xx Response – Information Responses

Table 50: Supported 1xx SIP Responses

1xx Response		Comments
100	Trying	The device generates this response upon receiving a Proceeding message from ISDN or immediately after placing a call for CAS signaling.
180	Ringing	The device generates this response for an incoming INVITE message. Upon receiving this response, the device waits for a 200 OK response.
181	Call is Being Forwarded	The device doesn't generate these responses. However, the device does receive them. The device processes these responses the same way that it processes the 100 Trying response.
182	Queued	The device generates this response in Call Waiting service. When the SIP device receives a 182 response, it plays a special waiting Ringback tone to the telephone side.
183	Session Progress	The device generates this response if the Early Media feature is enabled and if the device plays a Ringback tone to IP

5.2.5.2 2xx Response – Successful Responses

Table 51: Supported 2xx SIP Responses

2xx Response	
200	OK
202	Accepted

5.2.5.3 3xx Response – Redirection Responses

Table 52: Supported 3xx SIP Responses

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

5.2.5.4 4xx Response – Client Failure Responses

Table 53: Supported 4xx SIP Responses

4xx Response		Comments
400	Bad Request	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
401	Unauthorized	Authentication support for Basic and Digest. Upon receiving this message, the device issues a new request according to the scheme received on this response.
402	Payment Required	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
403	Forbidden	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
404	Not Found	The device generates this response if it is unable to locate the callee. Upon receiving this response, the device notifies the User with a Reorder Tone.
405	Method Not Allowed	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
406	Not Acceptable	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
407	Proxy Authentication Required	Authentication support for Basic and Digest. Upon receiving this message, the device issues a new request according to the scheme received on this response.
408	Request Timeout	The device generates this response if the no-answer timer expires. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
409	Conflict	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
410	Gone	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
411	Length Required	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
413	Request Entity Too Large	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
415	Unsupported Media	If the device receives a 415 Unsupported Media response, it notifies the User with a Reorder Tone. The device generates this response in case of SDP mismatch.

4xx Response		Comments
420	Bad Extension	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
423	Interval Too Brief	The device does not generate this response. On reception of this message the device uses the value received in the Min-Expires header as the registration time.
433	Anonymity Disallowed	If the device receives a 433 Anonymity Disallowed, it sends a DISCONNECT message to the PSTN with a cause value of 21 (Call Rejected). In addition, the device can be configured, using the Release Reason Mapping, to generate a 433 response when any cause is received from the PSTN side.
480	Temporarily Unavailable	If the device 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	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
482	Loop Detected	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
483	Too Many Hops	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
484	Address Incomplete	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
485	Ambiguous	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
486	Busy Here	The SIP device generates this response if the called party is off-hook and the call cannot be presented as a call waiting call. Upon receipt of this response, the device notifies the User and generates a busy tone.
487	Request Canceled	This response indicates that the initial request is terminated with a BYE or CANCEL request.
488	Not Acceptable	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
491	Request Pending	When acting as a UAS: the device sent a re-INVITE on an established session and is still in progress. If it receives a re-INVITE on the same dialog, it returns a 491 response to the received INVITE. When acting as a UAC: If the device receives a 491 response to a re-INVITE, it starts a timer. After the timer expires, the UAC tries to send the re-INVITE again.

5.2.5.5 5xx Response – Server Failure Responses

Table 54: Supported 5xx SIP Responses

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

5.2.5.6 6xx Response – Global Responses

Table 55: Supported 6xx SIP Responses

6xx Response		Comments
600	Busy Everywhere	Upon receipt of any of these responses, the device releases the call, sending an appropriate release cause to the PSTN side.
603	Decline	
604	Does Not Exist Anywhere	
606	Not Acceptable	

International Headquarters
Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com

Document #: **LTRT-27763**