MediaPack™ Media Gateways

Mediant™ Media Gateways

Multi-Service Business Gateways

SIP CPE Release Notes

Version 6.2

December 2010

Document #: LTRT-26901

AudioCodes

Table of Contents

List of Tables

Reader's Notes

Notice

This document describes the Release 6.2 of AudioCodes products – MP-1xx, Mediant 600, Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 1000, Mediant 2000, and Mediant 3000.

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 and other documents as well as software files can be downloaded by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: December-16-2010

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

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

Customer Support

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

Abbreviations and Terminology

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

Related Documentation

Document Name
Product Reference Manual for SIP Gateways and Media Servers
MP-11x & MP-124 SIP Installation Manual
Mediant 600 SIP Installation Manual
Mediant 800 MSBG SIP Installation Manual
Mediant 1000 MSBG SIP Installation Manual
Mediant 1000 SIP Installation Manual
Mediant 2000 SIP Installation Manual
Mediant 3000 SIP Installation Manual
MP-11x & MP-124 SIP User's Manual
Mediant 600 & Mediant 1000 SIP User's Manual
Mediant 800 SIP User's Manual
Mediant 1000 MSBG SIP User's Manual
Mediant 2000 SIP User's Manual
Mediant 3000 SIP User's Manual
MSBG Series CLI Reference Guide

Note: Throughout this manual, unless otherwise specified, the term *device* refers to the AudioCodes product.

1 What's New in Release 6.2

This document describes the software and hardware release of Version 6.2 and is applicable to the following AudioCodes products:

- MediaPack 1xx series (MP-11x and MP-124)
- Mediant 600
- Mediant 800 MSBG
- Mediant 1000 MSBG
- Mediant 1000
- Mediant 2000
- Mediant 3000 series (Mediant 3000/TP-6310, Mediant 3000 HA/TP-6310, Mediant 3000/TP-8410, and Mediant 3000 HA/TP-8410)

Throughout this document, a table is used to indicate the product(s) and management protocol(s) that are now also applicable to the feature. Only marked check boxes indicate applicability. For example, the table below indicates that the feature is applicable to Mediant 1000 only and for the Web interface management protocol.

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☒	Mediant 1000
☐	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☐	Mediant 2000	-	
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

Note: This Release Notes describes only features that are new to the specified devices. These features may already be supported on other devices (from previous releases). Therefore, in the table matrix used to indicate product applicability, only the products for which the feature is now supported are marked. To check whether the feature is already supported on other devices, refer to previous *Release Notes* or the *User's Manual*.

Note: Some of the features described in this document are available on the device only if the relevant software license key has been purchased from AudioCodes and installed on the device. For a list of available software license keys that can be purchased, please consult your AudioCodes sales representative.

Note: For Mediant 800 MSBG and Mediant 1000 MSBG, open source software may have been added and/or amended for this product. For further information, please visit our website at: http://audiocodes.com/support or contact your AudioCodes sales representative.

1.1 Supported Hardware Platforms

This section describes the supported hardware platforms in Release 6.2

1.1.1 New Hardware Platforms

This section describes the new hardware platforms introduced in Release 6.2.

1.1.1.1 MediaPack 1xx

No new hardware platforms.

1.1.1.2 Mediant 600

No new hardware platforms.

1.1.1.3 Mediant 800 MSBG

The Mediant 800 MSBG supports the following new hardware platforms in Release 6.2:

- Optional WAN Interfaces:
  - Symmetric High-Speed Digital Subscriber Line (SHDSL): Single SHDSL port with the following specifications:
    - Four SHDSL WAN ports housed on a single R-J45 connector
    - Conforms to ITU G.991.2 Annexes A, B, E, F and G SHDSL
    - Up to 5,696 Kbps over a single wire pair
    - Up to 22,784 Kbps over four wire pairs bonding, according to SHDSL.bis (ITU G.991.2 Annexes F, G)
    - EFM and ATM support
    - Wetting current support on the CPE side, according to G991.2
    - Supports both Central Office (CO) and CPE (wetting current on CO - excluded)
    - TC-PAM 16/32 Line Code
  - T1 WAN DSU/CSU:
    - IP over High-level Data Link Control (HDLC) and Point-to-Point Protocol (PPP) encapsulations
    - PPP password authentication protocol (PAP) and challenge-handshake authentication protocol (CHAP) authentication
    - Multiple IP interfaces on the T1 WAN interface
- E1/T1 copper wire line

The available customer-ordered hardware configurations are listed in the table below:

Table 1-1: Available Mediant 800 MSBG Models

Model	FXS	FXO	BRI	LAN GbE/FE	T1/E1	WAN	Power over Ethernet	OSN Server (CPU)
New:								
MP800-8S-12L-P	8	-	-	12 (4/8)	-	GbE	120W	-
MP800-1ET-2L	-	-	-	12 (4/8)	1	2 x T1	120W	-
MP800-1ET-12L-P-2T	-	-	-	12 (4/8)	1	GbE	120W	-
MP800-12S-12L-P-X1	12	-	-	12 (4/8)	-	GbE	120W	Atom
MP800-12O-12L-P-X1	-	12	-	12 (4/8)	-	GbE	120W	Atom
Existing:								
MP800-12S-12L-P	12	-	-	12 (4/8)	-	GbE	120W	-
MP800-4O-2L-X1	-	4	-	2 (2/0)	-	GbE	-	Atom
MP800-4S8O-2L-X1	4	8	-	2 (2/0)	-	GbE	-	Atom
MP800-4S4O-12L-P-X1	4	4	-	12 (4/8)	-	GbE	50XW	Atom
MP800-4B-12L-P	-	-	4	12 (4/8)	-	GbE	120W	-
MP800-4B-12L-P-X1	-	-	4	12 (4/8)	-	GbE	120W	Atom

1.1.1.4 Mediant 1000

No new hardware platforms.

1.1.1.5 Mediant 1000 MSBG

No new hardware platforms.

1.1.1.6 Mediant 2000

No new hardware platforms.

1.1.1.7 Mediant 3000

No new hardware platforms.

1.1.2 Existing Hardware Platforms

This section describes existing hardware platforms from the previous release that are also supported in Release 6.2.

1.1.2.1 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 analog FXO interfaces
  - MP-114/FXO providing 4 analog FXO interfaces
- MP-11x/FXS devices:
  - MP-118/FXS providing 8 analog FXS interfaces
  - MP-114/FXS providing 4 analog FXS interfaces
  - MP-112/FXS providing 2 analog FXS interfaces
- MP-124/FXS providing 24 analog FXS interfaces
- MP-124 with AC Power
- MP-124 with DC power

1.1.2.2 Mediant 600

This release supports the following existing hardware platforms:

- Up to 2 FXS modules (up to 8 FXS interfaces - RJ-11 ports)
- Up to 2 FXO modules (up to 8 FXO interfaces - RJ-11 ports)
- Up to 2 Digital TRUNKS modules (1 or 2 E1/T1/J1 PRI spans, including fractional E1/T1 - RJ-48c ports)
- Up to 2 BRI modules (4 to 8 ISDN Basic Rate Interfaces - RJ-45 ports, 4 ports per module)

These interfaces are available in one of the following configurations:

- 1 x E1/T1 port (also Fractional E1/T1)
- 2 x E1/T1 ports
- 4 x BRI ports (supporting up to 8 voice calls)
- 8 x BRI ports (supporting up to 16 voice calls)
- 4 x BRI ports and 1 x E1/T1 port
- 4 x BRI ports and 4 x FXS ports
- 4 x BRI ports and 4 x FXO ports
- 4 x FXS ports and 1 x E1/T1 port
- 4 x FXO ports and 1 x E1/T1 port

1.1.2.3 Mediant 800 MSBG

This release supports the following existing hardware platforms:

- Analog telephony interfaces, offering only FXS or only FXO interfaces, or a combination thereof. For a list of available hardware configurations and models, refer to Table 1-1.
- Optional, analog Lifeline on FXS Port 1, maintaining PSTN connectivity upon power failure. For the combined FXS/FXO configuration, one Lifeline is available; for the 12-FXS configuration, up to three Lifelines are available.
- One set of ISDN Basic Rate Interface (BRI) interfaces, providing four RJ-45 BRI S/T ports (supporting up to 8 voice channels) for connecting ISDN terminal equipment such as ISDN telephones. Each BRI port can be configured either as termination equipment/user side (TE) or network termination/network side (NT). Up to eight TE devices can be connected per BRI S/T port, by using an ISDN S-bus that provides eight ISDN ports.
- Optional, Open Solutions Network (OSN) server platform for hosting third-party applications such as IP PBX, based on the following:
  - CPU: Intel™ Atom 1.6 GHz processor (Intel Atom N270)
  - Memory: 1 GB (or 2 GB for devices with 12 FXO ports)
  - Hard disk drive (HDD): SATA with minimum of 20 GB
  - OSN ports (on rear panel) includes the following:
    - Three USB ports (Standard-A type) for connecting computer peripherals (e.g., mouse and keyboard)
    - 15-pin DB-type VGA port for connecting a monitor
  - OSN LEDs (on front panel) for hard disk drive (HDD) and link activity
  - Operating System – Microsoft Windows and Linux distributions (for certified support, please contact AudioCodes)
- Single WAN port (10/100/1000Base-T copper).
- Twelve Ethernet LAN ports, supporting half- and full-duplex modes, auto-negotiation, and straight or crossover cable detection:
  - Up to four RJ-45 10/100/1000Base-T (Gigabit) ports
  - Eight RJ-45 10/100Base-TX (Fast Ethernet) ports
- Power-over-Ethernet (PoE) supported on all LAN ports, complying with IEEE 802.3af-2003. The maximum wattage per port is 15.4W, providing a total wattage of 120W for all ports.
- Front-panel LEDs providing operating status of FXS/FXO interfaces, LAN interfaces, WAN interface, PoE, OSN, and power supply.
- Three-prong AC supply entry for AC power (standard electrical outlet) - single, universal 90-260 VAC.
- Protective earthing screws for grounding.
- Desktop or 19-inch rack mounting (using external mounting brackets).

1.1.2.4 Mediant 1000 MSBG

This release supports the following existing hardware platforms:

- Mediant 1000 and Mediant 1000B chassis. The Mediant 1000B chassis is based on the incumbent Mediant 1000 chassis, but designed to support Advanced Mezzanine Card (AMC/AdvancedMC) form-factor modules. This chassis provides eight AMC slots on its rear panel for housing single and mid-sized AMC modules. This chassis hosts the CRMX module (instead of the CMX) for supporting both VoIP Gateway and MSBG data-routing functionalities. The Mediant 1000B also provides support for the regular Mediant 1000 telephony modules (i.e., FXS, FXO, and digital PSTN).

> **Note:** The AMC chassis slots must only be housed with AMC modules approved and homologated by AudioCodes – ensure not to use these slots for AMC modules and configurations that have not been approved.

- CRMX module, providing three LAN 10/100/1000Base-T ports and one WAN port in one of the following configurations (customer ordered):
    - CRMX-C module: RJ-45 port (4-twisted pair copper cabling) providing 1 Gigabit Ethernet (GbE) interface for connection to the Internet
    - CRMX-S module: 1000Base-SX optical fiber port (multi-mode fiber)
    - CRMS-L module: 1000Base-LX optical fiber port (single-mode fiber)
    - CRMX-T: RJ-48c (2-twisted pairs copper cabling) Data Service Unit/Channel Service Unit (DSU/CSU) T1 WAN port, for connecting to a T1 line
    - CRMX-SD module: Symmetric High-Speed Digital Subscriber Line (SHDSL). This module provides 3 LAN ports and 1 SHDSL port. The SHDSL port has 4 wire-pairs, and therefore, supports 4 SHDSL ports on a single physical connector. SHDSL port specifications:
        - Conforms to ITU G.991.2 Annexes A, B, E, F and G SHDSL
        - Up to 5,696 Kbps over a single wire pair
        - Up to 22,784 Kbps over four wire pairs bonding, according to SHDSL.bis (ITU G.991.2 Annexes F, G)
        - EFM and ATM support
        - Wetting current support on the CPE side, according to G991.2
        - Supports both Central Office (CO) and CPE (wetting current on CO - excluded)
        - TC-PAM 16/32 Line Code
- Up to 6 FXS modules, where each module provides four RJ-11 ports. Therefore, the device can support up to 24 FXS interfaces (six modules * 4 ports per module).
- Up to 6 FXO modules, where each module provides four RJ-11 ports. Therefore, the device can support up to 24 FXO ground- or loop-start signaling interfaces (six modules * 4 ports per module).
- Up to 4 Digital E1/T1 TRUNKS modules (1 or 2 E1/T1/J1 PRI spans per module - RJ-48c ports).
- Up to 5 BRI modules (up to 20 ISDN Basic Rate Interface interfaces - 4 ports per module).
- Up to 3 Media Processing modules (MPM), for media processing such as announcements and conferencing

- Open Solutions Network (OSN) server platform, available in one of the following models:
  - OSN Ver. 1 (OSN1), based on Intel™ Celeron™ 600 MHz processor (for third-party applications such as IP PBX)
  - OSN Ver. 2 (OSN2), based on Intel™ Pentium™ M 1.4 GHz processor (for third-party applications such as IP PBX):
    - Integrated BroadSoft PacketSmart agent
  - OSN Ver 3 (OSN3) – supported only on the Mediant 1000B chassis, offering a high performance CPU, targeted for customer's requiring applications:
    - CPU: Intel® Core™ 2 Duo 1.5 GHz processors L7400 with Intel 3100 Chipset (64-bit)
    - RAM Memory: 2 G or 4 G DDR2 with ECC
    - Storage: Single or Dual hard-disk drive of 80 G SATA
    - Bus/Chipset: 64 Bit
    - L2 Cache: 2 M
    - Interfaces: Gigabit Ethernet, supporting automatic detection and switching between 10Base-T, 100Base-TX and 1000Base-T data transmission (Auto-Negotiation). Auto-wire switching for crossed cables is also supported (Auto-MDI/X); USB 2.0 via Connection Module; RS-232 COM

1.1.2.4.1 Module Hardware Revision Compatibility List

The Voice I/O module Hardware Revisions that are compatible with the Mediant 1000 MSBG chassis is listed in the table below:

Table 1-2: Mediant 1000 MSBG Voice I/O Module Hardware Revision Compatibility List

Item No.	Description	H/W Revision
FASB00334	M1K-SMX-1A1V1 Quad FXS w/ Life-Line Module	C08
FASB00335	M1K-SMX-1A1V1 Dual FXS w/ Life-Line Module	C08
FASB00398	M1K TMX-1A1V1 Dual trunks w/ life-line module	C08
FASB00399	M1K TMX-1A1V1 Single trunks w/ life-line module	C08
FASB00510	M1K-OMX-S 4 Indoor Ports With GS Rev.A1	C05
FASB00511	M1K-CFMX-1 Conference Module Rev A1v1	C06
FASB00520	M1K-OMX-S 4 Outdoor Ports W/O GS Rev. A1	C04
FASB00582	M1K-BMX-4A1	C03
GTPM00046	M1K-VM-2FXS	P03
GTPM00050	M1K-VM-1SPAN	P03
GTPM00052	M1K-VM-2SPAN	P03
GTPM00056	M1K-VM-4FXS	P03
GTPM00125	M1K-VM-4FXO-LS	P02
GTPM00126	M1K-VM-4FXO-GS/LS	P02
GTPM00127	M1K-M-CONF	P02
GTPM00174	M1K-VM-4BRI	P02

Item No.	Description	H/W Revision
FASU00587	CRMX-T (LAN 1, 2, 3, Dual T1 WAN DSU/CSU Trunk)	P1.2
FASU00557	CRMX-L (LAN 1, 2, 3, GE WAN 1000Base-LX)	P1.5
FASU00556	CRMX-C (LAN 1, 2, 3, GE WAN copper Ethernet)	P2
FASU00557	CRMX-S (LAN 1, 2, 3, GE WAN 1000Base-SX)	P1.5
FASU00636	CRMX-SD (LAN 1, 2, 3, SHDSL WAN)	No Revision Constraint

1.1.2.5 Mediant 1000

This release supports the following existing hardware platforms:

- Up to 6 FXS modules (up to 24 FXS interfaces - RJ-11 ports, 4 ports per module)
- Up to 6 FXO modules (up to 24 FXO interfaces, Ground-Start or Loop-Start signaling - RJ-11 ports, 4 ports per module)
- Up to 4 Digital TRUNKS modules (1, 2, or 4 E1/T1/J1 PRI spans - RJ-48c ports)
- Up to 5 BRI modules (up to 20 ISDN Basic Rate Interface channels - 4 ports per module)
- Up to 3 Media Processing modules (MPM - for media processing such as announcements and conferencing)
- OSN1 - Open Solutions Network Ver. 1, Intel™ Celeron™ 600 MHz, for third-party applications such as IP PBX
- OSN2 - Open Solutions Network Ver. 2, Intel™ Pentium™ M 1.4 GHz, for third-party applications such as IP PBX

The Mediant 1000 can be deployed with a combination of the modules listed above.

1.1.2.6 Mediant 2000

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

1.1.2.7 Mediant 3000

This release supports the following existing hardware platforms:

- Mediant 3000 hosting a single TP-6310 blade, providing SONET/SDH or T3 PSTN interfaces.
- Mediant 3000 hosting two TP-6310 blades for 1+1 HA, providing SONET/SDH or T3 PSTN interfaces.
- Mediant 3000 hosting a single TP-8410 blade, providing 16 E1/ 21 T1 PSTN interfaces.
- Mediant 3000 hosting a single TP-8410 blade, providing up to 63 E1/ 84 T1 PSTN interfaces.
- Mediant 3000 hosting two TP-8410 blades for 1+1 High Availability (HA), providing up to 16 E1/ 21 T1 PSTN interfaces.
- Mediant 3000 hosting two TP-8410 blades for 1+1 HA, providing up to 63 E1/ 84 T1 PSTN interfaces.
- Mediant 3000 hosting a single TP-8410 blade providing 16 E1/ 21 T1 PSTN interfaces with an integrated CPU (Intel Pentium) blade (M3K-ICPU-1), hosting third-party applications (such as SS7 GWC).
- Mediant 3000 hosting a single TP-8410 blade providing up to 63 E1/ 84 T1 PSTN interfaces with an integrated CPU (Intel Pentium) blade (M3K-ICPU-1), hosting third-party applications (such as SS7 GWC).

1.1.3 Hardware Platforms Not Supported

The following hardware platforms are not supported in Release 6.2:

- IPmedia 2000
- IPmedia 3000

1.2 SIP New Features

This section lists the new SIP features in Release 6.2.

1.2.1 SIP General New Features

The device supports the following new SIP general (Gateway and SBC applications) features:

1. **Maximum SIP Message Size:**

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature supports the configuration of the maximum size for each SIP message. This allows the user to limit the size of the SIP message that is sent over the network. The device rejects messages exceeding this user-defined size. The maximum SIP message size is defined using the new parameter, *MaxSIPMessageLength*. The maximum size can range between 1 and 50 Kbytes.

2. **Time Limit for Receipt of SIP Messages:**

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides a 30-second period (limit) for the receipt of a complete SIP message on the device's TCP socket. For example, if the device receives a SIP message whose SIP Content-Length header is larger than the actual message body, the TCP socket remains open and waits for the rest of the message body to arrive. During this time, no other messages are accepted by the socket. However, if the remaining message body does not arrive within 30 seconds, the device terminates the session on the socket in order to allow new messages to arrive.

3. SDP Offer/Answer Negotiation upon Modified Session:

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature enables the flexibility of ignoring a new SDP re-offer (from the media negotiation perspective) in certain scenarios (such as session expires). According to RFC 3264, once an SDP session is established, a new SDP offer is considered a new offer only when the SDP origin value is incremented. In scenarios such as session expires, SDP negotiation is irrelevant and thus, the origin field is not changed.

Even though some SIP devices don't follow this behavior and don't increment the origin value even in scenarios where they want to re-negotiate, the device up till now re-negotiated regardless of the origin field value. Since this caused problems in certain scenarios, this feature resolves this by assuming that the remote party operates according to RFC 3264, and in cases where the origin field is not incremented, the device does not re-negotiate SDP capabilities.

This feature offers the following options:

- The device negotiates any new SDP re-offer, regardless of the origin field (default).
- The device negotiates only an SDP re-offer with an incremented origin field.

This feature is configured using the new parameter, *EnableSDPVersionNegotiation*.

4. SIP Secure Connection Vulnerability:

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for securing the device's resources against SIP spam and invalid SIP messages:

- **Securing memory resources:**
  - Socket Resource Abuse: Connections that are established without subsequent data transmission are released (after one minute), allowing the establishment of new connections.
  - Established Connection Flood: The device detects and subsequently discards any flood of "false" connections (which typically prevents establishment of new legitimate connections). The device effectively manages its socket resources, releasing unused sockets for required connections.
- **CPU:**
  - Loop-Amplification Scenario: The device prevents routing between its interfaces. The attacker needs to convince the device to re-write a request to a location, which resolves to the device itself. This can be done if the routing is according to the SIP Request-URI header and the address specified is the device's IP address. This results in the server over loading itself. Another method for creating loops is through a SIP proxy to which the device routes and this proxy routes it back to the device.
    For MSBG products, the *SBCMaxForwardsLimit* parameter is used to limit the SIP Max-Forwards header value.
  - Malformed SIP Requests: Malformed SIP message requests are typically sent to cause false, expensive SIP parsing, thereby wasting CPU resources. The device's parsing has been significantly improved to detect malformed messages and to reject such messages in early parsing stages.
- **SIP Vulnerabilities:**
  - General Parser Errors: Parser errors (invalid SIP messages) do not cause loss of service.
  - SIP Content-Length header greater than the message's body: This can cause delayed or no service by causing a TCP to wait for that body to arrive.
    - TCP: maximum message length is dictated.
    - UDP: Content-Length is validated with the packet size. If the packet size is not as declared in the Content-Length header, only the actual body size is validated and the Content-Length header is ignored.
  - Invalid Content-Length header: The device ignores such messages.
  - Null characters are allowed only in the SIP message's body according to the SIP ABNF. The device rejects messages that arrive with null characters in the headers part of the message. This ensures that the device doesn't forward invalid messages that can be harmful to the internal network.

5. Transcoding Mode for SBC and IP-to-IP Applications:

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410
Management Protocol	
☒ Web ☒ INI ☐ SNMP ☐ EMS ☐ CLI	

This feature allows separate transcoding mode configuration for the SBC and IP-to-IP applications. This is important as the required DSP resources for transcoding between these applications differ. Typically, SBC uses less resources than the IP-to-IP application, which generally requires two DSP's. Therefore, two different parameters with the same options exist for configuring transcoding mode for these applications:

- *TranscodingMode*: used for the SBC application (the default–"Only if Required"–is to not use resources)
- *IP2IPTranscodingMode*: used for the IP-to-IP application (the default–"Force"–is to use full transcoding resources)

6. Proxy Redundancy Mode per Proxy Set:

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410
Management Protocol	
☒ Web ☒ INI ☐ SNMP ☐ EMS ☐ CLI	

This feature allows the configuration of the Proxy Redundancy mode per Proxy Set. Until now, the Proxy Redundancy mode could be configured only for the entire device (using the existing "global" *ProxyRedundancyMode* parameter). This feature is configured using the new parameter, *ProxyRedundancyMode* in the Proxy Set table (*ProxySet* parameter):

- Not configured - the "global" parameter *ProxyRedundancyMode* applies (default).
- Parking - the device continues operating with a redundant (now active) Proxy until the next failure, after which it operates with the next redundant Proxy.
- Homing - the device always attempts to operate with the primary Proxy server (i.e., returns to the primary Proxy whenever available).

Note that if this parameter is configured, then the global parameter is ignored.

7. SIP Authorization Header in Initial Registration Request:

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature supports the inclusion of the SIP Authorization header in initial registration (REGISTER) requests sent by the device. This feature is enabled by the new parameter, *EmptyAuthorizationHeader*.

The Authorization header contains the credentials of a User Agent (UA) in a request to a server. The sent REGISTER message populates the Authorization header with the following parameters:

- username - value of the private user identity
- realm - domain name of the home network
- uri - domain name's SIP URI of the home network
- nonce - empty value
- response - empty value

This feature complies with registration procedures according to the IMS 3GPP TS24.229 and PKT-SP-24.220 specifications.

An example of a REGISTER message with an Authorization header is shown below:

```
REGISTER sip:home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1.home1.net;branch=z9hG4bKea1dof
Max-Forwards: 68
From: <sip:alice@home1.net>;tag=s8732n
To: sip:alice@home1.net
Authorization: Digest username=alice_private@home1.net,
realm="home1.net", nonce="", response="e56131d19580cd833064787ecc"
```

8. SIP Route Header in Initial Registration Request:

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature supports the inclusion of the SIP Route header in initial registration (REGISTER) requests sent by the device. This feature is enabled by the new parameter, *InitialRouteHeader* (by default, this parameter is disabled).

When the device sends a REGISTER message (either for initial registration or to re-register), the Route header includes the proxy's FQDN or IP address and port according to the configured Proxy Set, for example:

```
Route: <sip:10.10.10.10;lr;transport=udp>
```

or

```
Route: <sip: pcscf-gm.ims.rr.com;lr;transport=udp>
```

9. CRLF Keep-Alive Mode:

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☐	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for the carriage-return and line-feed sequences (CRLF) Keep-Alive mechanism, according to RFC 5626 “Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)”. This feature prevents an “avalanche” of keep-alive messages by multiple SIP UAs to a specific server.

The SIP UA (i.e., device) uses a simple periodic message as a keep-alive mechanism to keep the flow to the proxy or registrar alive (used, for example, to keep NAT bindings open). For connection-oriented transports such as TCP/TLS, this is based on CRLF. This mechanism uses a client-to-server "ping" keep-alive and a corresponding server-to-client "pong" message. This ping-pong sequence allows the client, and optionally the server, to notify if its flow is still active and useful for SIP traffic. If the client does not receive a pong in response to its ping, it declares the flow “dead” and opens a new flow in its place. In the CRLF Keep-Alive mechanism, the client periodically sends a double-CRLF (the "ping"), then waits to receive a single CRLF (the "pong"). If the client does not receive a "pong" within this user-defined time, it considers the flow failed.

This feature is enabled by the new parameter, *UsePingPongKeepAlive*. In addition, the maximum interval after which a CRLF Keep-Alive ("ping") is sent after a received "pong" is configured using the new parameter, *PingPongKeepAliveTime* (5 to 2,000,000 sec; default is 120). The device uses the range of 80-100% of this user-defined value as the actual interval. For example, if the parameter value is set to 200 sec, the interval used is any random time between 160 to 200 seconds.

Notes:

- The Keep-Alive mechanism begins after a successful response from a SIP REGISTER request.
- The device sends a CRLF message to the Proxy Set only if the Proxy Keep-Alive feature (*EnableProxyKeepAlive* parameter) is enabled and its transport type is set to TCP or TLS. The device first sends a SIP OPTION message to establish the TCP/TLS connection and if it receives any SIP response, it continues sending the CRLF keep-alive sequences.

10. **Increase in SIP Configuration Tables:**

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

The following SIP protocol configuration tables have been increased to 32 indices (rows):

- SRD (*SRD* parameter) Proxy Set (*ProxySet* parameter)
- Proxy IPs (*ProxyIP* parameter)
- SIP Interface (*SIPInterface* parameter)
- IP Group (*IPGroup* parameter)
- Account (*Account* parameter)

11. **Increase in SIP Media Realm Table:**

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

The maximum number of row entries in the SIP Media Realm table (*CpMediaRealm* parameter) has been increased from 16 to 64. This now accommodates the increase of the Multiple Interface table (over 16 interfaces), allowing each IP interface to be assigned to a different SIP Media Realm.

12. Increased Characters for Request-URI Host Name per IP Group:

Product			
☐	MP-11x	☐	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

The maximum number of characters has been increased from 49 to 100 for defining the SIP Request-URI host name used in INVITE and REGISTER messages sent to an IP Group, or the host name in the From header of INVITE messages received from the IP Group. This host name is defined using the SIP Group Name parameter (*IPGroup_SIPGroupName*) in the IP Group table (*IPGroup* parameter).

13. Destination SRD in Tel-to-IP Routing Table:

Product			
☐	MP-11x	☐	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for defining an SRD as the IP destination for Tel-to-IP routing rules in the Outbound IP Routing table (*Prefix* parameter). Therefore, any one of the following IP destinations can be configured in this table:

- IP address or FQDN (existing support).
- IP Group - the call is routed to the Proxy Set (IP address) or SRD associated with the IP Group (existing support).
- SRD - the call is routed as follows (new support):
  - Proxy Set associated with the SRD.
  - If a Proxy Set is not defined for the SRD, then the call is sent to:
    - ✓ Media/RTP (voice): Media Realm (media port and media IP interface) associated with SRD.
    - ✓ SIP signaling: SIP Interface (SIP port and control IP interface) associated with SRD.

14. Multiple NATs for SIP Control and RTP Media using Static NAT Rules:

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☐	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for multiple network address translation (NAT) using static NAT IP rules. Different VoIP interfaces (SIP control and RTP media traffic) can now be translated into different NAT IP addresses. This feature allows, for example, the separation of VoIP traffic between different ISTP's and topology hiding (of internal IP addresses to the "public" network).

This feature is configured using the new configuration table, Static NAT table (*NATTranslation* parameter). Each IP interface configured in the Multiple Interface table (*InterfaceTable* parameter) can be associated with a NAT rule in this new table, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range). Up to 32 NAT rules can be defined.

Notes:

- Due to this enhanced feature, the *WANIPAddress* parameter (previously required to define the WAN IP address for the SIP application layer) is now obsolete. However, if this new table is not configured and the *WANIPAddress* parameter is set, then a NAT rule is automatically added to this table with an IP address defined as the *WANIPaddress* and a port range of 0-65535.
- The device's priority method for performing NAT is as follows (not relevant for SBC application):
    a. Using an external STUN server (*STUNServerPrimaryIP* parameter) to assign a NAT address for all interfaces.
    b. Using the *StaticNATIP* parameter to define one NAT IP address for all interfaces.
    c. Using the new NAT Translation table to define NAT per interface (*NATTranslation* parameter).

If NAT is not configured, the device sends the packet according to its IP address defined in the Multiple Interface table.

1.2.2 SIP Gateway New Features

The device supports the following new SIP Gateway application features:

1. **Microsoft's Wideband Real-Time RTAudio Codec Support:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☐	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☐	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☒	CLI

This feature provides support for Microsoft's Real-Time RTAudio (MS-RTA) wideband codec. The MS-RTA codec can be used in transcoding sessions with the G.722 wideband codec. In addition, wideband Linear PCM files can be played on an MS-RTA channel, preserving the file's wideband quality. The codec is available when DSP Version Template Number 1 is used.

- Valid packet intervals (range): 20 ms (intervals of multiples of 20 ms using m factor)
- Maximal m factor is 10
- Silence suppression is not supported
- Coder rates: 18000 - 29000
- Payload type (default): 114

This codec is configured using the existing *CodersGroup* parameter.

2. **Transparent Codec Packetization Time:**

Product			
☐	MP-11x	☐	MP-124
☒	Mediant 600	☒	Mediant 1000
☐	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for packetization time ("ptime") of 10 ms for the Transparent codec. This codec is configured using the existing *CodersGroup* parameter.

3. **Adapting Comfort Noise to Remote Party:**

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature enhances the device's negotiation of comfort noise generation (CNG) between SIP UAs. The device always attempts to adapt to the remote UA's request for CNG, even if silence suppression (SCE) is disabled for the voice codec.

CNG is indicated in the SIP INVITE's SDP media description line as "CN", i.e., payload type 13 (relevant only for G.711 and G.726 codecs).

To determine CNG support, the device uses the parameters *ComfortNoiseNegotiation* and *EnableStandardSIDPayloadType*, and the codec's SCE setting (enabled or disabled). If the *ComfortNoiseNegotiation* and *EnableStandardSIDPayloadType* parameters are enabled, then the following occurs:

- If the device is the initiator, it sends a "CN" in the SDP only if the SCE of the codec is enabled. If the remote UA responds with a "CN" in the SDP, then CNG occurs; otherwise, CNG does not occur.
- If the device is the receiver and the remote SIP UA does not send a "CN" in the SDP, then no CNG occurs. If the remote side sends a "CN", then CNG occurs even if the codec's SCE is disabled.

If the *ComfortNoiseNegotiation* parameter is disabled, then the device does not send "CN" in the SDP, unless the *EnableStandardSIDPayloadType* parameter and the codec's SCE are enabled, in which case, CNG occurs.

4. **Hotline Duration per Port for Automatic Dialing:**

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature allows the configuration of a timeout per port (channel) for automatic dialing when the Hotline feature is enabled. If the phone (connected to the specific port) is off-hooked and no digit is pressed for this user-defined duration (timeout), the device automatically initiates a call to the user-defined destination phone number. This timeout is configured using the new parameter, *HotLineToneDuration* in the existing Automatic Dialing table (*TargetOfChannel* parameter). This parameter has a value range of 0 to 60 seconds and default of 16.

Notes:

- The Hotline duration can be set for all ports using the existing, "global" parameter, *HotLineToneDuration*.
- This feature is applicable only to FXS and FXO interfaces.

5. **Distinctive Ringing per FXS Based on Destination Number:**

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature supports distinctive ringing patterns and call waiting tones based on destination (called) number (or prefix) for IP-to-Tel calls (FXS interfaces). This is in addition to the existing support based on calling number. For example, if multiple destination numbers are used to route incoming SIP INVITE requests to a specific FXS port, a different ringing pattern can be configured per destination number. This feature is configured using the existing *ToneIndex* parameter.

6. **Channel Select Mode for Ringing Hunt Group:**

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature offers a new channel select method–Ring to Hunt Group (9)–for allocating IP-to-Tel calls to FXS ports (channels) pertaining to a specific Hunt Group. This method routes calls to all the FXS ports pertaining to the Hunt Group. Therefore, when an IP-to-Tel call is received by the device for a specific Hunt Group, all telephones connected to the FXS ports belonging to the Hunt Group start ringing. The call is received by whichever telephone answers the call first (after which the other phones stop ringing).

The new Ring to Hunt Group channel select option is supported by the "global" *ChannelSelectMode* parameter as well as by the *ChannelSelectMode* parameter for the Trunk Group Settings table (*TrunkGroupSettings* parameter).

7. Increase in Characters for Endpoint Phone Number:

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

The maximum number of characters that can be defined for an endpoint phone number has been increased from 25 to 50. The phone numbers are configured using the *TrunkGroup* parameter (Endpoint Phone Number table for MP-1xx and Trunk Group table for digital devices).

8. Forwarding IP-to-Tel Calls to Alternative SIP Request-URI upon Busy Trunk:

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature enhances the existing Forward On Busy Trunk Destination feature (configured using the *ForwardOnBusyTrunkDest* parameter), which until now supported the configuration of only an IP address for call redirection. This feature now allows the redirect destination to be configured as a SIP Request-URI user name and host part (i.e., user@host), or host name (i.e., IP address). For example, the below configuration forwards IP-to-Tel calls to destination user "112" at host IP address 10.13.4.12, port 5060, using transport protocol TCP, if Trunk Group ID 2 is unavailable:

```
ForwardOnBusyTrunkDest 1 = 2, 112@10.13.4.12:5060;transport=tcp;
```

When configured with user@host, the original destination number is replaced by the user part.

9. **Flash-Hook with Digit Sequence:**

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides enhanced support for flash-hook digit sequences for FXS interfaces. The existing *FlashKeysSequenceStyle* parameter includes an additional option (2) that provides the following flash-hook digit sequences:

- Flash Hook key only (no other digit): Places an active call on hold.
- Flash Hook and then digit 2: Answers the call-waiting call (the first call is put on hold).
- Flash Hook and then digit 2: Toggles between active call and on-hold call.
- Flash Hook and then digit 3: Enters a three-way conference. Note that the settings of the existing *ConferenceCode* parameter are ignored.
- Flash Hook and then digit 4: Transfers a call (instead of going on-hook).

10. **On-Board, Three-Way Conferencing:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for on-board, three-way conferencing for FXS interfaces. The call conference is established by the device without the need of an external conference server. The device sets up the conference call using its IP media channels from the IP media module (i.e., MPM module). This feature is configured using the new option, On Board (2) for the existing *3WayConferenceMode* parameter.

The maximum number of simultaneous on-board, three-way conference calls supported by the device is:

- 2 for Mediant 800
- 5 for Mediant 1000 and Mediant 1000 MSBG

(Note that this feature is already supported by MP-11x.)

11. High Definition Three-Way Conferencing:

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☒	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature supports high definition, three-way conferencing using wideband codecs (e.g., G.722 and AMR-WB). Therefore, this feature allows conference participants to experience wideband voice quality. Call conferences can also include narrowband and wideband participants.

12. SIP Proprietary Header for Call QoS Statistics:

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature enables the inclusion of call quality of service (QoS) statistics in SIP BYE and SIP 200 OK responses to BYE, using a proprietary SIP header, X-RTP-Stat. This proprietary header is enabled using the new parameter, *QoSStatistics*. By default, this parameter is disabled.

The X-RTP-Stat header provides the following statistics:

- Number of received and sent voice packets
- Number of received and sent voice octets
- Received packet loss, jitter (in ms), and latency (in ms)

The X-RTP-Stat header includes the following fields:

- PS=<voice packets sent>
- OS=<voice octets sent>
- PR=<voice packets received>
- OR=<voice octets received>
- PL=<receive packet loss>
- JI=<jitter in ms>
- LA=<latency in ms>

An example of the X-RTP-Stat header in a SIP BYE message is shown below:

```
BYE sip:302@10.33.4.125 SIP/2.0
Via: SIP/2.0/UDP 10.33.4.126;branch=z9hG4bKac2127550866
Max-Forwards: 70
From: <sip:401@10.33.4.126;user=phone>;tag=1c2113553324
To: <sip:302@company.com>;tag=1c991751121
Call-ID: 991750671245200001912@10.33.4.125
CSeq: 1 BYE
X-RTP-Stat:
PS=207;OS=49680;;PR=314;OR=50240;PL=0;JI=600;LA=40;
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCR
IBE,UPDATE
User-Agent: Sip-Gateway-/v.6.2A.008.006
Reason: Q.850 ;cause=16 ;text="local"
Content-Length: 0
```

13. GRUU Support According to RFC 5627:

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for Globally Routable User Agent (UA) URI (GRUU), according to RFC 5627. This is used for obtaining a GRUU from a registrar and for communicating a GRUU to a peer within a dialog. This support is provided by the existing parameter *EnableGRUU*.

A GRUU is a SIP URI that routes to an instance-specific UA and can be reachable from anywhere. There are a number of contexts in which it is desirable to have an identifier that addresses a single UA (using GRUU) rather than the group of UA's indicated by an Address of Record (AOR). For example, in call transfer where user A is talking to user B, and user A wants to transfer the call to user C. User A sends a REFER to user C:

```
REFER sip:C@domain.com SIP/2.0
From: sip:A@domain.com;tag=99asd
To: sip:C@domain.com
Refer-To: (URI that identifies B's UA)
```

The Refer-To header needs to contain a URI that user C can use to place a call to user B. This call needs to route to the specific UA instance that user B is using to talk to user A. User B should provide user A with a URI that has to be usable by anyone. It needs to be a GRUU.

- Obtaining a GRUU: The mechanism for obtaining a GRUU is through registrations. A UA can obtain a GRUU by generating a REGISTER request containing a Supported header field with the value “gruu”. The UA includes a “+sip.instance” Contact header parameter of each contact for which the GRUU is desired. This Contact parameter contains a globally unique ID that identifies the UA instance. The global unique ID is created from one of the following:
    - If the REGISTER is per the device’s client (endpoint), it is the MAC address concatenated with the phone number of the client.
    - If the REGISTER is per device, it is the MAC address only.
    - When using TP, “User Info” can be used for registering per endpoint. Thus, each endpoint can get a unique id – its phone number. The globally unique ID in TP is the MAC address concatenated with the phone number of the endpoint.

  If the remote server doesn’t support GRUU, it ignores the parameters of the GRUU. Otherwise, if the remote side also supports GRUU, the REGISTER responses contain the “gruu” parameter in each Contact header. This parameter contains a SIP or SIPS URI that represents a GRUU corresponding to the UA instance that registered the contact. The server provides the same GRUU for the same AOR and instance-id when sending REGISTER again after registration expiration. RFC 5627 specifies that the remote target is a GRUU target if its’ Contact URL has the "gr" parameter with or without a value.
- Using GRUU: The UA can place the GRUU in any header field that can contain a URI. It must use the GRUU in the following messages: INVITE request, its 2xx response, SUBSCRIBE request, its 2xx response, NOTIFY request, REFER request and its 2xx response.

14. Sending/Receiving IP Calls to/from Trusted IP Addresses:

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for sending and receiving IP calls only to and from “trusted” IP addresses respectively. Trusted IP addresses are those that appear in the Outbound IP Routing/Tel to IP Routing table (*routing* table) or Proxy Set table. In addition, if a fully-qualified domain name (FQDN) is defined in the routing table or Proxy Set table, the call is allowed only if the resolved DNS IP address appears in one of these tables. Calls with IP addresses or resolved IP addresses (in case of DNS queries) that do not appear in the routing table or Proxy Set table are rejected.

This feature is configured using the new option, “Secure All Calls” (2) for the existing *SecureCallsfromIP* parameter.

15. Trunk Re-Registration upon Return to Service:

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature supports re-registration of the device's trunks that return to service. When using the Account table to register a Trunk Group (to a Proxy server), if all trunks pertaining to the Trunk Group are down, the device unregisters the trunks. If any trunk belonging to the Trunk Group is returned to service, the device registers them again. This ensures, for example, that the Proxy does not send INVITEs to trunks that are out of service.

16. Maximum Simultaneous TLS Connections:

Product									
☐	MP-11x				☐	MP-124			
☐	Mediant 600				☐	Mediant 1000			
☐	Mediant 800 MSBG				☐	Mediant 1000 MSBG			
☐	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for an increase in the maximum number of simultaneous Transport Layer Security (TLS) sessions. The device now supports up to 500 TLS sessions. The maximum TLS sessions for other products remains the same:

- 10: MP-1xx
- 50 Mediant 800 MSBG
- 100: Mediant 600, Mediant 1000, Mediant 1000 MSBG and Mediant 2000

17. **Table Increase for Source Phone Number Manipulation Table for IP-to-Tel Calls:**

Product									
☐	MP-11x				☐	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

The Source Phone Number Manipulation Table for IP-to-Tel Calls table (*SourceNumberMapIP2Tel* parameter) has been increased from 20 to 120 indices (rows).

18. **Enhanced IP-to-Tel Number Manipulation:**

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☐	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for configuring enhanced (additional) source and destination number manipulation rules for IP-to-Tel calls. This feature enhances the use of the existing number manipulation tables (NumberMapIP2Tel and SourceNumberMapIP2Tel parameters for destination and source number manipulation, respectively). The initial and additional number manipulations are both done in these tables. The additional manipulation is performed on the initially manipulated source and destination numbers. Therefore, additional manipulation can be implemented to perform complex manipulation rules that can now be accommodated by the limiting size of the manipulation tables.

This feature is enabled using the following new parameters:

- *PerformAdditionalIP2TELSourceManipulation* for source number manipulation
- *PerformAdditionalIP2TELDestinationManipulation* for destination number manipulation

19. RTCP XR Voice Quality Monitoring:

Product									
☐	MP-11x				☐	MP-124			
☐	Mediant 600				☐	Mediant 1000			
☐	Mediant 800 MSBG				☐	Mediant 1000 MSBG			
☐	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☒	CLI

This feature provides support for RTP Control Protocol Extended Reports (RTCP XR) according to RFC 3611. RTCP XR is a VoIP management control that defines a set of metrics containing information for assessing VoIP call quality and diagnosis. RTCP XR measures call quality such as packet loss, delay, signal/noise/echo levels, estimated R-factor, and mean opinion score (MOS). RTCP XR extends the RTCP reports defined in RFC 3550 by providing additional VoIP metrics.

RTCP XR information publishing is implemented in the device according to <draft-johnstonsipping-rtcp-summary-07>. This draft defines how a SIP UA publishes the detailed information to a defined collector. RTCP XR messages containing key call-quality-related metrics are exchanged periodically (user-defined) between the device and the SIP UA. This allows an analyzer to monitor these metrics midstream or a device to retrieve them using SNMP. The device can send RTCP XR reports to an Event State Compositor (ESC) server using SIP PUBLISH messages.

These reports can be sent at the end of each call (configured using *RTCPXRReportMode*) and according to a user-defined interval (*RTCPInterval* or *DisableRTCPRandomize*) between consecutive reports. To enable RTCP XR reporting, the *VQMonEnable* parameter is used. This feature requires that the device be installed with the relevant Software Upgrade Key.

Additional RTCP XR parameters include *VQMonGMin*, *VQMonBurstHR*, *VQMonDelayTHR*, *VQMonEOCRValTHR*, *RTCPXRESCTransportType*, and *RTCPXREscIP*.

20. T.38 SDP T38MaxBitRate Negotiation:

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature supports the negotiation of the T.38 maximum supported fax data rate provided in SIP's SDP T38MaxBitRate parameter. The negotiated T38MaxBitRate is the minimum rate supported between the local and remote endpoints. The maximum rate supported by the device is configured using the existing parameter, *FaxRelayMaxRate*.

21. New Range and Defaults for T.38 Fax Maximum Buffer Size:

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides a modified value range and default for the *T38FaxMaxBufferSize* parameter, which is used in SIP T.38 negotiation in SDP.

- Value range: 500 to 3000 bytes
- Default value:
  - 1,024 bytes: MP-1xx, Mediant 1000, Mediant 1000 MSBG, Mediant 2000
  - 3000 bytes: Mediant 800 MSBG, Mediant 3000

22. New Range and Defaults for T.38 Fax Maximum Datagram Size:

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides a modified value range and default for the *T38MaxDatagramSize* parameter, which is used in SIP T.38 negotiation in SDP.

- Value range: 120 to 600 bytes
- Default value:
  - 238 bytes: MP-1xx, Mediant 1000, Mediant 1000 MSBG, Mediant 2000
  - 560 bytes: Mediant 800 MSBG, Mediant 3000

23. Fax Transmission behind NAT:

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☐	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for transmission from fax machines (connected to the device) located inside a Network Address Translation (NAT). Generally, the firewall blocks T.38 (and other) packets received from the WAN, unless the device behind the 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.

This feature is enabled using the new parameter, *T38FaxSessionImmediateStart*. The No-Op packets are enabled using the existing *NoOpEnable* and *NoOpInterval* parameters.

24. Euro-ISDN Message Waiting Indication (MWI) for IP-to-Tel Calls:

Product			
☐	MP-11x	☐	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for Euro-ISDN MWI for IP-to-Tel calls. The device interworks SIP MWI NOTIFY messages to Euro-ISDN Facility information element (IE) MWI messages. This is supported by the existing *VoiceMailInterface* parameter (set to 8).

25. B-Channel Off-Hook Cut-Through:

Product									
☐	MP-11x				☐	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☐	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature enables PSTN CAS channels/endpoints to receive incoming IP calls even if the B-channel is in off-hook state. This feature is enabled using the new parameter, *DigitalCutThrough*.

The following scenario describes the mechanism of this feature:

a. A Tel-to-IP call is established (connected) by the device for a B-channel.

b. The device receives a SIP BYE (i.e., IP side ends the call) and plays a reorder tone to the PSTN side for the duration set by the new parameter, *CutThroughTimeForReOrderTone*. The device releases the call towards the IP side (sends SIP 200 OK).

c. The PSTN side, for whatever reason, doesn't go on-hook. However, the device regards the state as on-hook.

d. If a new IP call is received for this B-channel after the reorder tone has ended, the device “cuts through” the channel and connects the call immediately (even though the B-channel is in physical off-hook state) without playing a ring tone. If an IP call is received while the reorder tone is played, then the device rejects the call.

This new parameter has also been added to the Tel Profile table (*TelProfile* parameter), allowing the Digital Cut-Through feature to be applied to specific B-channels using specific CAS tables (by assigning this Tel Profile to the required B-channels only).

26. Sending and Receiving RTP Packets without SIP Messages:

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature enables the device to start sending and/or receiving RTP (media) packets to and from remote endpoints without the need to establish a SIP session. The remote IP address is determined according to the Outbound IP Routing table (*Prefix* parameter). The port used is the same port as the local RTP port (configured by the existing *BaseUDPPort* parameter and the channel on which the call is received).

This feature can be configured per trunk using the new *RTPOnlyModeForTrunk_ID* parameter or for all trunks using the new *RTPOnlyMode* parameter.

27. Pre-emption of IP-to-Tel E911 Emergency Calls:

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature supports the pre-emption of IP-to-Tel E911 emergency calls. If the device receives an E911 call and there are unavailable channels, the device terminates one of the calls and sends the E911 call to that channel. This feature is enabled by the new value option, “Emergency” (3) of the existing *CallPriorityMode* parameter.

Note that this feature is applicable to FXO, CAS, and ISDN interfaces.

28. Combined Support for Digit Map and External Dial Plan File:

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for implementing both the Digit Map (*DigitMapping* parameter) and external Dial Plan (*DialPlanIndex* parameter). For example, the Digit Map can be used for complex digit patterns (which are not supported by the Dial Plan) and the Dial Plan can be used for long lists of relatively simple digit patterns. In addition, as timeout between digits is not supported by the Dial Plan, the Digit Map can be used to define digit patterns (*MaxDigits* parameter) that are shorter than those defined in the Dial Plan or left at default. For example, “xx.T” instructs the device to use the Dial Plan and if no matching digit pattern, it waits for two more digits and then after timeout (*TimeBetweenDigits* parameter) it sends the collected digits. Therefore, this ensures that calls are not rejected as a result of their digit pattern not been completed in the Dial Plan.

Note: By default, the device first attempts to locate a matching digit pattern in the Dial Plan, and if not found, then uses the Digit Map.

29. Multi-AMD Sensitivity Table:

Product			
☐	MP-11x	☐	MP-124
☒	Mediant 600	☒	Mediant 1000
☐	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for multi-language/country Answering Machine Detection (AMD). This is achieved by the new Multi-AMD Sensitivity table. The table provides up to 4 different AMD Sensitivity suites (selected by the new *AMDSensitivityParameterSuit* parameter), where each suite comprises up to 16 different sensitivity permutations (selected by the new *AMDSensitivityLevel* parameter).

The AMD Sensitivity table is loaded to the device as a binary (*.dat) file) auxiliary file. The DConvert utility can be used to convert the file from XML before loading to the device. The file name or URL is configured using the new parameters, *AMDSensitivityFileUrl* and *AMDSensitivityFileName* respectively.

30. Answer Machine Detector (AMD) per Call:

Product			
☐	MP-11x	☐	MP-124
☒	Mediant 600	☒	Mediant 1000
☐	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for configuring AMD per call based on the called number or Trunk Group. This is achieved by the inclusion of the following AMD parameters in the IP Profile table (*IPProfile* parameter): *AMDSensitivityParameterSuit*, *AMDSensitivityLevel*, *AMDMaxGreetingTime*, and *AMDMaxPostSilenceGreetingTime*. This IP Profile can then be assigned to a Trunk Group in the Inbound IP Routing table (*PSTNPrefix* parameter).

31. Additional VXML Script Attributes for Invoking VXML Scripts:

Product									
☐	MP-11x				☐	MP-124			
☐	Mediant 600				☒	Mediant 1000			
☐	Mediant 800 MSBG				☐	Mediant 1000 MSBG			
☐	Mediant 2000								
☐	Mediant 3000/TP-6310				☐	Mediant 3000 HA/TP-6310			
☐	Mediant 3000/TP-8410				☐	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for the following additional VXML session variables and events:

- session.connection.local.uri
- session.connection.remote.uri
- session.connection.protocol.name
- session.connection.protocol.version (version is ‘2’ instead of ‘2.0’)
- session.connection.redirect (redirect reason and screening information contains ‘_’ instead of whitespace between words)
- session.connection.aai

32. Activating VXML Script on Receipt of Regular INVITE:

Applicable Product									
☐	MP-11x				☐	MP-124			
☐	Mediant 600				☒	Mediant 1000			
☐	Mediant 800 MSBG				☐	Mediant 1000 MSBG			
☐	Mediant 2000								
☐	Mediant 3000/TP-6310				☐	Mediant 3000 HA/TP-6310			
☐	Mediant 3000/TP-8410				☐	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for activating a Voice XML (VXML) script using the VXMLID parameter in the Request-URI user part only, upon receipt of a regular INVITE message. For example:

```
Request-URI = <VXMLID>http://mydomain.com/myscript.cgi@host;
```

Up till now, VXML was invoked on the receipt of SIP Request-URIs such as:

```
<VXMLID>@host;voicexml= http://...
```

This feature is supported for IP-to-Tel and Tel-to-IP calls. For specified dialed phone numbers, the user part can be manipulated by adding a VXML script path. For example, upon receipt of the INVITE request, **`INVITE sip:100@myhost`** the device can be configured to manipulate (using the IP to Tel Manipulation table) the Request-URI user part to **`voicexml=http://myhost.com/script.cgi@myhost`**.

33. Enhanced ISDN BRI Support:

Product									
☐	MP-11x				☐	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☐	Mediant 2000								
☐	Mediant 3000/TP-6310				☐	Mediant 3000 HA/TP-6310			
☐	Mediant 3000/TP-8410				☐	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☐	EMS	☐	CLI

This feature provides enhanced support for Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) phones connected to the device. This feature enables the device to route IP-to-Tel calls (including voice and fax) to specific BRI ports (channels). This is achieved by the following configuration elements:

- New ISDN Supplementary Services table (*ISDNSuppServ* parameter): This table allows you to define BRI phone extension numbers per BRI port pertaining to a specific BRI module. Therefore, this offers support for point-to-multipoint configuration of several phone numbers per BRI channel. Up to eight phone numbers can be defined per BRI trunk. In addition, for each BRI endpoint, the following optional configurations can be defined:
    - User ID and password - for registering the BRI endpoint to a third-party softswitch for authentication and/or billing
    - Caller ID name - for displaying the BRI endpoint's caller ID to a dialed destination, if enabled (i.e., "Presentation" is not restricted)
    - Caller ID presentation/restriction
    - Enable/disable sending caller ID to BRI phone
- Existing Channel Select Mode (*ChannelSelectMode* parameter): The new option, "Select Trunk by ISDN Supplementary Services Table" (10) in the Trunk Group Settings table (*TrunkGroupSettings* parameter), allows the routing of IP-to-Tel calls to specific BRI channels according to the settings in the ISDN Supplementary Services table.

34. Registration Status Display for BRI Endpoints:

Product									
☐	MP-11x				☐	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☐	Mediant 2000								
☐	Mediant 3000/TP-6310				☐	Mediant 3000 HA/TP-6310			
☐	Mediant 3000/TP-8410				☐	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☐	EMS	☐	CLI

This feature provides support for displaying the registration status of BRI endpoints in the Web interface. This information is displayed in the Registration Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **Registration Status**).

35. BRI Call Forwarding Supplementary Service:

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☐	EMS	☐	CLI

This feature provides support for call forwarding (CF) services initiated by ISDN Basic BRI phones connected to the device. Upon receipt of an ISDN Facility message for call forward from the BRI phone, the device sends a SIP INVITE to the softswitch with a user-defined code in the SIP To header, representing the reason for the call forward.

The codes for the call forward can be defined using the following new parameters:

- *SuppServCodeCFU* - Call Forward Unconditional
- *SuppServCodeCFUDeact* - Call Forward Unconditional Deactivation
- *SuppServCodeCFB* - Call Forward on Busy
- *SuppServCodeCFBDeact* - Call Forward on Busy Deactivation
- *SuppServCodeCFNR* - Call Forward on No Reply
- *SuppServCodeCFNRDeact* - Call Forward on No Reply Deactivation

Note that these codes must be defined according to the softswitch (i.e., the softswitch must recognize them).

Below is an example of an INVITE message sent by the device indicating unconditional call forward ("*72") to extension number 100. This code is defined using the *SuppServCodeCFU* parameter.

```
INVITE sip:*72100@10.33.8.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.5:5060;branch=z9hG4bKWDSUKUHWFEXQSVOUVJGM
From: <sip:400@10.33.2.5;user=phone>;tag=DUOROSXSOYJJLNBFRQTG
To: <sip:*72100@10.33.8.53;user=phone>
Call-ID: GMNOVQRRXUUCYCQSFAHS@10.33.2.5
CSeq: 1 INVITE
Contact: <sip:400@10.33.2.5:5060>
Supported: em,100rel,timer,replaces
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCR
IBE
User-Agent: Sip Message Generator V1.0.0.5
User-to-User: 31323334;pd=4
Content-Type: application/sdp
Content-Length: 155
```

36. BRI Suspend-Resume Supplementary Service:

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for call suspend and resume services initiated by ISDN BRI phones connected to the device. During an ongoing call, the BRI phone user can suspend the call by typically pressing the phone's "P" button or a sequence of buttons (depending on the phone) and then on-hooking the handset. To resume the call, the phone user typically presses the same button(s) again and then off-hooks the phone. During the suspended state, the device plays a Howler tone to the remote party.

Note that instead of pressing the call park button(s), the phone cable can also be disconnected (suspending the call) and then reconnected again (resuming the call).

If the phone user does not resume the call within a user-defined interval (configured using the existing *HeldTimeout* parameter), the device releases the call.

37. Attended Call Transfer for BRI Interfaces:

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for attended (consultation) call transfer for BRI phones (user side) connected to the device and using the Euro ISDN protocol. BRI call transfer is according to ETSI TS 183 036, Section G.2 (Explicit Communication Transfer – ECT). Call transfer is enabled using the existing parameters, *EnableTransfer* and *EnableHoldtoISDN*.

Note: Currently, the BRI interface does not support blind call transfer.

38. MWI for BRI Interfaces:

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for MWI on BRI phones connected to the device and using the Euro ISDN BRI variant. When this feature is activated and a voice mail message is recorded to the mail box of a BRI extension, the softswitch sends a notification to the device. In turn, the device notifies the BRI extension and a red light flashes on the BRI extension's phone. Once the voice message is retrieved, the MWI light on the BRI extension turns off.

This feature is configured by the new option, "ETSI" (8) of the existing *VoiceMailInterface* parameter and enabled by the existing *EnableMWI* parameter.

39. Keypad Protocol for DTMF Digits According to ETS 300 122-1:

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for ISDN Information messages received from BRI phones using Information messages. During a call, if the BRI phone user presses digits (for example, for interactive voice response/IVR applications such as retrieving voice mail messages), ISDN Information messages received by the device for each digit are sent in the voice channel to the IP network as DTMF signals. The method by which the device "injects" these DTMF signals into the IP is defined by the existing parameter, *TxDTMFOption*.

40. Interworking Date/Time between SIP and Euro-ISDN:

Product									
☐ MP-11x					☐ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for interworking date and time between SIP and Euro-ISDN:

- SIP-to-ISDN interworking: The date and time from the received SIP 200 OK message is included in the ISDN Connect message by the addition of the Date/Time Information Element (IE).
- ISDN-to-SIP interworking: The date and time in the Date/Time IE received from the ISDN Connect message is interworked to the SIP Date header and sent to the IP network.

This feature is essential for synchronization between the PSTN (for example, PBX) and the IP network.

Note: The Date/Time IE can only be sent by an ISDN network-side trunk.

41. Interworking ISDN Offhook IE to SIP INVITE:

Product									
☐ MP-11x					☐ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for interworking the ISDN Setup message with an offhook indicator IE to SIP INVITE's Request-URI header (in addition to the existing support for the Contact header). Upon receipt of an ISDN offhook indicator IE from the PSTN side, the device sends a SIP INVITE to the IP side with the parameters "tgrp=hotline" or "tgrp=hotline-ccdata" included in the Request-URI and Contact headers.

This feature is configured using the new option, "Hotline Extended" (4) of the existing *UseSIPTgrp* parameter.

Note: This feature is applicable to Department of Defense (DoD) applications, according to the UCR 2008 Change 1 specification.

42. Redirect Number Overwritten by Destination Number for IP-to-Tel Calls:

Product									
☐ MP-11x					☐ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature allows the device to overwrite the redirect number with the destination number from the received SIP INVITE message in the outgoing ISDN call. This is achieved by assigning an IP Profile (*IPProfile* parameter) defined with the *CopyDest2RedirectNumber* parameter set to 1, to the IP-to-Tel Routing table (*PSTNPrefix* parameter). Even if there is no SIP Diversion or History header in the incoming INVITE message, the outgoing Q.931 Setup message will contain a redirect number.

43. Replacing Calling Number with Redirect Number in Incoming ISDN-to-IP Call:

Product									
☐ MP-11x					☐ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature allows the device to replace the calling number with the redirect number in ISDN-to-IP calls. When such a replacement occurs, the calling name is deleted and left blank. The outgoing INVITE message does not include the redirect number that was used to replace the calling number. The replacement is done only if a redirect number is present in the incoming call. This feature is enabled using the new parameter, *ReplaceCallingWithRedirectNumber*.

44. Manipulation of Redirect Reason for Tel-to IP Calls:

Product					
☐ MP-11x			☐ MP-124		
☒ Mediant 600			☒ Mediant 1000		
☒ Mediant 800 MSBG			☒ Mediant 1000 MSBG		
☒ Mediant 2000					
☒ Mediant 3000/TP-6310			☒ Mediant 3000 HA/TP-6310		
☒ Mediant 3000/TP-8410			☒ Mediant 3000 HA/TP-8410		
Management Protocol					
☒ Web		☒ INI	☒ SNMP	☒ EMS	☐ CLI

This feature provides support for configuring a default redirect reason for Tel-to-IP calls. This is configured by the new parameter, *Tel2IPDefaultRedirectReason*.

The device includes this default redirect reason in the SIP History-Info header of the outgoing INVITE if the received Q931 ISDN Setup message does not include a redirect reason or includes only an “unknown” reason. If a redirect reason exists in the received Setup message, the new parameter is ignored and the device sends the INVITE message with the reason according to the received Setup message. If the parameter is not configured, the outgoing INVITE is sent with the redirect reason (if none or “unknown” then no reason) as received in the Setup message.

45. UC Namespace for MLPP Calls:

Product					
☐ MP-11x			☐ MP-124		
☒ Mediant 600			☒ Mediant 1000		
☒ Mediant 800 MSBG			☒ Mediant 1000 MSBG		
☒ Mediant 2000					
☒ Mediant 3000/TP-6310			☒ Mediant 3000 HA/TP-6310		
☒ Mediant 3000/TP-8410			☒ Mediant 3000 HA/TP-8410		
Management Protocol					
☒ Web		☒ INI	☒ SNMP	☒ EMS	☐ CLI

This feature provides support for configuring a new default namespace, “UC” for Multi-Level Precedence & Preemption (MLPP) calls received from the ISDN side and destined for the Application server. This is configured by setting the existing parameter *MLPPDefaultNamespace* to the new option, “UC” (5). The namespace value is not present in the Precedence IE of the PRI Setup message. Therefore, this value is used in the Resource-Priority header of the outgoing SIP INVITE request.

46. Response to SIP OPTIONS only if Trunk Group 1 is Available:

Product			
☐	MP-11x	☐	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for responding to received SIP OPTIONS (e.g., from a softswitch) only if Trunk Group #1 has available trunks. If all the trunks pertaining to Trunk Group #1 are down or busy, the device does not respond to received SIP OPTIONS. This feature is enabled using the new parameter, *TrunkStatusReportingMode*.

47. ISDN Facility IE Trace:

Product			
☐	MP-11x	☐	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for enabling ISDN traces of Facility Information Elements (IE) for ISDN call diagnostics. This allows you to trace all the parameters contained in the Facility IE and view them in the Syslog. This feature is enabled using the new parameter, *FacilityTrace*.

Note: For this feature to be functional, the *GWDebugLevel* parameter must be enabled (set to at least level 1).

1.2.3 SIP SAS New Features

The device supports the following new SIP Standalone Survivability (SAS) application features:

1. **Blocking Incoming Calls from Unregistered SAS Users:**

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature rejects SIP INVITE messages received from unregistered SAS users, in SAS Normal and Emergency modes. This feature is enabled by the new parameter *SASBlockUnRegUsers*.

2. **Maximum Registered SAS Users:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☒	Mediant 1000
☐	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

The maximum number of SAS users that can be registered to the device has been increased to 600.

3. **SAS Normal Mode Routing Enhancement:**

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☐ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☐ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature enhances routing capabilities for SAS Normal mode by using the IP-to-IP Routing table to route SAS IP-to-IP calls to different destinations (and not only to the SAS Proxy Set). This is configured by the new option, “Use Routing Table only in normal mode (before forward to proxy)” (4) of the existing *SASSurvivabilityMode* parameter. Note that when this parameter is set to this option, the IP-to-IP Routing table (*IP2IPRouting* parameter) is used only when SAS is in Normal mode and is unavailable when SAS is in Emergency mode.

4. **SAS Manipulation on INVITE Requests:**

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☐ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☐ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for SAS manipulation on the SIP Request-URI user part of incoming INVITE requests (in addition to the existing support for REGISTER requests). Once manipulated, the SAS application searches for the user in the registration database. Manipulation is configured in the existing SAS Registration Manipulation Table (*SASRegistrationManipulation*).

Note: This feature does not change the Request-URI of the outgoing INVITE message.

1.3 Session Border Controller New Features

The device supports the following new Session Border Controller (SBC) features:

1. **SBC Support by Mediant 3000:**

Product									
☐ Mediant 800 MSBG					☐ Mediant 1000 MSBG				
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

The SBC application is now fully supported by the Mediant 3000 (including Mediant 3000 High Availability). The SBC application now replaces the previously supported B2BUA application and includes all the SBC features supported by the MSBG series products, for example SIP header manipulations and USER-type IP Groups (i.e., registration of users in internal database).

2. **Maximum Registered SBC Users:**

Product									
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☐ Mediant 3000/TP-6310					☐ Mediant 3000 HA/TP-6310				
☐ Mediant 3000/TP-8410					☐ Mediant 3000 HA/TP-8410				
Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

The maximum number of SBC users that can be registered to the device's database has been increased to 200 for Mediant 800 MSBG and 600 for Mediant 1000 MSBG.

3. **Maximum Registered SBC Users:**

Product									
☐ Mediant 800 MSBG					☐ Mediant 1000 MSBG				
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

The maximum number of SBC users that can be registered to the database of a fully populated device has been increased to 2,000.

4. **SBC Registration Timers:**

Product			
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature now enables the device to retain the original value of the SIP Expires header received from the user or proxy. This feature also applies when the SBC is in “survivability” state (i.e., REGISTER requests cannot be forwarded to the proxy and is terminated by the SBC).

This feature is configured using the following new parameters:

- ***SBCUserRegistrationTime*:** This parameter replaces the now obsolete *SBCRegistrationTime* parameter. This parameter defines the duration of the periodic registrations between the user and the SBC. When set to 0, the SBC does not change the Expires value received in the user’s REGISTER request. If no Expires header is received in the REGISTER and *SBCUserRegistrationTime* is set to 0, the Expires value is set to 180 seconds (by default).
- ***SBCProxyRegistrationTime*:** This parameter replaces the *RegistrationTime* parameter. This parameter defines the duration for which the user is registered in the proxy database. When set to 0, the SBC sends the Expires value as received from the user to the proxy. (**Note:** The *RegistrationTime* parameter is still applicable to non-SBC applications.)
- ***SBCSurvivabilityRegistrationTime*:** This parameter defines the duration of the periodic registrations between the user and SBC when the SBC is in survivability state. When set to 0, the SBC uses the value of the *SBCUserRegistrationTime* parameter for the SBC response.

5. **IP Alert Timeout to SBC Outgoing INVITE Message:**

Product			
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature allows the configuration of a timeout (in seconds) for SBC outgoing (outbound IP routing) SIP INVITE messages. If the called IP party does not answer the call within this user-defined interval, the device disconnects the session. The device starts the timeout count upon receipt of a SIP 180 Ringing response from the called party. If no other SIP response (for example, 200 OK) is received thereafter within this timeout, the call is released. This feature is configured using the new parameter, *SBCAlertTimeout*.

6. **Max-Forwards SIP Header Size:**

Product			
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides control over the SIP Max-Forwards header value. The Max-Forwards header is used to limit the number of servers (such as proxies) that can forward the SIP request. The Max-Forwards value indicates the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request.

The Max-Forwards SIP header value is configured using the new parameter, *SBCMaxForwardsLimit*. The value range can be between 1 and 70 (the default is 10). This parameter affects the Max-Forwards header in the received message, as follows:

- If the received header's original value is 0, the message is not passed on and is rejected.
- If the received header's original value is less than the parameter's value, the header's value is decremented before being sent.
- If the received header's original value is greater than the parameter's value, the header's value is replaced by the parameter's value.

7. **Active SBC Call Continuity during High Availability Blade Switchover:**

Product			
☐	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for maintaining active SBC call sessions during a blade switchover. Upon blade failure, the standby blade takes over from the previously active blade and current SBC calls are preserved (and not disconnected as in the previous release).

8. Classifying IP Call to Proxy Set based on IP Address, Port, and Transport Type:

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides the ability to classify an IP call to a Proxy Set based on either its IP address, or its IP address, port, and transport type (e.g., UDP). As a Proxy Set can be defined with up to five Proxy IP addresses with or without associated ports and/or transport type, this provides greater flexibility in classifying a call with a Proxy Set. This feature is configured using the new parameter, *ClassificationInput* in the existing Proxy Set table (*ProxySet* parameter).

9. SIP-Dialog Rate Control:

Product			
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for SIP-dialog rate control, using the “token bucket” mechanism. The token bucket is a control mechanism that dictates the rate of SIP-dialog setups based on the presence of tokens in the bucket – a logical container that holds aggregate SIP dialogs to be accepted or transmitted. Tokens in the bucket are removed ("cashed in") for the ability to setup a dialog. Therefore, a flow can setup dialogs up to its peak burst rate if there are adequate tokens in the bucket and if the burst threshold is configured appropriately:

- Every SIP dialog setup request must attempt to take a token from the bucket.
- If there are no tokens, the request is dropped.
- New tokens are added to the bucket at a user-defined rate (token rate).
- If the bucket contains the maximum number of tokens, tokens to be added at that moment are dropped.

A token bucket is configured in the SBC Admission Control table (*SBCAdmissionControl* parameter), using the following new parameters:

- *Rate* = Rate at which tokens are added to the bucket (i.e., token rate). One token is added to the bucket every 1000/Rate milliseconds. The rate of dialog setups per second, or unlimited if set to 0 (default).
- *Max Burst* = Maximum tokens that can fill the bucket. At any given time, the bucket cannot contain more than this amount of tokens. The maximum burst size for the dialog setup rate, unlimited if set to 0 (default).

Dropped requests are replied with the 486 “Busy Here” SIP response. Dropped requests are not counted in the bucket.

10. Mediation without Transcoding:

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☐	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☐	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for mediation without transcoding. The device transparently relays RTP traffic (through Digital Signal Processing/DSP) and the following features are supported:

- SRTP-RTP, SRTP tunneling
- Remote media NAT traversal (RFC 4961)
- Broken connection notification
- RTCP XR statistics
- Rogue RTP filtering

11. Interworking SIP Diversion and History-Info Headers:

Product			
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for interworking between the SIP Diversion and History-Info headers. This is important, for example, to networks that support the Diversion header but not the History-Info header, or vice versa. Therefore, mapping between these headers is crucial for preserving the information in the SIP dialog regarding how and why (e.g., call redirection) the call arrived at a certain SIP UA.

This feature is configured in the IP Profile table (*IPProfile* parameter) using the following new parameters:

- *SBCDiversionMode* - defines the device's handling of the Diversion header:
- *SBCHistoryInfoMode* - defines the device's handling of the History-Info header:

The handling of the SIP Diversion and History-Info headers is described in the table below:

Parameter Value	SIP Header Present in Received SIP Message		
	Diversion	History-Info	Diversion and History-Info
HistoryInfoMode = Add **DiversionMode = Remove**	Diversion converted to History-Info. Diversion removed.	Not present.	Diversion added to History-Info. Diversion removed.

Parameter Value	SIP Header Present in Received SIP Message		
	Diversion	History-Info	Diversion and History-Info
HistoryInfoMode = Remove **DiversionMode = Add**	Not present.	History-Info converted to Diversion. History-Info removed.	History-Info added to Diversion. History-Info removed.
HistoryInfoMode = Disable **DiversionMode = Add**	Diversion converted to History-Info.	Not present.	Diversion added to History-Info.
HistoryInfoMode = Disable **DiversionMode = Add**	Not present.	History-Info converted to Diversion.	History-Info added to Diversion.
HistoryInfoMode = Add **DiversionMode = Add**	Diversion converted to History-Info.	History-Info converted to Diversion.	Headers are synced and sent.
HistoryInfoMode = Remove **DiversionMode = Remove**	Diversion removed.	History-Info removed.	Both removed.

12. GRUU Support According to RFC 5627:

Product			
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides support for Globally Routable User Agent (UA) URI (GRUU), according to RFC 5627. This is used for obtaining a GRUU from a registrar and for communicating a GRUU to a peer within a dialog. This support is provided by the existing parameter, *EnableGRUU*. In addition, this feature allows the device to act as a GRUU server for its SIP UA clients, providing them with public GRUU's, according to RFC 5627. The public GRUU provided to the client is depicted in the SIP Contact header parameters, "pub-gruu". Public GRUU remains the same over registration expirations. On the other SBC leg communicating with the Proxy/Registrar, the device acts as a GRUU client. The GRUU server feature is enabled by the new parameter, *SBCGruuMode*.

The device creates a GRUU value for each of its registered clients, which is mapped to the GRUU value received from the Proxy server. In other words, the created GRUU value is only used between the device and its clients (endpoints).

```
Public-GRUU: sip:userA@domain.com;gr=unique-id
```

- Obtaining a GRUU: The mechanism for obtaining a GRUU is through registrations. A UA can obtain a GRUU by generating a REGISTER request containing a Supported header field with the value “gruu”. The UA includes a “+sip.instance” Contact header parameter of each contact for which the GRUU is desired. This Contact parameter contains a globally unique ID that identifies the UA instance. The global unique ID is created from one of the following:

- If the REGISTER is per the device's client (endpoint), it is the MAC address concatenated with the phone number of the client.
- If the REGISTER is per device, it is the MAC address only.

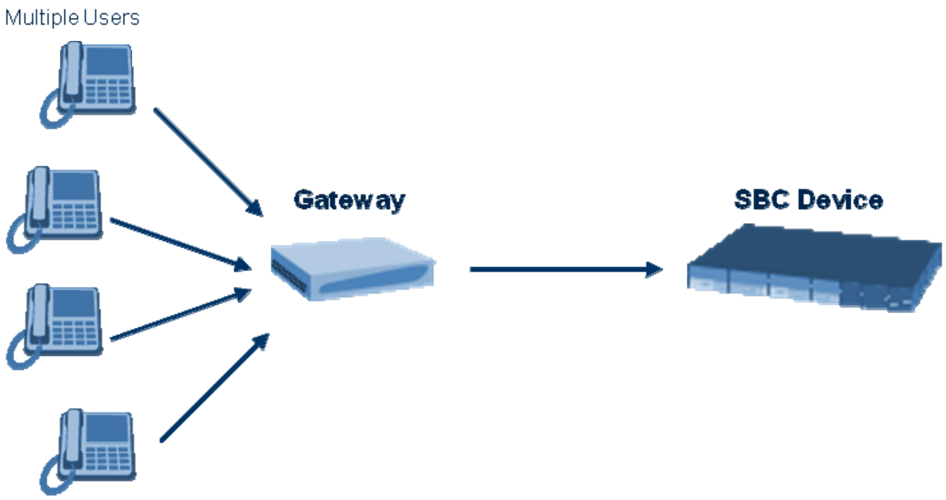
If the remote server doesn't support GRUU, it ignores the parameters of the GRUU. Otherwise, if the remote side also supports GRUU, the REGISTER responses contain the "gruu" parameter in each Contact header. This parameter contains a SIP or SIPS URI that represents a GRUU corresponding to the UA instance that registered the contact. The server provides the same GRUU for the same AOR and instance-id when sending REGISTER again after registration expiration. RFC 5627 specifies that the remote target is a GRUU target if its' Contact URL has the "gr" parameter with or without a value.

- Using GRUU: The UA can place the GRUU in any header field which can contain a URI. It must use the GRUU in the following messages: INVITE request, its 2xx response, SUBSCRIBE request, its 2xx response, NOTIFY request, REFER request and its 2xx response.

13. New IP Group Type "GATEWAY":

Product									
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for a new IP Group type–"GATEWAY"–defined in the IP Group table (*IPGroup* parameter). This is used for scenarios in which the SBC device receives requests to and from a gateway that represents multiple users, as shown below:



In previous releases, the IP Group could be defined as one of the following types:

- SERVER: Used when the destination address (configured by the Proxy Set – *ProxySet* parameter) of the IP Group such as an ITSP, a Proxy, an IP-PBX, or an Application server is known.
- USER: Represents a group of users (such as IP phones and softphones) where their location is dynamically obtained by the device, using the SIP Contact header, when REGISTER requests and responses traverse (or are terminated) by the device. These users are considered remote (far-end) users.

The “GATEWAY” type is necessary for requests representing multiple users, as the existing options above are not suitable:

- The IP Group cannot be defined as a SERVER since its destination address is unknown during configuration.
- The IP Group cannot be defined as a USER since the SIP Contact header of the incoming REGISTER does not represent a specific user. The Request-URI user part can change and therefore, the device is unable to identify an already registered user and therefore, adds an additional record to the database.

The IP address of the “GATEWAY” IP Group is obtained dynamically from the host part of the Contact header in the REGISTER request received from the IP Group. Therefore, routing to this IP Group is possible only once a REGISTER request is received. If a REGISTER refresh request arrives, the device updates the new location (i.e., IP address) of the IP Group. If the REGISTER fails, no update is performed. If an UN-REGISTER request arrives, the IP address associated with the IP Group is deleted and therefore, no routing to the IP Group is done.

The IP Group table also has a new read-only field–“Gateway Group Location”– which displays the current destination IP address of the IP Group.

14. **Minimum Session Expires (SIP Min-SE Header):**

Product									
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for configuring the minimum amount of time (in seconds) between session refresh requests in a dialog before the session is considered timed out. This value is sent in the SIP Min-SE header. This feature is configured using the new parameter, *SBCMinSE*. When set to zero (default), the SBC does not limit Session-Expires.

15. **Multiple RTP Media Streams per Call Session:**

Product									
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature provides support for multiple RTP media streams per SBC call session. Up to five different media types can be included in a session - audio (m=audio), video (m=video), text, (m=text), and fax (m=image). Therefore, this also allows the device to provide transcoding of various attributes in the SDP offer/answer (e.g., codec, port, and packetization time) per media type. If the device is unable to perform transcoding (for example, does not support the codec), it relays the SBC dialog transparently.

16. General SBC Configuration Enghancements:

Product									
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This release provides the following general SBC configuration enhancements:

- In Release 6.0, the IP address of the WAN interface had to be defined in the Data configuration section, and then once defined, it had to be assigned to the SIP application layer for the SBC configuration (using the *WANIPAddress* parameter). Now, in Release 6.2, there is no need to assign the WAN IP address in the SBC configuration section; it is acquired automatically from the Data section.
- In Release 6.0, the user had to configure port forwarding in the Data section for all SIP interfaces and Media Realms relating to the WAN interface. Now, in Release 6.2, port forwarding for the SIP interfaces and Media Realms are configured automatically.
- In Release 6.0, a “Static NAT” had to be configured in the Data section for all SIP interfaces and Media Realms relating to the WAN interface. Now, in Release 6.2, the Static NAT for SIP interfaces and Media Realms are configured automatically.
- In Release 6.0, it was forbidden to use the same port range for the WAN and LAN interfaces. For instance, the user couldn’t assign two SIP interfaces, one for LAN and one for WAN, using the same port (i.e. 5060). Now, in Release 6.2, this limitation no longer applies and these interfaces can be assigned the same ports.
- In Release 6.2, more than one VLAN is available on the WAN interface - one for media and control, and several VLANs for data. The user is required to choose the VLAN assigned to media and control. Note that it's not backward compatiable and the user MUST specify the WAN VLAN in the Multiple Interface page.
- To facilitate SBC configuration, Release 6.2 now provides a new “master” page - the new SRD page. This page allows the user to configure a new SRD and its parameters as well as assign SIP interfaces to the SRD. In addition, this page displays (read-only) all the IP Groups and Proxy Sets associated with the SRD.

1.4 Media New Features

The device supports the following new media features:

1. **Media Packet Forwarding:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☐	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☐	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☐	Gateway/GW	☒	SBC	☐	SAS

This feature provides support for UDP and RTP “aware” packet media streaming through a Media Forwarding session for the SBC application. This feature enhances the IP-to-IP forwarding capability by supporting UDP/RTP awareness. The following capabilities are included:

- Incoming Media latching
- NAT Traversal handling
- SRTP-to-RTP translation
- RTP statistics per endpoint in the SBC session
- Unknown RTP Payload Types handling
- Unknown codecs handling
- SRTP tunneling
- T.38 forwarding

2. **V.34 Fax Relay over T.38 Version 3:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☒	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☒	Gateway/GW	☐	SBC	☐	SAS

This feature provides support for ITU-T T.38 Version 3. This allows the transmission of V.34 fax over T.38, providing high fax transmission speeds and high fax transmission reliability. T.38 version 3 is enabled using the new parameter, *SIPT38Version*.

Note: To use V.34, the relevant DSP template must be used.

3. **G.722 Codec Support:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☒	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☒	Gateway/GW	☒	SBC	☐	SAS

This feature provides support for the G.722 speech codec, according to RFC 3551. G.722 was developed by ITU-T as a wideband codec with a bit rate of 64 kbps. This codec is configured using the *CodersGroup* parameter.

4. **Wideband AMR Codec Support:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☒	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☒	Gateway/GW	☒	SBC	☐	SAS

This feature provides support for the Adaptive Multi-Rate Wideband (AMR-WB) speech codec, according to RFC 3267. The AMR-WB speech codec was originally developed by 3GPP for GSM and 3G cellular systems. Similar to AMR, the AMR-WB codec is a multi-mode speech codec. AMR-WB supports nine wideband speech coding modes with bit rates ranging from 6.6 to 23.85 kbps. This codec is configured using the *CodersGroup* parameter.

1.5 PSTN New Features

The device supports the following new PSTN features:

1. **E1/T1 PSTN Interface:**

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☒	Gateway/GW	☐	SBC	☐	SAS

The device now supports a single E1/T1 PSTN port interface. This E1/T1 interface can be configured to any one of the following PSTN protocols: Transparent, CAS, or ISDN.

2. **Implicit Mode for Explicit Call Transfer (ECT):**

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☒	Gateway/GW	☐	SBC	☐	SAS

The device now supports Implicit ECT transfer for Euro ISDN BRI protocol (in addition to the existing Explicit ECT support). In Implicit ECT, the transfer is done between two calls on the same trunk. Typically, the Implicit mechanism is used for BRI and the Explicit mechanism for PRI.

3. T310 Timer Configuration for ISDN Variant NI2:

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☒	Gateway/GW	☐	SBC	☐	SAS

The device now supports configuration of the T310 timer for the ISDN variant National ISDN with sub variant 2 (NI2). This solution is similar to the T310 timer for DMS and Euro ISDN. The T310 timer is the timer that is set when the ISDN interface receives a Call Proceeding message. If no Alerting, Progress, or Connect message is received within the duration of T310, the call clears.

The T310 timer can be configured using the existing parameter, *ISDNTimerT310*. When set to 0, the timer uses the default timer according to the protocol's specifications.

4. Removing Validation Check of UUIE Data:

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☒	Gateway/GW	☐	SBC	☐	SAS

The device now supports a bit-field that determines the behavior of the Q.931 protocol. This is configured per trunk, using the new parameter, *ISDNNSBehaviour2*. The relevant bit is NS_BEHAVIOUR2_ANY_UUI (0x0008). When this bit is set, any User to User Information Element (UUIE) is accepted for any protocol discriminator. This feature is useful for interoperability with non-standard switches.

1.6 Networking New Features

The device supports the following new networking features:

1. **ARIA Encryption Algorithm for TLS:**

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☐	EMS	☐	CLI

Application					
☒	Gateway/GW	☒	SBC	☐	SAS

The device now supports ARIA algorithm cipher encryption for Transport Layer Security (TLS) connections. ARIA is a symmetric key block cipher algorithm standard developed by the Korean National Security Research Institute. To support this encryption, the existing *HTTPSCipherString* parameter must be set to a value which includes ARIA or ALL.

2. **VoIP Firewall:**

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☐	EMS	☐	CLI

Application					
☒	Gateway/GW	☒	SBC	☐	SAS

The device now supports the configuration of inbound access (block or allow) firewall rules for the VoIP interface. This feature is configured using the existing Firewall Settings table (*AccessList* parameter).

3. **VoIP Firewall per Network Interface:**

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☒	Gateway/GW	☒	SBC	☐	SAS

The device now supports the configuration of firewall access rules (block or allow) per VoIP network interface. These are the VoIP interfaces as defined in the Multiple Interface table (*InterfaceTable* parameter). The firewall rules are configured in the existing Firewall Settings table (*AccessList* parameter).

4. **LAN Port Monitoring:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

Application					
☒	Gateway/GW	☒	SBC	☐	SAS

The device now supports the monitoring of traffic traversing its LAN ports (i.e., Port Mirroring). This includes monitoring of egress and/or ingress traffic. This feature is useful for analyzing traffic or debugging network problems. The new CLI commands, **`port monitor`** and **`show data port-monitoring`** are used for displaying this information.

5. Default Gateway per IP Interface:

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☒	CLI
Application									
☒	Gateway/GW	☒	SBC	☐	SAS				

This feature provides enhanced routing with its support for multiple default gateways. Each IP network interface (whether it's Control, Media, or OAMP) can now be defined with a default gateway. This is configured in the existing Multiple Interface table (*InterfaceTable* parameter).

6. Static Routing Table Enhancements:

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☒	CLI
Application									
☒	Gateway/GW	☒	SBC	☐	SAS				

The device's IP Routing table (*StaticRouteTable* parameter) has been enhanced to provide offline configuration of IP routing rules. The rules in this table can now be associated with an IP interface defined in the Multiple Interface table (rather than the previously used index). Therefore, the routing decision is now based on the source subnet/VLAN. In the previous release, the routing decision was based on the destination IP address only and therefore, for example, packets from the Media subnet could be routed to the Control subnet and vice versa. This enhanced routing behavior prevents cases where static routes are lost and simplifies the static routes configuration for Control and Media subnets.

In addition, a new table column has been added to provide the current status of a configured route ("Active" or "Inactive"). After adding a new route, the device attempts to apply the route. If the operation fails, the route is marked as "Inactive" until it can become active (following a change in the routing/interface tables).

7. Increase in Maximum Call Control/Media Interfaces:

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☐	Mediant 800 MSBG	☐	Mediant 1000 MSBG
☐	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

Application					
☒	Gateway/GW	☒	SBC	☐	SAS

The device now supports the configuration of up to 31 Control/Media interfaces (as compared to 15 in the previous release). Together with the single OAMP interface, a total of 32 IP interfaces can be configured. This is done in the Multiple Interface table (*InterfaceTable* parameter).

8. Remote GARP Detection of Media Streams (VoIP)

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☐	EMS	☐	CLI

Application					
☒	Gateway/GW	☒	SBC	☐	SAS

The device now supports automatic change of the remote Ethernet MAC address in sent (Tx) packets of all relevant active media channels upon receiving Gratuitous Address Resolution Protocol (GARP) packet. This is configured in the existing parameter, *EnableDetectRemoteMACChange* (options 2 and 3).

9. Internet Protocol Version 6 (IPv6) Support:

Product									
☐ MP-11x					☐ MP-124				
☐ Mediant 600					☐ Mediant 1000				
☒ Mediant 800 MSBG					☐ Mediant 1000 MSBG				
☐ Mediant 2000									
☐ Mediant 3000/TP-6310					☐ Mediant 3000 HA/TP-6310				
☐ Mediant 3000/TP-8410					☐ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☒	CLI
Application									
☒	Gateway/GW	☒	SBC	☐	SAS				

The device now supports the configuration of IPv6 Internet Layer protocol IP interfaces (defined using the *InterfaceTable* parameter), which is based on the definition of a 128-bit address (as opposed to 32 bits for IPv4). The following table lists IPv6-related RFCs that are currently supported by the device (some only partially supported).

- RFC 1981 Path MTU Discovery for IP version 6
- RFC 2373 IP Version 6 Addressing Architecture
- RFC 2374 IPv6 Aggregatable Global Unicast Address Format
- RFC 2375 IPv6 Multicast Address Assignments
- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461 Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2463 Internet Control Message Protocol (ICMPv6)
- RFC 2464 Transmission of IPv6 Packets over Ethernet
- RFC 2474 Definition of the Differentiated Services Field (DSField) in the IPv4 & IPv6 Headers
- RFC 2553 Basic Socket Interface Extensions for IPv6
- RFC 2710 Multicast Listener Discovery (MLD) for IPv6
- RFC 2893 Transition Mechanisms for IPv6 Hosts and Routers.
- Note: Tunneling mechanisms are not supported.
- RFC 3266 Support for IPv6 in Session Description Protocol (SDP)
- RFC 3484 Default Address Selection for Internet Protocol version 6 (IPv6)
- RFC 4193 Unique Local IPv6 Unicast Addresses

For more information on these RFC's, contact AudioCodes.

1.7 Data-Router New Features

The device supports the following new data-router features:

1. **Dual WAN over T1 Interface Ports:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☒	Web	☒	INI	☒	SNMP	☐	EMS	☒	CLI

The device now supports two physical WAN T1 links, thereby allowing a bandwidth of up to 3 Mbps. The T1 WAN connection is through a Dual T1 line interface (according to ANSI T1.403-1999). The device uses its Dual T1 WAN Data Service Unit/Channel Service Unit (DSU/CSU) port interface to transmit and receive data using IP over Point-to-Point Protocol (PPP) framing (up to two separate links), IP over High-Level Data Link Control (HDLC) framing (up to two separate links), or bundling both physical links into a single logical link using IP over Multilink Point-to-Point Protocol (MLP) framing (RFC 1717).

2. **BER Test for T1 WAN Interface:**

Product			
☐	MP-11x	☐	MP-124
☐	Mediant 600	☐	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☐	Mediant 2000		
☐	Mediant 3000/TP-6310	☐	Mediant 3000 HA/TP-6310
☐	Mediant 3000/TP-8410	☐	Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

The device now supports bit error rate (BER) testing on the T1 WAN interface for the far-end transmission link. The BER Test is done by generating and detecting both pseudorandom and repeating bit patterns. The test is enabled using the `ber-test` CLI command.

3. **Local-line Loopback on T1 WAN Interface:**

Product									
☐ MP-11x					☐ MP-124				
☐ Mediant 600					☐ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☐ Mediant 2000									
☐ Mediant 3000/TP-6310					☐ Mediant 3000 HA/TP-6310				
☐ Mediant 3000/TP-8410					☐ Mediant 3000 HA/TP-8410				
Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

The device now supports local-line loopback on the T1 WAN interface. In this loopback, packets from the Tx line interface connect to the Rx line interface. The maximum time of this loopback is user-defined. This featured is enabled and configured using the `loopback` CLI command.

4. **WAN Ethernet Port Settings (Speed and Duplex Mode):**

Product									
☐ MP-11x					☐ MP-124				
☐ Mediant 600					☐ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☐ Mediant 2000									
☐ Mediant 3000/TP-6310					☐ Mediant 3000 HA/TP-6310				
☐ Mediant 3000/TP-8410					☐ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

The device now supports the configuration of link speed and duplex mode of the WAN Ethernet port:

- Port speed: 10BaseT, 100Base-T, 1000Base-T, or autonegotiation
- Duplex mode: half-duplex, full-duplex, or autonegotiation

5. **IPSec Crypto CLI:**

Product									
☐ MP-11x					☐ MP-124				
☐ Mediant 600					☐ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☐ Mediant 2000									
☐ Mediant 3000/TP-6310					☐ Mediant 3000 HA/TP-6310				
☐ Mediant 3000/TP-8410					☐ Mediant 3000 HA/TP-8410				
Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

The device now supports the configuration of IPSec tunneling using "crypto" CLI commands. The main CLI commands include the following:

- **`crypto isakmp key`**: defines a preshared authentication key

- **`crypto isakmp policy`**: defines an Internet Key Exchange (IKE) policy
- **`crypto ipsec transform-set`**: defines a transform set of acceptable combination of security protocols and algorithms
- **`crypto map`**: creates or modifies a crypto map entry and enters the crypto map configuration mode

6. **Ethernet in the First Mile (EFM) for SHDSL WAN Interface:**

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

The device's SHDSL WAN interface now supports the EFM standard. EFM provides a single (end-to-end) approach for transmitting Ethernet traffic between the WAN and LAN over different topologies such as copper and fiber optic point-to-point networks. This typically results in greater broadband access and reduces the bottleneck in the network.

7. **Virtual Routing and Forwarding (VRF) Lite:**

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

The device now supports Virtual Routing and Forwarding (VRF). This technology allows multiple instances of a routing table to co-exist within the same router at the same time. The device's VRF feature allows interfaces to be clustered into a VRF to provide segregated routing domains. The VRF feature uses the device's single physical router as multiple logical routers (up to 32). Each VRF is associated with its own routing table. When creating fully separated logical routers on the same physical router, every interface can be mapped to a specified VRF and static routes can be added to it. The main CLI command for configuring VRF is **`ip vrf`**.

Note: Some features are available only on the default, unnamed, VRF. These include, amongst others, BGP, OSPF, RIP, Management interfaces (Web, CLI and SNMP), and SIP (when using the device's VoIP component). For a complete list of features supported only on the default VRF, please contact AudioCodes.

1.8 Security New Features

The device supports the following new security feature:

1. **ARIA Encryption Algorithm for SRTP:**

Product					
☐ MP-11x			☐ MP-124		
☐ Mediant 600			☐ Mediant 1000		
☐ Mediant 800 MSBG			☐ Mediant 1000 MSBG		
☐ Mediant 2000					
☒ Mediant 3000/TP-6310			☒ Mediant 3000 HA/TP-6310		
☒ Mediant 3000/TP-8410			☒ Mediant 3000 HA/TP-8410		
Management Protocol					
☒ Web		☒ INI		☒ SNMP	
☒ EMS		☐ CLI			

This feature provides support for the ARIA algorithm cipher encryption for SRTP. This is an alternative option to the existing support for the AES algorithm. ARIA is a symmetric key block cipher algorithm standard developed by the Korean National Security Research Institute. The ARIA offered suite supports 128-bit and 192-bit key encryption sizes with HMAC SHA-1 cryptographic hash function.

ARIA encryption is enabled by the new parameter, *AriaProtocolSupport*. The required ARIA crypto suite for SRTP is according to the existing parameter, *SRTPofferedSuites*.

For ARIA encryption of SRTP, the device must be installed with the relevant Software Upgrade Feature Key.

1.9 Infrastructure New Features

The device supports the following new infrastructure features:

1. **Enhanced Syslog Message Management using Facility Levels:**

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☒	EMS	☐	CLI

This feature supports the configuration of the Facility level (0 through 7) for the device's Syslog messages, according to RFC 3164. This feature is useful, for example, to customers who collect the device's and other equipments' Syslog messages at one single server. The device's Syslog messages can easily be identified and distinguished from other Syslog messages by its Facility level. Therefore, in addition to filtering Syslog messages according to IP address, the messages can be filtered according to Facility level.

The Facility level is configured by the new parameter, *SyslogFacility*, which provides the following levels:

- 16 - local use 0 (local0) - default
- 17 - local use 1 (local1)
- 18 - local use 2 (local2)
- 19 - local use 3 (local3)
- 20 - local use 4 (local4)
- 21 - local use 5 (local5)
- 22 - local use 6 (local6)
- 23 - local use 7 (local7)

2. **Power over Ethernet (PoE) Port Status:**

Product									
☐ MP-11x					☐ MP-124				
☐ Mediant 600					☐ Mediant 1000				
☒ Mediant 800 MSBG					☐ Mediant 1000 MSBG				
☐ Mediant 2000									
☐ Mediant 3000/TP-6310					☐ Mediant 3000 HA/TP-6310				
☐ Mediant 3000/TP-8410					☐ Mediant 3000 HA/TP-8410				
Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

This feature provides Power over Ethernet (PoE) status indication when an IP Phone is connected to one of the device's LAN ports. This status is provided by the CLI `GetPOEPortStatusCmd` command, which when run, displays the status.

1.10 Management and Provisioning New Features

1.10.1 Web New Features

The device supports the following new Web interface features:

1. **New Web Navigation Tree:**

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides an improved hierarchical structure of the **Configuration** tab's menus in the Navigation tree of the Web interface. The **Configuration** tab is now organized according to the following main folders:

- **System:** contains the system-related configuration items
- **VoIP:** contains the VoIP-related configuration items
- **Data:** contains the data-routing related configuration items – applicable only to Mediant 800 MSBG and Mediant 1000 MSBG

2. **Management Web Pages Re-design:**

Product									
☒ MP-11x					☒ MP-124				
☒ Mediant 600					☒ Mediant 1000				
☒ Mediant 800 MSBG					☒ Mediant 1000 MSBG				
☒ Mediant 2000									
☒ Mediant 3000/TP-6310					☒ Mediant 3000 HA/TP-6310				
☒ Mediant 3000/TP-8410					☒ Mediant 3000 HA/TP-8410				
Management Protocol									
☒	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

The Web interface's management pages have been re-designed as follows:

- The configuration of management elements and applications (such as RADIUS, Telnet, and SSH) are now located in the Navigation tree under the **Configuration** tab in the new **System** menu.
- The active alarms are now located in the Navigation tree under the **Status** tab in a new folder **Carrier Grade Alarms** under the **System** menu.
- The maintenance and software upgrade pages are now located under the **Maintenance** tab.

3. **Reorganization of SIP Menus in Web Navigation Tree:**

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides an improved hierarchical structure of the SIP-related menus and items in the Navigation tree of the Web interface. The SIP menus and items are now organized according to functionality and feature and therefore, can now easily be found due to their improved logical grouping and location in the Navigation tree.

4. **Home Page Display of Device State:**

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides a new status field–“Gateway Operational State”–in the General Information pane on the Web interface’s Home page. This status field indicates the device’s operational state as follows:

- "LOCKED" – the device is locked (i.e. no new calls are accepted)
- "UNLOCKED" – the device is not locked
- “SHUTTING DOWN” – the device is currently shutting down

1.10.2 SNMP New Features

The device supports the following new Simple Network Management Protocol (SNMP) features:

1. **ini File Configuration through SNMP:**

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☐	Web	☐	INI	☒	SNMP	☐	EMS	☐	CLI

This feature allows the configuration of *ini* file parameters that are not supported by the Element Management System (EMS) tool, by using the existing acSysGenericINILine SNMP parameter. This feature is useful for parameters that are currently not supported by regular SNMP and where the user does not want to use the external *ini* file.

To enter more than one line, the character set “$@$” must be added between lines of *ini* file parameter settings.

2. **Engine ID Configuration:**

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☐	Web	☐	INI	☒	SNMP	☐	EMS	☐	CLI

This feature allows the configuration of the SNMP Engine ID for SNMP v2/v3 agents, by using the new *ini* file parameter, *SNMPEngineIDString*. This parameter is configured as a string value of up to 36 characters and needs a device reset to take effect. The Engine ID is used for authenticating a user attempting to access the SNMP agent on the device.

The default value is 00:00:00:00:00:00:00:00:00:00:00:00 12 hex characters. The provided key must be set with 12 hex values delimited by a colon (“:”).

If the supplied key does not pass validation of the 12 hex values or if it is set with the default value, the engine ID will be generated according to RFC 3411.

Note: Before setting this parameter, all SNMPv3 users must be deleted, otherwise the configuration is ignored.

1.10.3 CLI New Features

The device supports the following new command-line interface (CLI) features:

1. **Main CLI Configuration Modes:**

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

This feature provides support for three main CLI configuration modes in which the device can be configured. These include VoIP, system, and data. To enter one of these modes, the following commands must be run:

- **`configure voip`** (or **`conf v`**) – accesses the VoIP configuration mode
- **`configure system`** (or **`conf s`**) – accesses the System configuration mode
- **`configure data`** (or **`conf d`**) – accesses the Data configuration mode

2. **CLI show Command:**

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☒	CLI

This feature provides enhanced functioning of the CLI **`show`** command for displaying the status of the device according to the three main CLI configuration modes - VoIP, system, and data.

To view the relevant status, the following commands must be run:

- **`show voip`** <command> - displays VoIP status according to the available <command> command (for an explanation, run **`show voip ?`**)
- **`show system`** <command> - displays system status according to the available <command> command (for an explanation, run **`show system ?`**)
- **`show data`** <command> - displays data status according to the available <command> command (for an explanation, run **`show data ?`**)

Note: The **`show`** commands can be accessed from any configuration mode, by using the **`do`** command, for example, **`do show voip`** <command>.

1.10.4 SSH New Features

The device supports the following new Secure Shell (SSH) features:

1. **RSA-2048 Public-Key Encryption for SSH:**

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☒	Web	☒	INI	☒	SNMP	☐	EMS	☐	CLI

The device now supports the generation and handling of 2048-bit RSA public-key encryption algorithms for Secure Shell (SSH). This feature is configured using the new parameter, *TLSPkeySize*. Once this parameter is set to 2048, new self-signed certificates are generated with 2048-bit keys.

2. **Maximum SSH Login Attempts:**

Product									
☒	MP-11x				☒	MP-124			
☒	Mediant 600				☒	Mediant 1000			
☒	Mediant 800 MSBG				☒	Mediant 1000 MSBG			
☒	Mediant 2000								
☒	Mediant 3000/TP-6310				☒	Mediant 3000 HA/TP-6310			
☒	Mediant 3000/TP-8410				☒	Mediant 3000 HA/TP-8410			
Management Protocol									
☐	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

The device now supports the configuration of the maximum allowed SSH login attempts when entering an incorrect password by an administrator. If this maximum is attained, the SSH session is rejected. This feature is configured by the new parameter, *SSHMaxLoginAttempts*.

3. **SSH Last Login:**

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☒	INI	☐	SNMP	☐	EMS	☐	CLI

The device now supports the display in SSH sessions of the time and date of the last SSH login. The SSH login message displays the number of unsuccessful login attempts since the last successful login. To enable or disable this message the new parameter, *SSHEnableLastLoginMessage* is used. Note that the last login information is cleared when the device is reset.

4. **Maximum Simultaneous SSH Sessions:**

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☒	INI	☒	SNMP	☐	EMS	☐	CLI

The device now supports the configuration of the maximum number of allowed simultaneous SSH sessions (up to two). This feature is configured by the new parameter, *SSHMaxSessions*.

1.10.5 Utilities New Features

The device supports the following new utilities feature:

1. **Running DConvert from Command Line:**

Product			
☒	MP-11x	☒	MP-124
☒	Mediant 600	☒	Mediant 1000
☒	Mediant 800 MSBG	☒	Mediant 1000 MSBG
☒	Mediant 2000		
☒	Mediant 3000/TP-6310	☒	Mediant 3000 HA/TP-6310
☒	Mediant 3000/TP-8410	☒	Mediant 3000 HA/TP-8410

Management Protocol									
☐	Web	☐	INI	☐	SNMP	☐	EMS	☐	CLI

This feature provides a new software version of the TrunkPack Downloadable Conversion (DConvert) utility which can be run from a command line. This is a separate executable, called 'dccmd'. The 'dccmd' supports only the handling of secured *ini* file and dial plan file.

1.11 New Parameters

This section describes the new parameters for Release 6.2. The *ini* file parameter is enclosed in square brackets and if a corresponding Web interface parameter exists, then this parameter appears above it.

1.11.1 SIP New Parameters

This section describes the new SIP parameters for Release 6.2.

1.11.1.1 SIP General Parameters

The table below describes the new general SIP parameters for Release 6.2. These parameters are applicable to the device's Gateway and SBC applications.

Table 1-3: New SIP General Parameters for Release 6.2

Parameter	Description
Max SIP Message Length [KB] **[MaxSIPMessageLength]**	Defines the maximum size (in Kbytes) allowed for each SIP message that can be sent over the network. Messages exceeding this user-defined size are rejected by the device. The valid value range is 1 to 50. The default is 50.
Transcoding Mode **[IP2IPTranscodingMode]**	Defines the voice transcoding mode (media negotiation) between two user agents for the IP-to-IP application. ▪ **[0]** Only if Required = Do not force. Many of the media settings (such as gain control) are not implemented on the voice stream. The device passes packets RTP to RTP without any processing. ▪ **[1]** Force = Force transcoding on outgoing IP leg. The device interworks the media by implementing DSP transcoding. (default)
Aria Protocol Support **[AriaProtocolSupport]**	Enables ARIA crypto suite support. ▪ **[0]** Disable = ARIA support is disabled (default). ▪ **[1]** Enable = ARIA support is enabled. For configuring the ARIA bit-key size (128 or 192 bit), use the parameter *SRTPofferedSuites*.

Parameter	Description
Static NAT Table	
[NATTranslation]	This ini file table parameter defines multiple NATs for SIP control and RTP media using Static NAT Rules. This table creates NAT rules for translating source IP address per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses. This allows, for example, the separation of VoIP traffic between different ISTP's, and topology hiding (of internal IP addresses to the "public" network). Each IP interface (configured in the Multiple Interface table - InterfaceTable parameter) can be associated with a NAT rule in this table, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range). The format of this parameter is as follows: [NATTranslation] FORMAT NATTranslation_Index = NATTranslation_SourceIPInterfaceName, NATTranslation_TargetIPAddress, NATTranslation_SourceStartPort, NATTranslation_SourceEndPort, NATTranslation_TargetStartPort, NATTranslation_TargetEndPort; [\NATTranslation] Where: • SourceIPInterfaceName is the name of the IP interface as defined in the Multiple Interface table. • TargetIPAddress is the global IP address. • TargetStartPort and TargetEndPort is the port range (1-66535) of the global address. • SourceStartPort and SourceEndPort is the port range (1-66535)of the IP interface. **Note:** ▪ This table can include up to 32 indices. ▪ The device's priority method for performing NAT is as follows (not relevant for SBC application): ▪ Uses an external STUN server (STUNServerPrimaryIP parameter) to assign a NAT address for all interfaces. ▪ Uses the StaticNATIP parameter to define one NAT IP address for all interfaces. ▪ Uses the NATTranslation parameter to define NAT per interface. ▪ If NAT is not configured (by any of the above-mentioned methods), the device sends the packet according to its IP address defined in the Multiple Interface table. ▪ If the StaticNATIP parameter is not configured and the WANIPAddress parameter is configured, then a NAT rule is automatically added to this table with an IP address defined for WANIPaddress and a port range of 0-65535.

1.11.1.2 SIP Gateway Parameters

The table below describes the new SIP Gateway application parameters for Release 6.2.

Table 1-4: New SIP Gateway Parameters for Release 6.2

Parameter	Description
Add Empty Authorization Header **[EmptyAuthorizationHeader]**	Determines whether the SIP Authorization header is included in initial registration (REGISTER) requests sent by the device. ▪ **[0]** Disable (default) ▪ **[1]** Enable The Authorization header carries the credentials of a user agent (UA) in a request to a server. The sent REGISTER message populates the Authorization header with the following parameters: ▪ username - set to the value of the private user identity ▪ realm - set to the domain name of the home network ▪ uri - set to the SIP URI of the domain name of the home network ▪ nonce - set to an empty value ▪ response - set to an empty value For example: `Authorization: Digest username=alice_private@home1.net, realm="home1.net", nonce="", response="e56131d19580cd833064787ecc"` **Note:** This registration header is according to the IMS 3GPP TS24.229 and PKT-SP-24.220 specifications.

Add initial Route Header **[InitialRouteHeader]**	Determines whether the SIP Route header is included in initial registration or re-registration (REGISTER) requests sent by the device.
	▪ **[0]** Disable (default)
	▪ **[1]** Enable
	When the device sends a REGISTER message, the Route header includes either the Proxy's FQDN or the IP address and port according to the configured Proxy Set, for example:
	`Route: <sip:10.10.10.10;lr;transport=udp>`
	or
	`Route: <sip: pcscf-gm.ims.rr.com;lr;transport=udp>`

[TrunkStatusReportingMode]	Determines whether the device responds to SIP OPTIONS for Trunk Group #1. ▪ **[0]** Disable (default) ▪ **[1]** Enable = If all the trunks pertaining to Trunk Group #1 are down or busy, the device does not respond to received SIP OPTIONS

Parameter	Description
[EnableSDPVersionNegotiation]	This feature enables the flexibility of ignoring a new SDP re-offer (from the media negotiation perspective) in certain scenarios (such as session expires). According to RFC 3264, once an SDP session is established, a new SDP offer is considered a new offer only when the SDP origin value is incremented. In scenarios such as session expires, SDP negotiation is irrelevant and thus, the origin field is not changed. Even though some SIP devices don't follow this behavior and don't increment the origin value even in scenarios where they want to re-negotiate, the device can now assume that the remote party operates according to RFC 3264, and in cases where the origin field is not incremented, the device does not re-negotiate SDP capabilities. ▪ **[0]** Disable = The device negotiates any new SDP re-offer, regardless of the origin field (default). ▪ **[1]** Enable = The device negotiates only an SDP re-offer with an incremented origin field.
[FacilityTrace]	Enables ISDN traces of Facility Information Elements (IE) for ISDN call diagnostics. This allows you to trace all the parameters contained in the Facility IE and view them in the Syslog. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** For this feature to be functional, the GWDebugLevel parameter must be enabled.
[PerformAdditionalIP2TELDestinationManipulation]	Enables additional destination number manipulation for IP-to-Tel calls. ▪ **[0]** Disable (default) ▪ **[1]** Enable The additional manipulation is done on the initially manipulated destination number, and this additional rule is also configured in the manipulation table (*NumberMapIP2Tel* parameter). This enables you to configure only a few manipulation rules for complex manipulation (that generally require many rules).
[PerformAdditionalIP2TELSourceManipulation]	Enables additional source number manipulation for IP-to-Tel calls. ▪ **[0]** Disable (default) ▪ **[1]** Enable The additional manipulation is done on the initially manipulated source number, and this additional rule is also configured in the manipulation table (*SourceNumberMapIP2Tel* parameter). This enables you to configure only a few manipulation rules for complex manipulation (that generally require many rules).
[ReplaceCallingWithRedirectNumber]	Enables replacing the calling number with the redirect number in ISDN-to-IP calls. When such a replacement occurs, the calling name is deleted and left blank. The outgoing INVITE message does not include the redirect number that was used to replace the calling number. The replacement is done only if a redirect number is present in the incoming call. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable

Parameter	Description

QoS statistics in SIP Release Call
[QoSStatistics]
	Determines whether the device includes call quality of service (QoS) statistics in SIP BYE and SIP 200 OK response to BYE, using the proprietary SIP header, X-RTP-Stat.
	▪ **[0]** = Disable (default)
	▪ **[1]** = Enable
	The X-RTP-Stat header provides the following statistics:
	▪ Number of received and sent voice packets
	▪ Number of received and sent voice octets
	▪ Received packet loss, jitter (in ms), and latency (in ms)
	The X-RTP-Stat header contains the following fields:
	▪ PS=<voice packets sent>
	▪ OS=<voice octets sent>
	▪ PR=<voice packets received>
	▪ OR=<voice octets received>
	▪ PL=<receive packet loss>
	▪ JI=<jitter in ms>
	▪ LA=<latency in ms>
	Below is an example of the X-RTP-Stat header in a SIP BYE message:
	`BYE sip:302@10.33.4.125 SIP/2.0`
	`Via: SIP/2.0/UDP 10.33.4.126;branch=z9hG4bKac2127550866`
	`Max-Forwards: 70`
	`From: <sip:401@10.33.4.126;user=phone>;tag=1c2113553324`
	`To: <sip:302@company.com>;tag=1c991751121`
	`Call-ID: 991750671245200001912@10.33.4.125`
	`CSeq: 1 BYE`
	`X-RTP-Stat:`
	`PS=207;OS=49680;;PR=314;OR=50240;PL=0;JI=600;LA=40;`
	`Supported: em,timer,replaces,path,resource-priority`
	`Allow:`
	`REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REF`
	`ER,INFO,SUBSCRIBE,UPDATE`
	`User-Agent: Sip-Gateway-/v.6.2A.008.006`
	`Reason: Q.850 ;cause=16 ;text="local"`
	`Content-Length: 0`

RTP-Only Mode	
RTP Only Mode **[RTPOnlyMode]**	Enables the device to start sending and/or receiving RTP packets to and from remote endpoints without the need to establish a SIP session. The remote IP address is determined according to the Outbound IP Routing table. The port is the same port as the local RTP port (configured by the parameter *BaseUDPPort* and the channel on which the call is received). ▪ **[0]** Disable (default) ▪ **[1]** Transmit & Receive = Send and receive RTP ▪ **[2]** Transmit Only= Send RTP only ▪ **[3]** Receive Only= Receive RTP only **Notes:** ▪ To configure the RTP Only mode per trunk, use the RTPOnlyModeForTrunk_ID. ▪ If per trunk configuration (using *RTPOnlyModeForTrunk*) is set to a

Parameter	Description
	value other than the default, the *RTPOnlyMode* parameter value is ignored.
[RTPOnlyModeForTrunk_ID]	Enables the device to start sending and/or receiving RTP packets to and from remote endpoints without the need to establish a SIP session. This is configured per trunk. The remote IP address is determined according to the 'Outbound IP Routing' table. The port is the same port as the local RTP port (configured by the parameter *BaseUDPPort* and the channel on which the call is received). ▪ **[-1]** Not Configured = use the global parameter (*RTPOnlyMode*) value for all channels (default) ▪ **[0]** Disable ▪ **[1]** Transmit & Receive = send and receive RTP packets ▪ **[2]** Transmit Only = send RTP packets only ▪ **[3]** Receive Only = receive RTP packets only **Note:** The *ID* in the *ini* file parameter depicts the trunk number, where 0 is the first trunk.
AMD Parameters	
Web: Answer Machine Detector Sensitivity Parameter Suit **[AMDSensitivityParameterSuit]**	Determines the AMD parameter suit that you want the device to use. ▪ **[0]** = USA Parameter suite with normal detection sensitivity resolution (8 sensitivity levels, from 0 to 7). The level is configured by the *AMDSensitivityLevel* parameter. (default) ▪ **[1]** = USA Parameter Suite with high detection sensitivity resolution (16 sensitivity levels, from 0 to 15). The level is configured by the *AMDSensitivityLevel* parameter. ▪ **[2]**-**[3]** **=** Other countries parameter suites with up to 16 sensitivity levels. **Note:** This parameter replaces the existing *AMDSensitivityResolution* parameter.
Web: AMD Sensitivity Level **[AMDSensitivityLevel]**	Determines the AMD detection sensitivity level of the selected AMD parameter suite. The valid value range is 0 (for best detection of an answering machine) to 15 (for best detection of a live call). The default value is 8. **Note:** This parameter replaces the existing *AMDDetectionSensitivityHighResolution* parameter.
[AMDMaxGreetingTime]	Maximum greeting time
[AMDMaxPostGreetingSilenceTime]	Maximum duration of silence from after the greeting time is over (defined by AMDMaxGreetingTime) until the AMD decision.
[AMDSensitivityFileName]	Name of the AMD Sensitivity auxiliary file.
[AMDSensitivityFileUrl]	URL path to the AMD Sensitivity file for download from a remote server.

Parameter	Description
CRLF Keep-Alive Mode Parameters	
[UsePingPongKeepAlive]	Determines whether the carriage-return and line-feed sequences (CRLF) Keep-Alive mechanism, according to RFC 5626 “Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)” is used for reliable, connection-orientated transport types such as TCP. ▪ **[0]** Disable (default) ▪ **[1]** Enable The SIP user agent/client (i.e., device) uses a simple periodic message as a keep-alive mechanism to keep their flow to the proxy or registrar alive (used for example, to keep NAT bindings open). For connection-oriented transports such as TCP/TLS this is based on CRLF. This mechanism uses a client-to-server "ping" keep-alive and a corresponding server-to-client "pong" message. This ping-pong sequence allows the client, and optionally the server, to tell if its flow is still active and useful for SIP traffic. If the client does not receive a pong in response to its ping, it declares the flow “dead” and opens a new flow in its place. In the CRLF Keep-Alive mechanism the client periodically sends a double-CRLF (the "ping") then waits to receive a single CRLF (the "pong"). If the client does not receive a "pong" within an appropriate amount of time, it considers the flow failed. **Note:** The device sends a CRLF message to the Proxy Set only if the Proxy Keep-Alive feature (*EnableProxyKeepAlive* parameter) is enabled and its transport type is set to TCP or TLS. The device first sends a SIP OPTION message to establish the TCP/TLS connection and if it receives any SIP response, it continues sending the CRLF keep-alive sequences.
Ping-Pong Keep-Alive Time **[PingPongKeepAliveTime]**	Defines the periodic interval (in seconds) after which a “ping” (double-CRLF) keep-alive is sent to a proxy/registrar, using the CRLF Keep-Alive mechanism. The default range is 5 to 2,000,000. The default is 120. The device uses the range of 80-100% of this user-defined value as the actual interval. For example, if the parameter value is set to 200 sec, the interval used is any random time between 160 to 200 seconds. This prevents an “avalanche” of keep-alive by multiple SIP UAs to a specific server.
RTCP XR Parameters	
Enable RTCP XR **[VQMonEnable]**	Enables voice quality monitoring and RTCP XR, according to draft-ietf-sipping-rtcp-summary-13. ▪ **[0]** Disable = Disable (default) ▪ **[1]** Enable = Enables **Note:** For this parameter to take effect, a device reset is required.
Minimum Gap Size **[VQMonGMin]**	Voice quality monitoring - minimum gap size (number of frames). The default is 16.
Burst Threshold **[VQMonBurstHR]**	Voice quality monitoring - excessive burst alert threshold. if set to -1 (default), no alerts are issued.
Delay Threshold **[VQMonDelayTHR]**	Voice quality monitoring - excessive delay alert threshold. if set to -1 (default), no alerts are issued.

Parameter	Description
R-Value Delay Threshold **[VQMonEOCRValTHR]**	Voice quality monitoring - end of call low quality alert threshold. if set to -1 (default), no alerts are issued.
RTCP Packet Interval **[RTCPInterval]**	Defines the time interval (in msec) between adjacent RTCP reports. The interval range is 0 to 65,535. The default interval is 5,000.
Disable RTCP Interval Randomization **[DisableRTCPRandomize]**	Controls whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter *RTCPInterval*. ▪ **[0]** Disable = Randomize (default) ▪ **[1]** Enable = No Randomize
Esc Transport Type **[RTCPXRESCTransportType]**	Determines the transport layer used for outgoing SIP dialogs initiated by the device to the RTCP XR Collection Server. ▪ **[-1**] Not Configured (default) ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS **Note:** When set to 'Not Configured', the value of the parameter *SIPTransportType* is used.
RTCP XR Collection Server **[RTCPXREscIP]**	IP address of the Event State Compositor (ESC). The device sends RTCP XR reports to this server, using SIP PUBLISH messages. The address can be configured as a numerical IP address or as a domain name.
RTCP XR Report Mode **[RTCPXRReportMode]**	Determines whether RTCP XR reports are sent to the Event State Compositor (ESC), and if so, defines the interval in which they are sent. ▪ **[0]** Disable = RTCP XR reports are not sent to the ESC (default). ▪ **[1]** End Call = RTCP XR reports are sent to the ESC at the end of each call. ▪ **[2]** End Call & Periodic = RTCP XR reports are sent to the ESC at the end of each call and periodically according to the parameter *RTCPInterval*.

Parameter	Description
Cut Through Parameters	
[DigitalCutThrough]	Enables PSTN CAS channels/endpoints to receive incoming IP calls even if the B-channels are in off-hook state. ▪ **[0]** Disabled (default) ▪ **[1]** Enabled When enabled, this feature operates as follows: 1 A Tel-to-IP call is established (connected) by the device for a B-channel. 2 The device receives a SIP BYE (i.e., IP side ends the call) and plays a reorder tone to the PSTN side for the duration set by the *CutThroughTimeForReOrderTone* parameter. The device releases the call towards the IP side (sends SIP 200 OK). 3 The PSTN side, for whatever reason, remains off-hook. 4 If a new IP call is received for this B-channel after the reorder tone has ended, the device "cuts through" the channel and connects the call immediately (even though the B-channel is in physical off-hook state) without playing a ring tone. If an IP call is received while the reorder tone is played, then the device rejects the call. **Notes:** ▪ If this parameter is disabled and the PSTN side remains in off-hook state after the IP call ends the call, the device releases the call after 60 seconds. ▪ A special CAS table can be used to report call status events (Active/Idle) to the PSTN side during Cut Through mode.
[CutThroughTimeForReOrderTone]	Defines the duration (in seconds) of the reorder tone played to the PSTN side after the IP call party releases the call, for the Cut Through feature. After the tone has ended, incoming call is answered immediately if the FXS is off-hook (analog) / PSTN is connected (digital). The valid values are 0 to 30. The default is 0 (i.e., no reorder tone is played). For enabling the Cut Through feature, use the DigitalCutThrough (CAS channels) or *CutThrough* (FXS channels) parameter.

1.11.1.3 SIP SAS Parameters

The table below describes the new SIP SAS application parameter for Release 6.2.

Table 1-5: New SIP SAS Parameter for Release 6.2

Parameter	Description
SAS Block Unregistered Users **[SASBlockUnRegUsers]**	Determines whether the device rejects SIP INVITE requests received from unregistered SAS users. This applies to SAS Normal and Emergency modes. ▪ **[0]** Un-Block =Allow INVITE from unregistered SAS users (default) ▪ **[1]** Block = Reject dialog-establishment requests from un-registered SAS users

1.11.2 SBC New Parameters

The table below describes the new SBC application parameters for Release 6.2.

Table 1-6: New SBC Parameters for Release 6.2

Parameter	Description
SBC No Answer Timeout **[SBCAlertTimeout]**	Defines the timeout (in seconds) to SBC outgoing (outbound IP routing) SIP INVITE messages. If the called IP party does not answer the call within this user-defined interval, the device disconnects the session. The device starts the timeout count upon receipt of a SIP 180 Ringing response from the called party. If no other SIP response (for example, 200 OK) is received thereafter within this timeout, the call is released. The valid range is 0 to 3600 seconds. the default is 600.
SBC GRUU Mode **[SBCGruuMode]**	Determines the Globally Routable User Agent (UA) URI (GRUU) support (according to RFC 5627). ▪ **[0]** None = No GRUU is supplied to users. ▪ **[1]** As Proxy = The device provides same GRUU types as the proxy provided the device's GRUU clients. (default) ▪ **[2]** Temporary only = Supply only temporary GRUU to users. (Currently not supported.) ▪ **[3]** Public only = The device provides only public GRUU to users. ▪ **[4]** Both = The device provides temporary and public GRUU to users. (Currently not supported.)
SBC Max Forwards Limit **[SBCMaxForwardsLimit]**	Defines the value of the Max-Forwards SIP header. The valid value range is 1-70. The default is 10. This parameter affects the Max-Forwards header in the received message, as follows: ▪ If the received header's original value is 0, the message is not passed on and is rejected. ▪ If the received header's original value is less than the user-defined parameter, the header's value is decremented before being sent on. ▪ If the received header's original value is greater than the user-defined parameter, the header's value is replaced by the user-defined parameter's value
Minimum Session-Expires **[SBCMinSE]**	Defines the minimum amount of time (in seconds) between session refresh requests in a dialog before the session is considered timed out. This value is conveyed in the SIP Min-SE header. The valid range is 0 (default) to 1,000,000 (where 0 means that the device does not limit Session-Expires).

Parameter	Description
SBC Registration Timers	
SBC User Registration Time **[SBCUserRegistrationTime]**	Defines the duration of the periodic registrations between the user and the SBC (SBC responds with this value to user). When set to 0, the SBC does not change the Expires value received in the user's REGISTER request. If no Expires header is received in the REGISTER and SBCUserRegistrationTime = 0, the Expires value is set to 180 seconds (by default). The valid range is 0 to 2,000,000 seconds. The default is 0.
SBC Proxy Registration Time **[SBCProxyRegistrationTime]**	Defines the duration for which the user is registered in the proxy database (after the device forwarded the REGISTER). When set to 0, the SBC sends the Expires value as received from the user to the proxy. The valid range is 0 to 2,000,000 seconds. The default is 0.
SBC Survivability Registration Time **[SBCSurvivabilityRegistrationTime]**	Defines the duration of the periodic registrations between the user and SBC, when the SBC is in survivability state (i.e., when REGISTER requests cannot be forwarded to the proxy, and is terminated by the SBC). When set to 0, the SBC uses the value of the parameter *SBCUserRegistrationTime* for the SBC response. The valid range is 0 to 2,000,000 seconds. The default is 0.

1.11.3 Media New Parameters

The table below describes the new media parameters for Release 6.2.

Notes: These parameters are applicable only to the Gateway application.

Table 1-7: New Media Parameters for Release 6.2

Parameter	Description
[T38FaxSessionImmediateStart]	Enables fax transmission of T.38 "no-signal" packets to the terminating fax machine. ▪ **[0]** Disable (default) ▪ **[1]** Enable This is used for transmission from fax machines (connected to the device) located inside a Network Address Translation (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.
T38 Version **[SIPT38Version]**	Selects the T.38 fax relay version. ▪ **[-1]** Not Configured = No T.38 (default) ▪ **[0]** T.38 version 0 (default) ▪ **[3]** T.38 version 3 = T.38 Version 3 (V.34 over T.38 support)

1.11.4 PSTN New Parameters

The table below describes the new PSTN parameters for Release 6.2.

Notes: These parameters are applicable only to the Gateway application.

Table 1-8: New PSTN Parameters for Release 6.2

Parameter	Description
[ISDNNSBehaviour2]	Bit-field to determine several behavior options, which influences the behavior of the Q.931 protocol. When this bit is set to NS_BEHAVIOUR2_ANY_UUI (0x0008), any User to User Information Element (UUIE) is accepted for any protocol discriminator. This feature is useful for interoperability with non-standard switches.
Tel2IP Default Redirect Reason **[Tel2IPDefaultRedirectReason]**	Default redirect reason for Tel-to-IP calls when no redirect reason (or “unknown”) exists in the received Q931 ISDN Setup message. The device includes this default redirect reason in the SIP History-Info header of the outgoing INVITE. If a redirect reason exists in the received Setup message, this parameter is ignored and the device sends the INVITE message with the reason according to the received Setup message. If this parameter is not configured (-1), the outgoing INVITE is sent with the redirect reason as received in the Setup message (if none or “unknown” reason, then without a reason). ▪ **[-1]** Not Configured (default) = Received redirect reason is not changed ▪ **[1]** Busy = Call forwarding busy ▪ **[2]** No Reply = Call forwarding no reply ▪ **[9]** DTE Out of Order = Call forwarding DTE out of order ▪ **[10]** Deflection = Call deflection ▪ **[15]** Systematic/Unconditional = Call forward unconditional
BRI-to-SIP Supplementary Services Codes for Call Forward Note: Upon receipt of an ISDN Facility message for call forward from the BRI phone, the device sends a SIP INVITE to the softswitch with a user-defined code in the SIP To header, representing the reason for the call forward.	
Call Forward Unconditional **[SuppServCodeCFU]**	Prefix code for activating Call Forward Unconditional sent to the softswitch. The valid value is a string. The default is an empty string. **Note:** The string must be enclosed in single apostrophe (e.g., ‘*72’).
Call Forward Unconditional Deactivation **[SuppServCodeCFUDeact]**	Prefix code for deactivating Call Forward Unconditional Deactivation sent to the softswitch. The valid value is a string. The default is an empty string. **Note:** The string must be enclosed in single apostrophe (e.g., ‘*72’).

Parameter	Description
Call Forward on Busy **[SuppServCodeCFB]**	Prefix code for activating Call Forward on Busy sent to the softswitch. The valid value is a string. The default is an empty string. **Note:** The string must be enclosed in single apostrophe (e.g., '*72').
Call Forward on Busy Deactivation **[SuppServCodeCFBDeact]**	Prefix code for deactivating Call Forward on Busy Deactivation sent to the softswitch. The valid value is a string. The default is an empty string. **Note:** The string must be enclosed in single apostrophe (e.g., '*72').
Call Forward on No Reply **[SuppServCodeCFNR]**	Prefix code for activating Call Forward on No Reply sent to the softswitch. The valid value is a string. The default is an empty string. **Note:** The string must be enclosed in single apostrophe (e.g., '*72').
Call Forward on No Reply Deactivation **[SuppServCodeCFNRDeact]**	Prefix code for deactivating Call Forward on No Reply Deactivation sent to the softswitch. The valid value is a string. The default is an empty string. **Note:** The string must be enclosed in single apostrophe (e.g., '*72').

Parameter	Description
BRI Supplementary Services Table	
[ISDNSuppServ]	This table configures the BRI endpoints and their authentication and caller ID settings. [ISDNSuppServ] FORMAT ISDNSuppServ_Index = ISDNSuppServ_PhoneNumber, ISDNSuppServ_Module, ISDNSuppServ_Port, ISDNSuppServ_UserId, ISDNSuppServ_UserPassword, ISDNSuppServ_CallerID, ISDNSuppServ_IsPresentationRestricted, ISDNSuppServ_IsCallerIDEnabled; [\ISDNSuppServ] Where: ▪ PhoneNumber = The telephone extension number for the BRI endpoint. ▪ Module = The BRI module number to which the BRI extension pertains. ▪ Port = The port number (on the BRI module) to which the BRI extension is connected. ▪ UserID = User ID for registering the BRI endpoint to a third-party softswitch for authentication and/or billing. ▪ UserPassword = User password for registering the BRI endpoint to a third-party softswitch for authentication and/or billing. Note: For security, the password is displayed as an asterisk (*). ▪ CallerID = Caller ID name of the BRI extension (sent to the IP side). The valid value is a string of up to 18 characters. ▪ IsPresentationRestricted = Determines whether the BRI extension sends its Caller ID information to the IP when a call is made. ✓ **[0]** Allowed = The device sends the string defined in the 'Caller ID' field when this BRI extension makes a Tel-to-IP call. ✓ **[1]** Restricted = The string defined in the 'Caller ID' field is not sent. ▪ IsCallerIDEnabled = Enables the receipt of Caller ID. ✓ **[0]** Disabled = The device does not send Caller ID information to the BRI extension. ✓ **[1]** Enabled = The device sends Caller ID information to the BRI extension For example: ISDNSuppServ 0 = 400, 1, 1, user, pass, callerid, 0, 1; ISDNSuppServ 1 = 401, 1, 1, user, pass, callerid, 0, 1;

1.11.5 Networking New Parameters

The table below describes the new networking parameters for Release 6.2.

Notes: These parameters are applicable to the Gateway and SBC applications.

Table 1-9: New Networking Parameters for Release 6.2

Parameter	Description
[TLSPkeySize]	Defines key size (in bits) for RSA public-key encryption for newly self-signed generated keys. ▪ **[512]** ▪ **[768]** ▪ **[1024]** (default) ▪ **[2048]**
[SSHMaxLoginAttempts]	Maximum SSH login attempts allowed for entering an incorrect password by an administrator before the SSH session is rejected. The valid range is 1 to 3. the default is 3.
[SSHEnableLastLoginMessage]	Enables or disables the message display in SSH sessions of the time and date of the last SSH login. The SSH login message displays the number of unsuccessful login attempts since the last successful login. ▪ **[0]** Disable ▪ **[1]** Enable (default) **Note:** The last SSH login information is cleared when the device is reset.
[SSHMaxSessions]	Maximum number of simultaneous SSH sessions. The valid range is 1 to 2. The default is 2 sessions.

Parameter	Description
[StaticRouteTable]	This ini file table parameter configures the IP Routing table for defining static IP routing rules. These rules can be associated with IP interfaces defined in the Multiple Interface table. The routing decision is thus based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination IP address. The format of this table is as follows: [StaticRouteTable] FORMAT StaticRouteTable_Index = StaticRouteTable_InterfaceName, StaticRouteTable_Destination, StaticRouteTable_PrefixLength, StaticRouteTable_Gateway, StaticRouteTable_Description; [\StaticRouteTable] Where: ▪ InterfaceName = IP network interface associated with this routing rule (index of the network interface as defined in the Multiple Interface table) ▪ Destination = IP address of the destination host/network ▪ PrefixLength = Subnet mask of the destination host/network ▪ Gateway = IP address of the router (next hop) to which the packets are sent if their destination matches the rules in the adjacent columns ▪ Description = Arbitrary description of this rule
Syslog Facility Number **[SyslogFacility]**	Facility level (0 through 7) for the device's Syslog messages, according to RFC 3164. This allows the user to identify Syslog messages generated by the device. This is useful, for example, if you collect the device's and other equipments' Syslog messages, at one single server. The device's Syslog messages can easily be identified and distinguished from other Syslog messages by its Facility level. Therefore, in addition to filtering Syslog messages according to IP address, the messages can be filtered according to Facility level. ▪ 16 - local use 0 (local0) - default ▪ 17 - local use 1 (local1) ▪ 18 - local use 2 (local2) ▪ 19 - local use 3 (local3) ▪ 20 - local use 4 (local4) ▪ 21 - local use 5 (local5) ▪ 22 - local use 6 (local6) ▪ 23 - local use 7 (local7)

1.11.6 Management and Provisioning New Parameters

The table below describes the new management and provisioning parameter for Release 6.2.

Notes: These parameters are applicable to the Gateway and SBC applications.

Table 1-10: New Management and Provisioning Parameter for Release 6.2

Parameter	Description
[SNMPEngineIDString]-	Defines the SNMP engine ID for SNMPv3/SNMPv2 agents. This is used for authenticating a user attempting to access the agent on the device. The ID can be a string of up to 36 characters. The default value is 00:00:00:00:00:00:00:00:00:00:00:00 (12 Hex octets characters). The provided key must be set with 12 Hex values delimited by a colon (":") in the format xx:xx:...:xx. For example, 00:11:22:33:44:55:66:77:88:99:aa:bb **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ Before setting this parameter, all SNMPv3 users must be deleted; otherwise, the parameter setting is ignored. ▪ If the supplied key does not pass validation of the 12 Hex values input or it is set with the default value, the engine ID is generated according to RFC 3411.

1.12 Modified Parameters

This section describes parameters from the previous release that have been modified in Release 6.2.

1.12.1 SIP Parameters

This section describes SIP parameters from the previous release that have been modified in Release 6.2.

1.12.1.1 SIP General Parameters

The table below describes the SIP general parameters from the previous release that have been modified in Release 6.2.

Table 1-11: Modified SIP General Parameters for Release 6.2

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Coders Group Table
[CodersGroup0]
[CodersGroup1]
[CodersGroup2]
[CodersGroup3]
[CodersGroup4]</td>
<td>Modifications:
▪ WB-RTA (Mediant 3000)
▪ G.722 (Mediant 800 MSBG) AMR-WB (Mediant 800 MSBG)
▪ Transparent ptime (Mediant 600, Mediant 1000, Mediant 1000 MSBG, Mediant 2000)
The format of this parameter is as follows:
[CodersGroup0]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime, CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
[\CodersGroup0]
<table>
<tr><th>Coder Name</th><th>Packetization Time (msec)</th><th>Rate (kbps)</th><th>Payload Type</th><th>Silence Suppression</th></tr>
<tr><td>WB-MS-RTA
[ms_rta_wb]</td><td>20 ms</td><td>29000</td><td>114</td><td>n/a</td></tr>
<tr><td>G.722
[g722]</td><td>20 (default), 40, 60, 80, 100, 120</td><td>64 (default)</td><td>Always 9</td><td>N/A</td></tr>
<tr><td>AMR-WB
[Amr-WB]</td><td>20 (default)</td><td>6.6 [0], 8.85 [1], 12.65 [2], 14.25 [3], 15.85 [4], 18.25 [5], 19.85 [6], 23.05 [7], 23.85 [8] (default)</td><td>Dynamic (0-127)</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>Transparent
[Transparent]</td><td>10, 20 (default), 40, 60, 80, 100, 120</td><td>Always 64</td><td>Dynamic (0-127)</td><td>Disable [0]
Enable [1]</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Proxy Set Table
[ProxySet]</td><td>Modifications:
▪ ClassificationInput (Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 3000)
▪ ProxyRedundancyMode (All Products)
The format of this parameter is as follows:
[ProxySet]
FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD, ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode;
[\ProxySet]
Where:
▪ ClassificationInput = classifies an IP call to a Proxy Set based on either its IP address, or its IP address, port, and transport type (e.g., UDP:
✓ [0] Compare only IP (default)
✓ [1] Compare IP, port and transport type
▪ ProxyRedundancyMode = defines the Proxy Redundancy feature per Proxy Set:
✓ [-1] = Not configured – the “global” parameter ProxyRedundancyMode applies (default).
✓ [0] Parking = The device continues operating with a redundant (now active) Proxy until the next failure, after which it operates with the next redundant Proxy.
✓ [1] Homing = The device always attempts to operate with the primary Proxy server (i.e., returns to the primary Proxy whenever available).
Note: If Proxy Redundancy mode is configured per Proxy Set, then the global ProxyRedundancyMode parameter is ignored.</td></tr>
<tr><td>IP Security
[SecureCallsFromIP]</td><td>Modification: Option [2] “Secure All Calls” added (all products).
Determines the device’s handling (allowing or rejecting) of the receipt of IP calls. This feature is useful for preventing unwanted SIP calls, SIP messages, and/or VoIP spam.
▪ [0] Disable = The device accepts all SIP calls (default).
▪ [1] Secure Incoming Calls = The device accepts SIP calls only from IP addresses defined in the 'Outbound IP Routing’ table/’Tel to IP Routing' or Proxy Set table, or IP addresses resolved from DNS servers from FQDN which appear in the Proxy Set table. All other incoming calls are rejected.
▪ [2] Secure All Calls = The device accepts SIP calls only from IP addresses (in dotted-decimal notation format) defined in the 'Outbound IP Routing’ table or Proxy Set table, and rejects all other incoming calls. In addition, if a fully-qualified domain name (FQDN) is defined in the routing table or Proxy Set table, the call is allowed to be sent only if the resolved DNS IP address appears in one of these table; otherwise it is rejected.
Note: If the parameter is set to [2], when using Proxies or Proxy Sets, it’s unnecessary to configure the Proxy IP addresses in the routing table. The device allows SIP calls received from the Proxy IP addresses even if these are not configured in the routing table.</td></tr>
</table>

Parameter	Description
Outbound IP Routing Table **[Prefix]**	**Modification:** PREFIX_DestSRD added. This *ini* file table parameter configures the Outbound IP Routing table for routing Tel-to-IP and IP-to-IP calls. The format of this parameter is as follows: [PREFIX] FORMAT PREFIX_Index = PREFIX_DestinationPrefix, PREFIX_DestAddress, PREFIX_SourcePrefix, PREFIX_ProfileId, PREFIX_MeteringCode, PREFIX_DestPort, PREFIX_SrcIPGroupID, PREFIX_DestHostPrefix, PREFIX_DestIPGroupID, PREFIX_SrcHostPrefix, PREFIX_TransportType, PREFIX_SrcTrunkGroupID, **PREFIX_DestSRD**; [\PREFIX]

1.12.1.2 SIP Gateway Parameters

The table below describes the SIP Gateway parameters from the previous release that have been modified in Release 6.2.

Table 1-12: Modified SIP Gateway Parameters for Release 6.2

Parameter	Description
Automatic Dialing Table **[TargetOfChannel]**	**Modification:** *HotLineToneDuration* parameter added (MP-1xx, Mediant 600, Mediant 1000, Mediant 1000 MSBG). [TargetOfChannel] FORMAT TargetOfChannel_Index = TargetOfChannel_Destination, TargetOfChannel_Type, TargetOfChannel_HotLineToneDuration, TargetOfChannel_Module, TargetOfChannel_Port; [\TargetOfChannel] Where: ▪ HotLineToneDuration = defines the timeout per port (channel) for automatic dialing when the Hotline feature is enabled. If the phone (connected to the specific port) is off-hooked and no digit is pressed for this user-defined duration (timeout), the device automatically initiates a call to the user-defined destination phone number. This parameter has a valid value range of 0 to 60 seconds, with default as 16.
Tone Index Table **[ToneIndex]**	**Modification:** ToneIndex_DestinationPrefix parameter added (MP-1xx, Mediant 600, Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 1000). [ToneIndex] FORMAT ToneIndex_Index = ToneIndex_FXSPort_First, ToneIndex_FXSPort_Last, ToneIndex_SourcePrefix, ToneIndex_DestinationPrefix, ToneIndex_PriorityIndex; [\ToneIndex] Where: ▪ DestinationPrefix = destination (called) number (or prefix) for associating a distinctive ringing pattern and call waiting tone for IP-to-Tel calls (FXS interfaces).

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Trunk Group Settings Table
[TrunkGroupSettings]</td><td>Modifications: New ChannelSelectMode options:
▪ [9] Ring to Hunt Group (MP-1xx, Mediant 600, Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 1000) [10] Select Trunk by ISDN Supplementary Services Table (Mediant 600, Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 1000)
[TrunkGroupSettings]
FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId, TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode, TrunkGroupSettings_GatewayName, TrunkGroupSettings_ContactUser, TrunkGroupSettings_ServingIPGroup, TrunkGroupSettings_MWIInterrogationType;
[\TrunkGroupSettings]
Where ChannelSelectMode defines the method for allocating incoming IP-to-Tel calls to a channel (port):
▪ [0] By Dest Phone Number = Selects the device's channel according to the called number (default.)
▪ [1] Cyclic Ascending = Selects the next available channel in an ascending cyclic order. Always selects the next higher channel number in the Trunk Group. When the device reaches the highest channel number in the Trunk Group, it selects the lowest channel number in the Trunk Group and then starts ascending again.
▪ [2] Ascending = Selects the lowest available channel. It always starts at the lowest channel number in the Trunk Group and if that channel is unavailable, selects the next higher channel.
▪ [3] Cyclic Descending = Selects the next available channel in descending cyclic order. It always selects the next lower channel number in the Trunk Group. When the device reaches the lowest channel number in the Trunk Group, it selects the highest channel number in the Trunk Group and then starts descending again.
▪ [4] Descending = Selects the highest available channel. It always starts at the highest channel number in the Trunk Group and if that channel is unavailable, selects the next lower channel.
▪ [5] Dest Number + Cyclic Ascending = The device first selects the channel according to the called number. If the called number isn't found, it then selects the next available channel in ascending cyclic order. Note that if the called number is found but the port associated with this number is busy, the call is released.
▪ [6] By Source Phone Number = The device selects the channel according to the calling number.
▪ [7] Trunk Cyclic Ascending = The device selects the channel from the first channel of the next trunk (adjacent to the trunk from which the previous channel was allocated). This option is applicable only to digital interfaces.
▪ [8] Trunk & Channel Cyclic Ascending = The device implements the Trunk Cyclic Ascending and Cyclic Ascending methods to select the channel. This method selects the next physical trunk (pertaining to the Trunk Group) and then selects the B-channel of this trunk according to the cyclic ascending method (i.e., selects the channel after the last allocated channel). This option is applicable only to digital interfaces.</td></tr>
</table>

Parameter	Description
	▪ **[9]** Ring to Hunt Group = The device allocates IP-to-Tel calls to all the FXS ports (channels) belonging to a specific Hunt Group. When an IP-to-Tel call is received by the device for a specific Hunt Group, all telephones connected to the FXS ports belonging to the Hunt Group start ringing. The call is eventually received by whichever telephone answers the call first (and the other phones will stop ringing). ▪ **[10]** Select Trunk by ISDN SuppServ Table = The device selects the BRI port/module according to the settings in the ISDN Supplementary Services table.
IP Profile Table **[IPProfile]**	**Modifications:** ▪ AMD parameters added: *AMDSensitivityParameterSuit*, *AMDSensitivityLevel*, *AMDMaxGreetingTime*, *AMDMaxPostGreetingSilenceTime* (Mediant 600, Mediant 1000 MSBG, Mediant 1000, Mediant 2000, Mediant 3000) ▪ *SBCDiversionMode*, *SBCHistoryInfoMode* (Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 3000) [IPProfile] FORMAT IPProfile_Index = IPProfile_ProfileName, IPProfile_IpPreference, IPProfile_CodersGroupID, IPProfile_IsFaxUsed, IPProfile_JitterBufMinDelay, IPProfile_JitterBufOptFactor, IPProfile_IPDiffServ, IPProfile_SigIPDiffServ, IpProfile_SCE, IPProfile_RTPRedundancyDepth, IPProfile_RemoteBaseUDPPort, IPProfile_CNGmode, IPProfile_VxxTransportType, IPProfile_NSEMode, IpProfile_IsDTMFUsed, IPProfile_PlayRBTone2IP, IPProfile_EnableEarlyMedia, IPProfile_ProgressIndicator2IP, IPProfile_EnableEchoCanceller, IPProfile_CopyDest2RedirectNumber, IPProfile_MediaSecurityBehaviour, IPProfile_CallLimit, IPProfile_ DisconnectOnBrokenConnection, IPProfile_FirstTxDtmfOption, IPProfile_SecondTxDtmfOption, IPProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume, IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID, IPProfile_MediaIPVersionPreference, IPProfile_TranscodingMode, IpProfile_SBCAllowedCodersGroupID, IpProfile_SBCAllowedCodersMode, IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior, IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity, IpProfile**_AMDSensitivityParameterSuit**, IpProfile**_AMDSensitivityLevel**, IpProfile**_AMDMaxGreetingTime**, IpProfile**_AMDMaxPostSilenceGreetingTime**, IpProfile**_SBCDiversionMode**, IpProfile**_SBCHistoryInfoMode**; [\IPProfile]
Call Priority Mode **[CallPriorityMode]**	**Modification:** Option [3] “Emergency” added (all products). Enables priority call handling. ▪ **[0]** Disable = Disable (default). ▪ **[1]** MLPP = MLPP Priority Calls handling is enabled. ▪ **[3]** Emergency = Pre-emption of IP-to-Tel E911 emergency calls. If the device receives an E911 call and there are currently no available channels, the device terminates one of the channel calls and sends the E911 call.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Flash Keys Sequence Style
[FlashKeysSequenceStyle
]</td><td>Modification: Option [2] added (MP-1xx, Mediant 600, Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 1000).
Hook flash keys sequence style.
▪ [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 Flash, 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 Flash 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 + 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 parameter Enable3WayConference is set to 1 and the parameter 3WayConferenceMode is set to 2). Note that the settings of the ConferenceCode parameter are ignored.
✓ Flash + 4: makes a call transfer.</td></tr>
<tr><td>3-Way Conference Mode
[3WayConferenceMode]</td><td>Modification: Option [2] On-Board added (Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 1000).
Defines the mode of operation when the 3-Way Conference feature is used.
▪ [0] AudioCodes Media Server = The Conference-initiating INVITE (sent by the device) uses the ConferenceID concatenated with a unique identifier as the Request-URI. This same Request-URI is set as the Refer-To header value in the REFER messages that are sent to the two remote parties. This conference mode is used when operating with AudioCodes IPMedia conferencing server. (Default)
▪ [1] Non-AudioCodes Media Server = The Conference-initiating INVITE (sent by the device) uses only the ConferenceID as the Request-URI. The conference server sets the Contact header of the 200 OK response to the actual unique identifier (Conference URI) to be used by the participants. This Conference URI is then included (by the device) in the Refer-To header value in the REFER messages sent by the device to the remote parties. The remote parties join the conference by sending INVITE messages to the conference using this conference URI.
▪ [2] On Board = On-board 3-way conference. The conference is established on the device without the need for an external Conference server. The device sets up the call conference using its IP media channels. These channels are obtained from the IP media module (i.e., MPM module). Note that the MPM module(s) must be installed to support three-way conferencing. You can limit the</td></tr>
</table>

Parameter	Description
	number of simultaneous, on-board 3-way conference calls, by using the parameter *MaxInBoardConferenceCalls*. **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ When using an external conference server (i.e., [0] or [1]), up to six three-way conference calls is supported.
T38 Fax Max Buffer **[T38FaxMaxBufferSize]**	**Modification:** Value range and default (all products). Defines the maximum size (in bytes) of the device's T.38 buffer. This value is included in the outgoing SDP when T.38 is used for fax relay over IP. The valid range is 500 to 3,000. The default value is: ▪ 1024 - MP-1xx, Mediant 1000 MSBG, Mediant 1000, Mediant 2000 ▪ 3000 - Mediant 800 MSBG, Mediant 3000
T.38 Max Datagram Size **[T38MaxDatagramSize]**	**Modification:** Value range and default (all products). Defines the maximum size (in bytes) of a T.38 datagram that the device can receive. This value is included in the outgoing SDP when T.38 is used. The valid range is 120 to 600. The default value is: ▪ 238 - MP-1xx, Mediant 1000 MSBG, Mediant 1000, Mediant 2000 ▪ 560 - Mediant 800 MSBG, Mediant 3000
SRTP offered Suites **[SRTPofferedSuites]**	**Modification:** Options [4] and [8] added (Mediant 3000). Defines the offered SRTP crypto suites. ▪ **[0]** All = All available crypto suites (default) ▪ **[1]** AES_CM_128_HMAC_SHA1_80 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 80-bit tag. ▪ **[2]** AES_CM_128_HMAC_SHA1_32 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag. ▪ **[4]** ARIA_128_BIT = device uses ARIA_128 encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag. ▪ **[8]** ARIA_192_BIT = device uses ARIA_192 encryption with a 192-bit key and HMAC-SHA1 message authentication with a 32-bit tag.

Parameter	Description
Voice Mail Interface **[VoiceMailInterface]**	**Modification:** Option [8] ETS added (Mediant 600, Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 1000). Enables the device's Voice Mail application and determines the communication method used between the PBX and the device. ▪ **[0]** None (default) ▪ **[1]** DTMF ▪ **[2]** SMDI (N/A) ▪ **[3]** QSIG ▪ **[4]** SETUP Only = For ISDN ▪ **[5]** MATRA/AASTRA QSIG ▪ **[6]** QSIG SIEMENS = QSIG MWI activate and deactivate messages include Siemens Manufacturer Specific Information (MSI) ▪ **[7]** IP2IP = The device's IP2IP application is used for interworking between an IP Voice Mail server and the device. This is implemented for sending unsolicited SIP NOTIFY messages received from the Voice Mail server to an IP Group (configured using the parameter *NotificationIPGroupID*). ▪ **[8]** ETSI = Euro ISDN, according to ETS 300 745-1 V1.2.4, section 9.5.1.1. Enables MWI interworking from IP to Tel, typically used for BRI phones.
MLPP Default Namespace **[MLPPDefaultNamespace]**	**Modification:** Option [5] UC added (all except MP-1xx). Determines the Namespace used for MLPP calls received from the ISDN side and destined for the Application server. The Namespace value is not present in the Precedence IE of the PRI Setup message. Therefore, the value is used in the Resource-Priority header of the outgoing SIP INVITE request. **[1]** DSN = DSN (default) **[2]** DOD = DOD **[3]** DRSN = DRSN **[5]** UC = UC
Use Tgrp Information **[UseSIPTgrp]**	**Modification:** Option [4] Hotline Extended added (all except MP-1xx). Determines whether the SIP 'tgrp' parameter is used. This SIP parameter specifies the Trunk Group to which the call belongs (according to RFC 4904). For example, the SIP message below indicates that the call belongs to Trunk Group ID 1: INVITE sip::+16305550100;tgrp=1;trunk-context=example.com@10.1.0.3;user=phone SIP/2.0 ▪ **[0]** Disable (default) = The 'tgrp' parameter isn't used. ▪ **[1]** Send Only = The Trunk Group number is added to the 'tgrp' parameter value in the Contact header of outgoing SIP messages. If a Trunk Group number is not associated with the call, the 'tgrp' parameter isn't included. If a 'tgrp' value is specified in incoming messages, it is ignored. ▪ **[2]** Send and Receive = The functionality of outgoing SIP messages is identical to the functionality described in option 1. In addition, for incoming SIP INVITEs, if the Request-URI includes a 'tgrp' parameter, the device routes the call according to that value (if possible). The Contact header in the outgoing SIP INVITE (Tel-to-IP call) contains "tgrp=<source trunk group ID>;trunk-

Parameter	Description
	context=<gateway IP address>". The <source trunk group ID> is the Trunk Group ID where incoming calls from Tel is received. For IP-Tel calls, the SIP 200 OK device's response contains "tgrp=<destination trunk group ID>;trunk-context=<gateway IP address>". The <destination trunk group ID> is the Trunk Group ID used for outgoing Tel calls. The <gateway IP address> in "trunk-context" can be configured using the parameter *SIPGatewayName*. ▪ **[3]** UCR 2008 = Interworks the hotline "Off Hook Indicator" parameter between SIP and ISDN: ✓ For IP-to-ISDN calls: - The device interworks the SIP tgrp=hotline parameter (received in INVITE) to ISDN Setup with the Off Hook Indicator IE of "Voice", and "Speech" Bearer Capability IE. Note that the Off Hook Indicator IE is described in UCR 2008 specifications. - The device interworks the SIP tgrp=hotline-ccdata parameter (received in INVITE) to ISDN Setup with an Off Hook Indicator IE of "Data", and with "Unrestricted 64k" Bearer Capability IE. The following is an example of the INVITE with tgrp=hotline-ccdata: `INVITE sip:1234567;tgrp=hotline-ccdata;trunk-context=dsn.mil@example.com` ✓ For ISDN-to-IP calls: - The device interworks ISDN Setup with an Off Hook Indicator of "Voice" to SIP INVITE with "tgrp=hotline;trunk-context=dsn.mil" in the Contact header. - The device interworks ISDN Setup with an Off Hook indicator of "Data" to SIP INVITE with "tgrp=hotline-ccdata;trunk-context=dsn.mil" in the Contact header. - If ISDN Setup does not contain an Off Hook Indicator IE and the Bearer Capability IE contains "Unrestricted 64k", the outgoing INVITE includes "tgrp=ccdata;trunk-context=dsn.mil". If the Bearer Capability IE contains "Speech", the INVITE in this case does not contain tgrp and trunk-context parameters. ▪ **[4]** Hotline Extended = Interworks the ISDN Setup message's hotline "OffHook Indicator" Information Element (IE) to SIP INVITE's Request-URI and Contact headers. (**Note:** For IP-to-ISDN calls, the device handles the call as described for option [3].) ✓ The device interworks ISDN Setup with an Off Hook Indicator of "Voice" to SIP INVITE Request-URI and Contact header with "tgrp=hotline;trunk-context=dsn.mil". ✓ The device interworks ISDN Setup with an Off Hook indicator of "Data" to SIP INVITE Request-URI and Contact header with "tgrp=hotline-ccdata;trunk-context=dsn.mil". ✓ If ISDN Setup does not contain an Off Hook Indicator IE and the Bearer Capability IE contains "Unrestricted 64k", the outgoing INVITE Request-URI and Contact header includes "tgrp=ccdata;trunk-context=dsn.mil". If the Bearer Capability IE contains "Speech", the INVITE in this case does not contain tgrp and trunk-context parameters. **Note:** IP-to-Tel configuration (using the parameter *PSTNPrefix*) overrides the 'tgrp' parameter in incoming INVITE messages.

1.12.1.3 SIP SAS Parameters

The table below describes the SIP SAS parameters from the previous release that have been modified in Release 6.2.

Table 1-13: Modified SIP SAS Parameters for Release 6.2

Parameter	Description
SAS Survivability Mode **[SASSurvivabilityMode]**	**Modification:** Option [4] Use IP-to-IP Routing Table added (all products). Determines the Survivability mode used by the SAS application. ▪ **[0]** Standard = Incoming INVITE and REGISTER requests are forwarded to the defined Proxy list of SASProxySet in Normal mode and handled by the SAS application in Emergency mode (default). ▪ **[1]** Always Emergency = The SAS application does not use Keep-Alive messages towards the SASProxySet, instead it always operates in Emergency mode (as if no Proxy in the SASProxySet is available). ▪ **[2]** Ignore Register = Use regular SAS Normal/Emergency logic (same as option [0]), but when in Normal mode incoming REGISTER requests are ignored. ▪ **[3]** Auto-answer REGISTER = When in Normal mode, the device responds to received REGISTER requests by sending a SIP 200 OK (instead of relaying the registration requests to a Proxy), and enters the registrations in its SAS database. ▪ **[4]** Use Routing Table only in Normal mode = The device uses the IP-to-IP Routing table to route IP-to-IP SAS calls only when in SAS Normal mode (and is unavailable when SAS is in Emergency mode).

1.12.2 SBC Parameters

The table below describes SBC parameters from the previous release that have been modified in Release 6.2.

Table 1-14: Modified SBC Parameter for Release 6.2

Parameter	Description
IP Group Table **[IPGroup]**	**Modification:** Option [2] for IPGroup_Type (Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 3000); Option [2] for IPGroup_EnableSurvivability. [IPGroup] FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description, IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_EnableSurvivability, IPGroup_ServingIPGroup, IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable, IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm, IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet; [\IPGroup] Where: ▪ IPGroup_Type: ✓ **[0]** SERVER ✓ **[1]** USER ✓ **[2]** GATEWAY ▪ IPGroup_EnableSurvivability: ✓ **[0]** Disable (default) ✓ **[1]** Enable if Necessary ✓ **[2]** Always Enable = Survivability mode is always enabled. The communication with the Serving IP Group (e.g., IP-PBX) is always considered as failed. The device uses its database for routing calls between the clients (e.g., IP phones) of the USER-type IP Group.
Admission Control Table **[SBCAdmissionControl]**	**Modification:** Rate and MaxBurst parameters added (Mediant 800 MSBG, Mediant 1000 MSBG). [SBCAdmissionControl] FORMAT SBCAdmissionControl_Index = SBCAdmissionControl_LimitType, SBCAdmissionControl_IPGroupID, SBCAdmissionControl_SRDID, SBCAdmissionControl_RequestType, SBCAdmissionControl_RequestDirection, SBCAdmissionControl_Limit, SBCAdmissionControl_LimitPerUser, SBCAdmissionControl_Rate, SBCAdmissionControl_MaxBurst; [\SBCAdmissionControl] Where: ▪ Rate = rate at which tokens are added to the bucket (i.e., token rate). One token is added to the bucket every 1000/Rate milliseconds. In other words, this is the rate of dialog setups per second, or unlimited if set to 0 (default). ▪ MaxBurst = Maximum tokens that can fill the bucket. At any given time, the bucket cannot contain more than this amount of tokens. In other words, this is the maximum burst size for the dialog setup rate, or unlimited if set to 0 (default).

1.12.3 Networking Parameters

The table below describes networking parameters from the previous release that have been modified in Release 6.2.

Notes: These parameters are applicable to the Gateway and SBC applications.

Table 1-15: Modified Networking Parameter for Release 6.2

Parameter	Description
Firewall Settings **[AccessList]**	**Modification:** Use_Specific_Interface and AccessList_Interface_ID parameters added (all products). [AccessList] FORMAT AccessList_Index = AccessList_Source_IP, AccessList_PrefixLen, AccessList_Start_Port, AccessList_End_Port, AccessList_Protocol, AccessList_Use_Specific_Interface, AccessList_Interface_ID, AccessList_Packet_Size, AccessList_Byte_Rate, AccessList_Byte_Burst, AccessList_Allow_Type; [\AccessList] Where: ▪ Use_Specific_Interface = determines whether you want to apply the rule to a specific network interface (defined in the Multiple Interface table): ✓ **[0]** Disable (default) ✓ **[1]** Enable ▪ AccessList_Interface_ID = network interface (as defined in the Multiple Interface table) to which you want to apply the rule. This is applicable if you enabled the 'Use Specific Interface' field.

1.13 Obsolete Parameters

The table below lists parameters from the previous release that are now obsolete in Release 6.2.

Table 1-16: Obsolete Parameters

Obsolete Parameter	Description
[AMDSensitivityResolution]	This parameter has been replaced by the new parameter, *AMDSensitivityParameterSuit*.
[AMDDetectionSensitivityHighResolution]	This parameter has been replaced by the new parameter, *AMDSensitivityLevel*.
[RoutingTableDestinationsColumn]	This parameter has been replaced by the new *ini* file table parameter, *StaticRouteTable*.
[RoutingTableDestinationMasksColumn]	This parameter has been replaced by the new *ini* file table parameter, StaticRouteTable.
[RoutingTableGatewaysColumn]	This parameter has been replaced by the new *ini* file table parameter, *StaticRouteTable*.
[RoutingTableHopsCountColumn]	This parameter has been replaced by the new *ini* file table parameter, *StaticRouteTable*.
[RoutingTableInterfacesColumn]	This parameter has been replaced by the new *ini* file table parameter, *StaticRouteTable*.
[VLANControlVLANID]	This parameter has been replaced by the Multiple Interface Table.
[VLANOamVLANID]	This parameter has been replaced by the Multiple Interface Table.
[VLANMediaVLANID]	This parameter has been replaced by the Multiple Interface Table.
[SBCRegistrationTime]	This parameter has been replaced by the new *ini* file parameter *SBCUserRegistrationTime*.
[T38Version]	This parameter has been replaced by the new *ini* file parameter *SIPT38Version*.
[WANIPAddress]	This parameter has been replaced by the new *ini* file table parameter *NATTranslation*.
[EnableStandardSIDPayloadType]	This parameter is now obsolete.
[EnableNoiseReduction]	This parameter is now obsolete.
[L1L1ComplexTxUDPPort]	This parameter is now obsolete.
[L1L1ComplexRxUDPPort]	This parameter is now obsolete.

2 Supported Features

This chapter describes various features supported by the device.

2.1 SIP Gateway Features

This section lists the SIP Gateway application's main features.

2.1.1 Supported SIP Features

The device supports the following main SIP Gateway features:

- Reliable User Datagram Protocol (UDP) transport, with retransmissions.
- Transmission Control Protocol (TCP) Transport layer.
- SIPS using TLS.
- T.38 real-time fax using SIP (including V.34 T.38 fax relay for Mediant 800 MSBG and Mediant 3000). Note that if the remote side includes the fax maximum rate parameter in the SDP body of the INVITE message, the device returns the same rate in the response SDP.
- Operates with proxy server, or without using an internal routing table.
- Fallback to internal routing table if proxy server does not respond.
- Up to 32 IP Groups and 32 Proxy Sets. Each Proxy Set can comprise up to 15 IP addresses. If the primary proxy server fails, the device automatically switches to a redundant proxy server.
- Up to 32 Registration Accounts, where each account can be used for operation with different ITSP/SIP Trunks.
- Domain name resolving using DNS NAPTR and SRV records for Proxy, Registrar and domain names that appear in the SIP Contact and Record-Route headers.
- Load balancing of proxy servers using round robin or random weights.
- Proxy and registrar authentication (handling 401 and 407 responses) using MD5 Digest method. Accepted challenges are kept for future requests to reduce the network traffic.
- Single device registration, multiple registration of all device endpoints, or registration per Trunk Group (using Accounts).
- Supported SIP Methods (messages): INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, INFO, REFER, UPDATE, NOTIFY, PRACK, SUBSCRIBE and PUBLISH.
- Modifying connection parameters for an already established call (re-INVITE).
- Operating with Redirect server and handling 3xx responses.
- Early media (supporting 183 Session Progress).
- Receipt of SIP REFER messages outside of a dialog.
- Responds to SIP OPTIONS messages outside a SIP dialog and in mid-call. Generates OPTIONS messages as Proxy keep-alive mechanism.
- Publishes the total number of free Tel channels in a 200 OK response to an OPTIONS requests.
- Receipt and DNS resolution of FQDNs received in SDP.
- Negotiation of coder from a list of given coders.
- Negotiation of dynamic payload types.
- Multiple ptime values per coder.

- DTMF out-of-band transfer using:
  - INFO method <draft-choudhuri-sip-info-digit-00.txt>
  - INFO method, compatible with Cisco gateways
  - NOTIFY method <draft-mahy-sipping-signaled-digits-01.txt>
  - INFO method, compatible with Korea Telecom format
- Handling forking proxy multiple responses.
- Supports ITU V.152 - Procedures for supporting Voice-Band Data over IP Networks.
- Call Hold and Transfer Supplementary services using SIP REFER, Refer-To, Referred-By, Replaces and NOTIFY messages.
- Three-way conferencing.

Table 2-1: Supported IETF RFC's

RFC Number	RFC Title
RFC 2327	SDP
RFC 5079	Rejecting Anonymous Requests in SIP
RFC 4904	Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication
RFC 2782	A DNS RR for specifying the location of services
RFC 2833	Telephone event
RFC 3261	SIP
RFC 3262	Reliability of Provisional Responses in SIP
RFC 3263	Locating SIP Servers
RFC 3264	Offer/Answer Model
RFC 3265	(SIP)-Specific Event Notification
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)
RFC 3311	UPDATE Method
RFC 3323	Privacy Mechanism
RFC 3325	Private Extensions to the SIP for Asserted Identity within Trusted Networks
RFC 3326	Reason header
RFC 3327	SIP Extension Header Field for Registering Non-Adjacent Contacts
RFC 3361	Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers (Not applicable to Mediant 800 MSBG and Mediant 1000 MSBG.)
RFC 3372	SIP-T
RFC 3389	RTP Payload for Comfort Noise
RFC 3420	Internet Media Type message/sipfrag
RFC 3455	Private Header (P-Header) Extensions to SIP for the 3rd-Generation Partnership Project (3GPP)
RFC 3489	STUN - Simple Traversal of UDP Through NATs
RFC 3515	Refer Method

RFC Number	RFC Title
RFC 3578	Interworking of ISDN overlap signalling to SIP
RFC 3581	Symmetric Response Routing - rport
RFC 3605	RTCP attribute in SDP
RFC 3608	SIP Extension Header Field for Service Route Discovery During Registration
RFC 3611	RTP Control Protocol Extended Reports (RTCP XR)
RFC 3665	SIP Basic Call Flow Examples
RFC 3666	SIP to PSTN Call Flows
RFC 3680	A SIP Event Package for Registration (IMS)
RFC 3711	The Secure Real-time Transport Protocol (SRTP)
RFC 3725	Third Party Call Control
RFC 3824	Using E.164 numbers with SIP (ENUM)
RFC 3842	MWI
RFC 3891	"Replaces" Header
RFC 3892	The SIP Referred-By Mechanism
RFC 3903	SIP Extension for Event State Publication
RFC 3911	The SIP Join Header [Partial]
RFC 3959	The Early Disposition Type for SIP
RFC 3960	Early Media and Ringing Tone Generation in SIP (partial compliance)
RFC 3966	The tel URI for Telephone Numbers
RFC 4028	Session Timers in the Session Initiation Protocol
RFC 4040	RTP Payload Format for a 64 kbit/s Transparent Call - Clearmode
RFC 4117	Transcoding Services Invocation
RFC 4235	An INVITE-Initiated Dialog Event Package for SIP (partial)
RFC 4240	Basic Network Media Services with SIP - NetAnn
RFC 4244	An Extension to SIP for Request History Information
RFC 4320	Actions Addressing Identified Issues with SIP Non-INVITE Transaction
RFC 4321	Problems Identified Associated with SIP Non-INVITE Transaction
RFC 4411	Extending SIP Reason Header for Preemption Events
RFC 4412	Communications Resource Priority for SIP
RFC 4458	SIP URIs for Applications such as Voicemail and Interactive Voice Response
RFC 4475	SIP Torture Test Messages
RFC 4497 or ISO/IEC 17343	Interworking between SIP and QSIG
RFC 4568	SDP Security Descriptions for Media Streams for SRTP
RFC 4715	Interworking of ISDN Sub Address to sip isub parameter
RFC 4730	A SIP Event Package for Key Press Stimulus (KPML) [Partial]

RFC Number	RFC Title
RFC 4733	RTP Payload for DTMF Digits
RFC 4961	Symmetric RTP and RTCP for NAT
RFC 5022	Media Server Control Markup Language (MSCML)
RFC 5627	Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP
RFC 5628	Registration Event Package Extension for GRUU
ECMA-355, ISO/IEC 22535	QSIG tunneling
draft-ietf-sip-privacy-04.txt	SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header
draft-levy-sip-diversion-08	Diversion Indication in SIP
draft-ietf-sipping-cc-transfer-05	Call Transfer
draft-ietf-sipping-realtimefax-01	SIP Support for Real-time Fax: Call Flow Examples
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol
draft-ietf-sip-connect-reuse-06	Connection Reuse in SIP
draft-ietf-sipping-rtcp-summary-10	SIP Package for Voice Quality Reporting Event, using SIP PUBLISH
draft-johnston-sipping-cc-uui-04	Transporting User to User Information for Call Centers using SIP
draft-mahy-iptel-cpc-06	The Calling Party's Category tel URI Parameter

Note: The following SIP features are not supported:

- Preconditions (RFC 3312)
- SDP - Simple Capability Declaration (RFC 3407)
- S/MIME
- Outbound, Managing Client-Initiated Connections (RFC 5626)
- SNMP SIP MIB (RFC 4780)
- SIP Compression – RFC 5049 (SigComp)
- ICE (RFC 5245)
- Connected Identity (RFC 4474)

2.1.2 SIP Compliance Tables

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

2.1.2.1 SIP Functions

The device supports the following SIP Functions:

Table 2-2: Supported SIP Functions

Function	Supported
User Agent Client (UAC)	Yes
User Agent Server (UAS)	Yes
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

2.1.2.2 SIP Methods

The device supports the following SIP Methods:

Table 2-3: Supported SIP Methods

Method	Supported	Comments
INVITE	Yes	
ACK	Yes	
BYE	Yes	
CANCEL	Yes	
REGISTER	Yes	Send only
REFER	Yes	Inside and outside of a dialog
NOTIFY	Yes	
INFO	Yes	
OPTIONS	Yes	
PRACK	Yes	
UPDATE	Yes	
PUBLISH	Yes	Send only
SUBSCRIBE	Yes	

2.1.2.3 SIP Headers

The device supports the following SIP Headers:

Table 2-4: Supported SIP Headers

Header Field	Supported
Accept	Yes
Accept–Encoding	Yes
Alert-Info	Yes
Allow	Yes
Also	Yes
Asserted-Identity	Yes
Authorization	Yes
Call-ID	Yes
Call-Info	Yes
Contact	Yes
Content-Disposition	Yes
Content-Encoding	Yes
Content-Length	Yes
Content-Type	Yes
Cseq	Yes
Date	Yes
Diversion	Yes
Encryption	No
Expires	Yes
Fax	Yes
From	Yes
History-Info	Yes
Join	Yes
Max-Forwards	Yes
Messages-Waiting	Yes
MIN-SE	Yes
Organization	No
P-Associated-URI	Yes
P-Asserted-Identity	Yes
P-Charging-Vector	Yes
P-Preferred-Identity	Yes
Priority	Yes

Header Field	Supported
Proxy- Authenticate	Yes
Proxy- Authorization	Yes
Proxy- Require	Yes
Prack	Yes
Reason	Yes
Record- Route	Yes
Refer-To	Yes
Referred-By	Yes
Replaces	Yes
Require	Yes
Remote-Party-ID	Yes
Response- Key	Yes
Retry-After	Yes
Route	Yes
Rseq	Yes
Session-Expires	Yes
Server	Yes
Service-Route	Yes
SIP-If-Match	Yes
Subject	Yes
Supported	Yes
Target-Dialog	Yes
Timestamp	Yes
To	Yes
Unsupported	Yes
User- Agent	Yes
Via	Yes
Voicemail	Yes
Warning	Yes
WWW- Authenticate	Yes

2.1.2.4 SDP Headers

The device supports the following SDP Headers:

Table 2-5: Supported SDP Headers

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

2.1.2.5 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

2.1.2.5.1 1xx Response – Information Responses

Table 2-6: Supported 1xx SIP Responses

1xx Response		Supported	Comments
100	Trying	Yes	The device generates this response upon receiving a Proceeding message from ISDN or immediately after placing a call for CAS signaling.
180	Ringing	Yes	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	Yes	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	Yes	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	Yes	The device generates this response if the Early Media feature is enabled and if the device plays a Ringback tone to IP

2.1.2.5.2 2xx Response – Successful Responses

Table 2-7: Supported 2xx SIP Responses

2xx Response		Supported	Comments
200	OK	Yes	-
202	Accepted	Yes	-

2.1.2.5.3 3xx Response – Redirection Responses

Table 2-8: Supported 3xx SIP Responses

3xx Response		Supported	Comments
300	Multiple Choice	Yes	The device responds with an ACK, and then resends the request to the first new address in the contact list.
301	Moved Permanently	Yes	The device responds with an ACK, and then resends the request to the new address.
302	Moved Temporarily	Yes	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	Yes	The device responds with an ACK, and then resends the request to a new address.
380	Alternate Service	Yes	The device responds with an ACK, and then resends the request to a new address.

2.1.2.5.4 4xx Response – Client Failure Responses

Table 2-9: Supported 4xx SIP Responses

4xx Response		Supported	Comments
400	Bad Request	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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		Supported	Comments
420	Bad Extension	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	This response indicates that the initial request is terminated with a BYE or CANCEL request.
488	Not Acceptable	Yes	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	Yes	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.

2.1.2.5.5 5xx Response – Server Failure Responses

Table 2-10: 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	

2.1.2.5.6 6xx Response – Global Responses

Table 2-11: 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	

2.2 Supported PSTN-SIP Interworking Features

Note: This section is applicable only to digital PSTN products (i.e., Mediant 600, Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 1000, Mediant 2000, and Mediant 3000).

The SIP device supports various ISDN PRI protocols such as EuroISDN, North American NI2, Lucent 4/5ESS, Nortel DMS100, Meridian1 DMS100, Japan J1, as well as QSIG. PRI support includes User Termination or Network Termination side. ISDN-PRI protocols can be defined on an E1/T1 basis (i.e., different variants of PRI are allowed on different E1/T1 spans).

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

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

PSTN-to-SIP and SIP-to-PSTN Called and Calling numbers can be optionally modified according to rules defined using the device's configuration parameters.

Mediant 600, Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 1000 also support various ISDN BRI protocols such as Euro-ISDN and QSIG. BRI support includes User Termination or Network Termination side.

The device supports the following PSTN-SIP interworking features:

- Definition and use of Trunk Groups for routing IP-to-PSTN calls.
- B-channel negotiation for PRI spans.
- ISDN Non Facility Associated Signaling (NFAS). (Not applicable to Mediant 800 MSBG.)
- PRI-to-SIP interworking according to RFC 4497 or ISO/IEC 17343.
- PRI-to-SIP Interworking of Q.931 Display (Calling Name) information element (IE).
- PRI (NI-2, 5ESS)/EURO ISDN/QSIG to SIP interworking of Calling Name using Facility IE in Setup and Facility messages.
- Configuration of Numbering Plan and Type for IP-to-ISDN calls.
- Interworking and flexible mapping of PSTN-to-SIP release causes.
- Interworking of ISDN redirect number to SIP Diversion header (according to IETF <draft-levy-sip-diversion-05.txt>) or to History-Info header (RFC 4244).
- Optional change of redirect number to called number for ISDN-to-IP calls.
- Interworking of ISDN calling line Presentation & Screening indicators using RPID header <draft-ietf-sip-privacy-04.txt>.
- Interworking of Q.931 Called and Calling Number Type and Number Plan values using the RPID header or using the phone-context parameter (RFC 4904).
- Interworking of Calling and Called Subaddress values for SIP-to-ISDN calls (RFC 4715).
- ISDN en-block or overlap dialing for incoming Tel-to-IP calls.
- ISDN to SIP interworking of ISDN Overlap Dialing according to RFC 3578.
- Digit map pattern to reduce the dialing period when Overlap dialing is used.
- Routing of IP-to-Tel calls to predefined trunk groups.

- Configurable channel-select mode per trunk group.
- Various number manipulation rules for IP-to-Tel and Tel-to-IP, called and calling numbers.
- Option to configure ISDN Transfer Capability per trunk.
- Transfer of User-to-User Information Element (UUIE) between SIP and PRI.
- ISDN Transfer using TBCT / RLT / ECT.
- QSIG messages tunneling over SIP according to ECMA-355(ISO/IEC 22535).
- ISDN PRI messages tunneling over SIP messages according to RFC 3372 - SIP-T.
- Interworking of Hold/Retrieve supplementary services from QSIG/EuroISDN to SIP and vice versa.
- QSIG and EURO ISDN Deflection (Rerouting), interworking of Call Rerouting Facility to SIP 302 response in both IP-to-Tel and Tel-to IP directions.
- QSIG MWI Notifications and QSIG MWI Interrogation.
- QSIG Single Step Transfer from QSIG to SIP, and vice versa.
- QSIG Path Replacement from SIP to QSIG.
- QSIG BRI Suspend/Resume.
- Euro-ISDN MWI
- BRI Call Forwarding (supported by the softswitch that does the call forward operation; the device simply provides the softswitch the information (by DTMF) about the forward numbers.
- Comply with DoD UCR 2008 Change 1 specifications, including Multi-Level Precedence & Preemption (MLPP) using NI-2. (Not applicable to Mediant 800 MSBG.)
- Calling Party Category interworking between PRI and SIP according to <draft-mahy-iptel-cpc-05>.
- E911 Generic Information IE (according to Telcordia GR-2968-CORE) from SIP to NI-2. (Not applicable to Mediant 800 MSBG.)

2.3 Supported IP Media Features

> **Note:** This section is applicable only to Mediant 1000 and Mediant 1000 MSBG.

The Mediant 1000 and Mediant 1000 MSBG support the following IP media features:

- VoIP Conference Bridge, supporting up to 60 channels.
- Up to 20 three-way conferences.
- Up to 60 participants in a single conference. Up to 3 active talkers; the rest being listeners only.
- VoIP Announcement media server supporting up to 120 VoIP channels.
- Playing via HTTP/NFS streaming.
- Recording via NFS streaming.
- Play/Record using Low Bit Rate (LBR) coders.
- Repeat playing announcement.
- Playing announcements using Early Media SIP session.
- Detection and relay of DTMF digits using INFO messages.
- Conferencing and Network Announcements (NetAnn) according to RFC 4240.
- The following features are supported via MSCML (RFC 5022):
  - Play request for playing of complex, dynamic announcements.
  - PlayCollect request for playing announcements and collecting digits.
  - PlayRecord request for playing announcements and then recording the voice stream received from the user.
  - Applying IVR services on PSTN-to-IP calls.
  - Enhanced conferencing according to the MSCML framework.
  - Signal Events Notifications, allowing a client to be notified of various call progress signals.
- Bearer Channel Tandeming (BCT) for Lawful Intercept purposes.
- Voice Extensible Markup Language (VXML) Version 2.0.
- Transcoding according to RFC 4240 and RFC 4117.

2.4 Supported Data-Router Features

The supported data-router features are listed in the subsections below.

Note: This section is applicable only to Mediant 800 MSBG and Mediant 1000 MSBG.

2.4.1 LAN Switching

The device supports the following LAN switching features:

- **Mediant 800 MSBG:**
  1. LAN switch ports with non-blocking switching performance.
  2. Up to four RJ-45 10/100/1000Base-T (Gigabit Ethernet) LAN ports.
  3. Eight RJ-45 10/100Base-TX (Fast Ethernet) LAN ports.
  4. 802.1Q for VLAN tagging.
  5. Power-over-Ethernet (PoE) supported on all LAN ports, complying with IEEE 802.3af-2003 (15.4W maximum wattage per port; 120 total wattage over all ports).
  6. LAN ports support half- and full-duplex modes, auto-negotiation, and straight or crossover cable detection.
- **Mediant 1000 MSBG:**
  1. CRMX module supporting three on-board 10/100/1000Base-T, auto-negotiated LAN switch ports with non-blocking switching performance.
  2. 802.1Q for VLAN tagging.
  3. High performance lookup engine with support for up to 1024 MAC addresses.

2.4.2 Routing

The device supports the following new routing features:

1. Dynamic Host Configuration Protocol (DHCP):
   - DHCP server, DHCP relay and DHCP client
   - DHCP server supports fixed binding of IP-to-MAC address
   - DHCP server supports user-defined DNS server allocation
2. Multiple IP interfaces for LAN routing: IP interfaces assignment to different VLANs.
3. Assignment of different VLAN IDs to VoIP and Data traffic.
4. Symmetric High-Speed Digital Subscriber Line (SHDSL):
   - ATM:
     - RFC 2684 over AAL5 with LLC-SNAP and VC-MUX over AAL5.
     - ATM UNI 4.1
     - UBR, CBR, VBR-RT and VBR-NRT
     - IP QoS
     - Multiple IP interfaces
     - RFC 2684 Routed Mode
     - RFC 2364 PPPoA
     - RFC 2516 PPPoE over ATM
     - Up to 8 PVCs

- EFM:
  - ITU G.991.2 Annex E for Ethernet, also known as EFM or 2Base-TL, as defined in IEEE 802.3ah
  - Up to 8 IP interfaces for EFM/2Base-TL
  - IP QoS classification, Marking, scheduling and shaping
  - 802.1Q VLANs

5. Routing protocols:
   - Static routing
   - RIPv1 - RFC 1058
   - RIPv2 - RFC 2453
   - OSPFv2 - RFC 2328
   - BGPv4 - RFC 1771 and RFC 2858
   - BGP Extended Community Attribute for BGP/MPLS VPNs
   - Policy-based routing (e.g. DSCP-based and BGP policy routing)
6. Network Address Translation (NAT/NAPT):
   - ACL-like classification with ALG support
   - Source and destination-based IP addresses ACLs
   - Multiple NAT and NAPT WAN addresses
7. WAN access via PPPoE, PPTP, L2TP, DHCP.
8. Quality of service (QoS):
   - Traffic Classification and Marking:
     - Connection-based (with SPI) or packet-based classification.
     - VoIP classification for both SIP signaling and media traffic: tracking UDP ports selected by SDP offer-answer negotiations.
     - Explicit classification criteria:
       - ✓ Source/destination MAC and IP addresses
       - ✓ Protocol (ALG-based)
       - ✓ L4 port numbers
       - ✓ DSCP/802.1p
       - ✓ Length of packets or their data portion only
     - DSCP and 802.1p marking
   - Traffic scheduling and shaping:
     - Ingress traffic policing
     - Traffic reservation - when not utilized, other classes are served with extra bandwidth
     - Maximum egress traffic shaping
     - Scheduling: Strict Priority, Fair, Weighted Round-Robin Queuing, and Class-Based WRR Queuing
     - Queue management:
       - ✓ RED
       - ✓ TCP Serialization Reduction to minimize jitter in VoIP environments

2.4.3 Data Security

The device supports the following new data security features:

1. Zero Configuration Firewall wizard with three security levels:
   - Minimum (Inbound and Outbound policies set to 'Accept')
   - Typical (Inbound policy set to 'Reject'; Outbound Policy to 'Accept')
   - Maximum (only selected applications are allowed in Outbound policy)
2. Access Control for pinpoint security policy.
3. Extensive list of ALG-modules combined with SPI for error-free configuration and maximum security.
4. Port-forwarding and DMZ support for local applications and hosts.
5. Website Restriction allows static URL-based blocking of public/extranet websites.
6. Advanced Filtering allows full control on Inbound/Outbound Rules per interface/device.
7. Site-to-Site VPN:
   - Supports two IPSec use-cases:
     - Site-to-Site (Gateway-to-Gateway) VPN
     - Teleworker (User-to-Gateway) VPN
   - Fully compliant with IPSec RFCs:
     - RFC 2401 - Security Architecture for IP
     - RFC 2402 - IP Authentication Header
     - RFC 2406 – ESP
     - RFC 2403 and RFC 2404 for Authentication
8. PPTP/L2TP Client-Server VPN:
   - Supports two VPN use-cases:
     - Server support for remote Teleworker VPN access
     - Client-to-Gateway support with PPTP/L2TP
   - Point-to-Point Tunneling Protocol - RFC 2637
   - Layer Two Tunneling Protocol - RFC 2661 (with L2TP/IPSec)
   - Support all WiN OS versions as well as Linux
9. DoS and IDS/IPS:
   - Denial of Service (DoS) protection: TCP RST, Ping Flood, ICMP Echo storm, UDP snork attack, ICMP Smurf, UDP fraggle and more
   - IP spoofing attacks: FTP bounce, Broadcast/multicast source IP attack
   - Intrusion and scanning attacks:
     - IP source route, ICMP Echo reply without request, ICMP Ping sweep, TCP Stealth
     - Scan (FIN, XMAS, NULL), UDP port, FTP passive attack, loopback/Echo chargen, Block security hazard ICMP messages
   - IP fragment overlap, Ping of Death, Fragmentation attacks and more

2.4.4 Supported RFC's

The device materially supports the following RFC's:

- **IP/Routing:**
  - RFC 768 UDP
  - RFC 791 IP
  - RFC 792 ICMP
  - RFC 793 TCP
  - RFC 959 FTP
  - RFC 2822 Internet Message Format
  - RFC 1305 NTP
  - RFC 826 ARP
  - RFC 2131 DHCP
  - RFC 1918 IP Addressing
  - RFC 2516 PPPoE
  - RFC 2663 NAT
- **QoS:**
  - IEEE 802.1p Priority Tagging
  - RFC 1349
  - RFC 2475
  - RFC 2597
  - RFC 3246
- **IPSec:**
  - RFC 2401 Security Architecture for IP
  - RFC 2402 AH - IP Authentication Header
  - RFC 2403 IPsec Authentication - MD5
  - RFC 2404 IPsec Authentication - SHA-1
  - RFC 2405 IPsec Encryption - DES
  - RFC 2406 ESP - IPsec Encryption
  - RFC 2407 IPsec DOI
  - RFC 2408 ISAKMP
  - RFC 2409 IKE
  - RFC 2410 IPsec Encryption – NULL
  - RFC 2411
  - RFC 2412 OAKLEY

2.5 DSP Firmware Templates (Voice Codecs)

This section lists the DSP templates and corresponding voice codecs support.

2.5.1 MediaPack 1xx

The device supports the following DSP firmware templates:

Table 2-12: DSP Firmware Templates for MediaPack Series

	DSP Template			
	0		1	
	Number of Channels			
	Default	SRTP Enabled	Default	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
MP-124	24	20	20	20
Voice Coder				
G.711 A/Mu-law PCM	Yes		Yes	
G.726 ADPCM	Yes		Yes	
G.727 ADPCM	Yes		Yes	
G.723.1	Yes		Yes	
G.729 A, B	Yes		Yes	
EG.711	Yes		-	
G.722	-		Yes	

Notes:

- Installation and use of vocoders is subject to obtaining the appropriate license and to royalty payments.
- The number of channels refers to the device's maximum channel capacity.
- For other DSP template configurations, please contact AudioCodes.

2.5.2 Mediant 600 and Mediant 1000

The device supports the following DSP firmware templates:

Notes:

- Installation and use of vocoders is subject to obtaining the appropriate license and to royalty payments.
- The number of channels refers to the device's maximum channel capacity.
- The maximum number of channels on any form of analog, digital and MPM modules assembly is 120.
- Assembly of the MPM module in Slot 6 enables DSP conferencing capabilities.
- For other DSP template configurations, please contact AudioCodes.

Table 2-13: DSP Firmware Templates for Mediant 600 and Mediant 1000 Analog (FXS/FXO) Interfaces

	DSP Template	
	0, 1, 2, 4, 5	**10, 11, 12, 14,15**
	Number of Channels	
Default Settings	4	3
With SRTP	3	3
Voice Coder		
G.711 A/Mu-law PCM	Yes	Yes
G.726 ADPCM	Yes	Yes
G.727 ADPCM	Yes	Yes
G.723.1	Yes	Yes
G.729 A, B	Yes	Yes
EG.711	Yes	-
G.722	-	Yes

Table 2-14: DSP Firmware Templates for Mediant 600 and Mediant 1000 Digital Interfaces

	DSP Template																	
	0 or 10			1 or 11			2 or 12			4 or 14			5 or 15			6 or 16		
	Number of Spans																	
	1	2	4	1	2	4	1	2	4	1	2	4	1	2	4	1	2	4
	Number of Channels																	
Default Settings	31	62	120	31	48	80	24	36	60	31	60	100	24	36	60	31	60	100
128-ms EC	31	60	100	31	48	80	26	36	60	31	60	100	24	36	60	31	60	100
SRTP	31	60	100	-	-	-	-	-	-	31	48	80	24	36	60	31	48	80
IPM Features*	31	60	100	-	-	-	-	-	-	-	-	-	-	-	-	31	60	100
IPM Features & SRTP	31	48	80	-	-	-	-	-	-	-	-	-	-	-	-	31	48	80
Voice Coder																		
G.711 A/ Mu-law PCM	Yes			Yes			Yes			Yes			Yes			Yes		
G.726 ADPCM	Yes			Yes			Yes			Yes			Yes			-		
G.727 ADPCM	Yes			Yes			Yes			Yes			Yes			-		
G.723.1	Yes			-			-			-			-			-		
G.729 A, B	Yes			Yes			Yes			Yes			Yes			Yes		
GSM FR	Yes			Yes			-			-			-			-		
MS GSM	Yes			Yes			-			-			-			-		
iLBC	-			-			-			-			Yes			-		
EG.711	-			-			-			Yes			Yes			-		
EVRC	-			-			Yes			-			-			-		
QCELP	-			-			Yes			-			-			-		
AMR	-			Yes			-			-			-			-		
GSM EFR	-			Yes			-			-			-			-		
Transparent	Yes			Yes			Yes			Yes			Yes			Yes		

* IPM Features refers to configuration that includes at least one of the following:

- Mounted MPM module in Slot 6 for conferencing applications.
- Enabled IPM Detectors (e.g. Answer Detector).
- Mounted MPM modules with the IP Media Channels feature enabled.

Table 2-15: DSP Firmware Templates for Mediant 1000 MPM Module

	DSP Template											
	0 or 10		1 or 11		2 or 12		4 or 14		5 or 15		6 or 16	
	Assembly Slot Number											
	1-5	6	1-5	6	1-5	6	1-5	6	1-5	6	1-5	6
	Number of Channels											
Default Settings	40	20	32	16	24	12	40	20	24	12	40	20
SRTP	32	16	-	-	-	-	32	16	24	12	32	16
Voice Coder												
G.711 A/Mu-law PCM	Yes		Yes		Yes		Yes		Yes		Yes	
G.726 ADPCM	Yes		Yes		Yes		Yes		Yes		-	
G.727 ADPCM	Yes		Yes		Yes		Yes		Yes		-	
G.723.1	Yes		-		-		-		-		-	
G.729 A, B	Yes		Yes		Yes		Yes		Yes		Yes	
GSM FR	Yes		Yes		-		-		-		-	
MS GSM	Yes		Yes		-		-		-		-	
iLBC	-		-		-		-		Yes		-	
EG.711	-		-		-		Yes		Yes		-	
EVRC	-		-		Yes		-		-		-	
QCELP	-		-		Yes		-		-		-	
AMR	-		Yes		-		-		-		-	
GSM EFR	-		Yes		-		-		-		-	
Transparent	Yes		Yes		Yes		Yes		Yes		Yes	

Note: Only DSP Templates 0, 6, 10, and 16 support IPM detectors.

2.5.3 Mediant 800 MSBG

The device supports the following DSP firmware capabilities:

Table 2-16: DSP Firmware Capabilities

Telephony Ports	Number of Basic DSP Channels	Advanced DSP Capabilities			
		IPM Detectors	AMR (WB/NB)	Transcoding Sessions	Conference (WB/NB)
1 x E1/T1	31 / 24	Yes	-	-	-
	30 / 24	Yes	Yes	-	-
12 x FXS	12	-	-	-	-
FXS/FXO Combination x 12	11	Yes	-	-	-
	10	Yes	Yes	-	-
FXO/FXS Combination x 8	8	Yes	Yes	-	-
4 x BRI	8	Yes	Yes	-	-
4 x FXS	4	-	-	2	1 conference bridge with up to 4 participants
		Yes	Yes	1	
4 x FXO	4	Yes	Yes	1	

Notes:

- *Basic* includes the following functionality: G.711 A/Mu-law, G.722, G.726, G.729 A/B, G.723.1, T38 Version 3, Fax/Modem VBD, IBS (CPT, UDT, DTMF, MF), Caller ID, and Echo Canceller.
- Transcoding capability may require an appropriate Software Upgrade Feature Key.
- IPM Detectors currently supports only the Answer Detector.
- Installation and use of vocoders is subject to obtaining the appropriate license in advance of use, and royalty payments.
- The Number of Channels represents maximum capacity. On Analog/BRI depopulated hardware interface assemblies, remaining DSP channels may be used as IP-only channels for three-way conferencing and transcoding.
- Digital hardware assemblies do not support IP-only channels.

2.5.4 Mediant 1000 MSBG

The device supports the following DSP firmware templates:

Notes:

- Installation and use of vocoders is subject to obtaining the appropriate license and to royalty payments.
- The number of channels refers to the device's maximum channel capacity.
- The maximum number of channels on any form of analog, digital and MPM modules assembly is 120.
- Assembly of the MPM module in Slot 6 enables DSP conferencing capabilities.
- For other DSP template configurations, please contact AudioCodes.

Table 2-17: DSP Firmware Templates for Mediant 1000 MSBG Analog (FXS/FXO) Interfaces

	DSP Template	
	0, 1, 2, 4, 5, 6	**10, 11, 12, 14,15, 16**
	Number of Channels	
Default Settings	4	3
With SRTP	3	3
Voice Coder		
G.711 A/Mu-law PCM	Yes	Yes
G.726 ADPCM	Yes	Yes
G.727 ADPCM	Yes	Yes
G.723.1	Yes	Yes
G.729 A, B	Yes	Yes
EG.711	Yes	-
G.722	-	Yes

Table 2-18: DSP Firmware Templates for Mediant 1000 MSBG Digital Interfaces

	DSP Template																	
	0 or 10			1 or 11			2 or 12			4 or 14			5 or 15			6 or 16		
	Number of Spans																	
	1	2	4	1	2	4	1	2	4	1	2	4	1	2	4	1	2	4
	Number of Channels																	
Default Settings	31	72	120	31	48	80	24	36	60	31	60	100	24	36	60	31	60	100
With 128-ms EC	31	60	100	31	48	80	26	36	60	31	60	100	24	36	60	31	60	100
With SRTP	31	60	100	-	-	-	-	-	-	31	48	80	24	36	60	31	48	80
With IPM Features (*)	31	60	100	-	-	-	-	-	-	-	-	-	-	-	-	31	60	100
With IPM Features & SRTP	31	48	80	-	-	-	-	-	-	-	-	-	-	-	-	31	48	80
Voice Coder																		
G.711 A/Mu-law PCM	Yes			Yes			Yes			Yes			Yes			Yes		
G.726 ADPCM	Yes			Yes			Yes			Yes			Yes			-		
G.727 ADPCM	Yes			Yes			Yes			Yes			Yes			-		
G.723.1	Yes			-			-			-			-			-		
G.729 A, B	Yes			Yes			Yes			Yes			Yes			Yes		
GSM FR	Yes			Yes			-			-			-			-		
MS GSM	Yes			Yes			-			-			-			-		
iLBC	-			-			-			-			Yes			-		
EG.711	-			-			-			Yes			Yes			-		
EVRC	-			-			Yes			-			-			-		
QCELP	-			-			Yes			-			-			-		
AMR	-			Yes			-			-			-			-		
GSM EFR	-			Yes			-			-			-			-		
G.722	-			-			-			-			-			Yes		
Transparent	Yes			Yes			Yes			Yes			Yes			Yes		

* IPM Features refers to configuration that includes at least one of the following:

- Mounted MPM module in Slot 6 for conference applications.
- Enabled IPM Detectors (e.g. Answer Detector).
- Mounted MPM modules with the IP Media Channels feature enabled.

Table 2-19: DSP Firmware Templates for Mediant 1000 MSBG MPM Module

	DSP Template											
	0 or 10		1 or 11		2 or 12		4 or 14		5 or 15		6 or 16	
	Assembly Slot Number											
	1-5	6	1-5	6	1-5	6	1-5	6	1-5	6	1-5	6
	Number of Channels											
Default Settings	40	20	32	16	24	12	40	20	24	12	40	20
With SRTP	32	16	-	-	-	-	32	16	24	12	32	16
Voice Coder												
G.711 A/Mu-law PCM	Yes		Yes		Yes		Yes		Yes		Yes	
G.726 ADPCM	Yes		Yes		Yes		Yes		Yes		-	
G.727 ADPCM	Yes		Yes		Yes		Yes		Yes		-	
G.723.1	Yes		-		-		-		-		-	
G.729 A, B	Yes		Yes		Yes		Yes		Yes		Yes	
GSM FR	Yes		Yes		-		-		-		-	
MS GSM	Yes		Yes		-		-		-		-	
iLBC	-		-		-		-		Yes		-	
EG.711	-		-		-		Yes		Yes		-	
EVRC	-		-		Yes		-		-		-	
QCELP	-		-		Yes		-		-		-	
AMR	-		Yes		-		-		-		-	
GSM EFR	-		Yes		-		-		-		-	
G.722	-		-		-		-		-		Yes	
Transparent	Yes		Yes		Yes		Yes		Yes		Yes	

Note: Only DSP Templates 0, 6, 10, and 16 support IPM detectors.

2.5.5 Mediant 2000

The device supports the following DSP firmware templates:

Notes:

- Installation and use of vocoders is subject to obtaining the appropriate license and to royalty payments.
- The number of channels refers to the device's maximum channel capacity.
- DSP templates 1 and 2 are not supported on reduced hardware assemblies (i.e., one or two trunks).
- For other DSP template configurations, please contact AudioCodes.

Table 2-20: DSP Firmware Templates for Mediant 2000

	DSP Template				
	0	1	2	4	5
	Number of Channels				
Default Setting	480	320	240	400	240
With 128 ms EC	400	320	240	400	240
With SRTP	400	-	240	240	240
With IPM Detectors	400	320	240	400	240
With IPM Detectors & SRTP	320	-	240	240	240
Voice Coder					
Transparent	Yes	Yes	Yes	Yes	Yes
G.711 A/Mu-law PCM	Yes	Yes	Yes	Yes	Yes
G.726 ADPCM	Yes	Yes	Yes	Yes	Yes
G.727 ADPCM	Yes	Yes	Yes	Yes	Yes
G.723.1	Yes	-	-	-	-
G.729 A, B	Yes	Yes	Yes	-	-
GSM FR	Yes	Yes	-	-	-
MS GSM	Yes	Yes	-	-	-
EVRC	-	-	Yes	-	-
QCELP	-	-	Yes	-	-
AMR	-	Yes	-	-	-
GSM EFR	-	Yes	-	-	-
iLBC	-	-	-	-	Yes
EG.711	-	-	-	Yes	Yes

2.5.6 Mediant 3000

The device supports the following DSP firmware templates:

Notes:

- Installation and use of vocoders is subject to obtaining the appropriate license and to royalty payments.
- Number of channels refers to the device's maximum channel capacity.
- For other DSP template configurations, please contact AudioCodes.

Table 2-21: DSP Firmware Templates for Mediant 3000

			DSP Template								
			0	**1**	**2**	**4**	**5**	**7**	**9**	**10**	**11**
Supplementary Capabilities			**Number of Channels**								
SRTP	**ARIA**	**RTCP XR**									
-	-	-	2016	2016	1764	1260	1260	1638	1008	1512	630
-	-	Yes	1890	1890	1638	1134	1134	1638	1008	1386	630
Yes	-	-	1764	-	-	-	-	1638	1008	-	630
Yes	-	Yes	1638	-	-	-	-	1512	1008	-	630
Yes	Yes	-	1638	-	-	-	-	1638	1008	-	504
Yes	Yes	Yes	1638	-	-	-	-	1638	1008	-	504
Voice Coders											
AMR			-	Yes	-	Yes	-	-	-	-	-
AMR-WB			-	-	-	Yes	-	-	-	-	-
EVRC			-	-	Yes	-	Yes	-	-	-	-
EVRC-B			-	-	-	-	Yes	-	-	-	-
G.711 A/Mu-law PCM			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
G.722			-	-	-	Yes	-	-	-	Yes	Yes
G.723.1			Yes	-	-	-	-	-	-	-	-
G.726 ADPCM			Yes	Yes	Yes	Yes	Yes	Yes	-	-	-
G.727 ADPCM			Yes	Yes	Yes	Yes	Yes	Yes	-	-	-
G.729 A, B			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GSM EFR			-	Yes	-	Yes	-	-	-	-	-
GSM FR			Yes	Yes	-	Yes	-	-	-	-	-
iLBC			-	-	-	-	-	Yes	-	-	-
MS GSM			Yes	Yes	-	Yes	-	-	-	-	-
EG.711			-	-	-	-	-	Yes	-	-	-
MS RTA (NB)			-	-	-	-	-	-	Yes	-	Yes
MS RTA (WB)			-	-	-	-	-	-	-	-	Yes
T.38 Version 3			-	-	-	-	-	-	-	Yes	-

Table 2-22: DSP Firmware Templates for Mediant 3000 16E1/21T1

			DSP Template								
			0	1	2	4	5	7	9	10	11
Supplementary Capabilities			Number of Channels								
SRTP	ARIA	RTCP XR									
-	-	-	480	480	480	360	360	468	288	432	150
-	-	Yes	480	480	468	324	324	468	288	396	150
Yes	-	-	480	-	-	-	-	468	288	-	150
Yes	-	Yes	468	-	-	-	-	432	288	-	150
Yes	Yes	-	468	-	-	-	-	396	288	-	120
Yes	Yes	Yes	468	-	-	-	-	396	288	-	120
Voice Coders											
AMR			-	Yes	-	Yes	-	-	-	-	-
AMR-WB			-	-	-	Yes	-	-	-	-	-
EVRC			-	-	Yes	-	Yes	-	-	-	-
EVRC-B			-	-	-	-	Yes	-	-	-	-
G.711 A/Mu-Law PCM			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
G.722			-	-	-	Yes	-	-	-	Yes	Yes
G.723.1			Yes	-	-	-	-	-	-	-	-
G.726 ADPCM			Yes	Yes	Yes	Yes	Yes	Yes	-	-	-
G.727 ADPCM			Yes	Yes	Yes	Yes	Yes	Yes	-	-	-
G.729 A, B			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GSM EFR			-	Yes	-	Yes	-	-	-	-	-
GSM FR			Yes	Yes	-	Yes	-	-	-	-	-
iLBC			-	-	-	-	-	Yes	-	-	-
MS GSM			Yes	Yes	-	Yes	-	-	-	-	-
EG.711			-	-	-	-	-	Yes	-	-	-
MS RTA (NB)			-	-	-	-	-	-	Yes	-	Yes
MS RTA (WB)			-	-	-	-	-	-	-	-	Yes
T.38 Version 3			-	-	-	-	-	-	-	Yes	-

2.5.6.1 DSP Template Mix Feature for Mediant 3000

Mediant 3000 can operate (and be loaded) with up to two DSP templates. The channel capacity per DSP template is approximately 50%, with alignment to the number of DSP's present in the device.

Table 2-23: Template Mix Feature Channel Capacity

DSP Template Mix	Number of Channels
	Mediant 3000
1 (AMR) / 2 (EVRC)	960/924
1 (AMR) / 5 (EVRCB)	768/780
1 (AMR) / 7 (iLBC)	864/936

Reader's Notes

3 Known Constraints

This section lists known constraints in Release 6.2.

Note for Mediant 1000 MSBG:

When upgrading from Version 5.8 to Version 6.0, ensure that you use firmware file version F6.00AL.003.015 or later. Previous 6.0 firmware versions cause loss of IP connectivity when DHCP is enabled (default). If you use a previous 6.0 firmware version, ensure that you disable DHCP or that a DHCP serve exists.

Note for Mediant 2000:

Software version 4.6 and later cannot be loaded to Mediant 2000 with an 8-span TPM operating with a 64-MByte RAM. In addition, regardless of the amount of spans, Mediant 2000 with 64-MByte on-board memory can't be upgraded to 5.8 or later.

3.1 SIP Constraints

This release includes the following known SIP constraints:

1. IP media features such as play and/or record of announcements, and conferencing are not supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

2. The SBC application does not support termination of REFER\3xx\Hold\Re-INVITE.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3. The ICMP protocol is not supported. The device is unable to generate ICMP PING packets. The SIP Gateway Alternative Routing feature using PING packets is not supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

4. T.38 fax relay using the same port as RTP (T38UseRTPport = 1) is not supported.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

5. For the IP-to-IP application, since the back-to-back user agent (B2BUA) mode is based on full termination at each leg, some 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

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

6. High Transcoding probability (devices other than MSBG always perform transcoding).

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3.2 Media Constraints

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

1. The RTP payload size on RTP forwarding in the SBC application cannot exceed 1,000 bytes. A workaround for this constraint is to reduce the MTU to less than 1,000 bytes on remote endpoints.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

2. If the initial transcoding session has one side using a narrowband coder (e.g. G.711), modifying the transcoding connection to wideband coders still results in narrowband voice quality. A workaround for this constraint is to ensure that the entire session uses wideband coders.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

4. When the device is assembled with eight trunks (240 channels) and using the G.729 or G.711 coder with sample interval of 10 ms, the channel capacity is reduced to seven trunks (or 210 channels).

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☒ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

5. When performing an IP-to-IP call with a wideband (WB) coder on each leg, if the Fax/Modem Transport type for one of the legs is not Transparent, the interconnection is made using a narrowband coder, therefore, the wideband quality of the call is not maintained. The user should avoid setting any Fax/Modem enhanced capabilities on WB IP-to-IP calls for which the user wants to maintain wideband quality.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

6. Announcements and streaming cannot be performed on IP-to-IP wideband calls.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

7. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

8. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

9. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

10. 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.

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

11. To change the DSP template, either the Mixed Template table or the DSP Template single values can be used.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

12. 30 msec RTP frames using the EG.711 coder is not supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

13. Playback with duration set to less than 20 msec is not supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

14. RTCP XR is not supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

15. When using IP-to-IP mediation, the channel capacity may be reduced.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3.3 PSTN Constraints

This release includes the following known PSTN constraints:

1. All the device's trunks must belong to the same Protocol Type (i.e., either E1 or T1).

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

2. 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).

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3. 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).

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

4. When configuring the device with E1 trunks, negotiation of CRC4 (for either EXTENDED_SUPER_FRAME or E1_FRAMING_MFF_CRC4_EXT framing methods) should not be used. A framing method other than EXTENDED_SUPER_FRAME and E1_FRAMING_MFF_CRC4_EXT must be selected.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3.3.1 DS3 Constraints

This release includes the following known DS3 constraints:

1. The BIT voice path can fail when using the DS3 interface.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

2. When the DS3 interface is not connected, a trunk under this DS3 interface can appear in either LOF or AIS alarm state.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3. The DS3 External clock is not relevant for Asynchronous mapping of DS3 in OC3.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3.3.2 SDH Constraints

This release includes the following known SDH constraints:

1. TU-11 Byte Synchronous mapping is not supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

2. For SDH/SONET and DS3 interfaces, if a trunk was in LOF alarm and the alarm was then cleared, the trunk tends to revert to the RAI alarm for a short period before moving to “no alarm” state.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3. In STM-1 and OC3 configurations, path alarms do not show the correct state if the higher level is not synchronized. For example, if there is no LOS on both PSTN Port A and Port B, the path level displays "No Alarm".

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3.3.3 SS7 Constraints

This release includes the following known SDH constraints:

1. SS7 capacity limitations:
   - Up to 2 signaling nodes can be configured per device.
   - Up to 2 Alias Point Codes can be configured per signaling node, but only 1 signaling node can be configured with Alias Point Codes.
   - Up to 64 signaling links can be configured per device.
   - Up to 32 link-sets can be configured per signaling node.
   - Up to 8 links can be configured per link-set.
   - Up to 30 route-sets can be configured per signaling node.
   - Up to 4 link-sets can be configured per route-set (routes per route-set).

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

2. SS7 MTP3 Signaling Node (SN) Redundancy Limitations:
   - Up to two blades can be configured as Shared Point Code.
   - Blade redundancy parameters cannot be changed on-the-fly (except for SS7MTP3RdcyTblSyncInterval).
   - The Add & Delete commands can be performed on the SN-Blade Table Configuration when the SN is set to Offline.
   - *ini* file configurations after reset are not relayed to remote devices.
   - SN operations (InService/Start/Stop) are local to the device they are performed on.
   - On-the-fly configurations that are performed on one device are passed only to the remote devices that established a TCP connection with that device. (For this reason, redundancy SN-Blade table configurations are not passed between the new device that is configured and the other device.)
   - SS7 operations that are performed on one device are passed only to the remote devices that have an InService x-link to that device.

- SS7 and UAL configuration must be the same on devices that share the same Point Code.
- On-the-fly configuration of a link (Create/InService/Offline/Delete) must be performed from the device that the link physically belongs to.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3. The following tables cannot be configured in offline configuration mode: SN_Timers, LinkSet_Timers and MTP2_Parms. (Offline configuration mode is used in configuring SS7 using ini file via Web interface - restore all defaults, load ini to the device and reset with burn).

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3.4 IP Media Constraints

This release includes the following known IP media constraints:

1. Playback to the IP side of LBR Voice Prompts:
   - Sending DTMF signals present in the file as RFC 2833 is not supported during playback, i.e., if the file/voice prompt contains digits, they are passed as voice and not as RFC 2833.
   - Generation of signals to the IP during playback is not possible.
   - If the user wishes to pass DTMF signals present in the file over RFC 2833, or generate in-band signals towards the network during playback, the user must convert the LBR file into an HBR file (G.711 Alaw or G.711 uLaw).

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

2. Voice Prompts files larger than 1 Mbyte cannot be permanently stored on flash memory. Therefore, they are loaded directly to the RAM and must be loaded again after the device is reset.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3. When playing or recording an announcement when using a variable rate coder, the configured MSCML offset must be set to zero.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

4. No option to detect the beginning and end of speech and therefore, the signal is unable to start or stop recording accordingly. This means that the MSCML play/record function ("endsilence" attribute) is supported only when PRT (pre-recording time) and PST (post-recording time) value equals 0.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

5. The number of simultaneous recorded voice channels is limited by the HTTP server's capability. This capacity can be less than the capacity supported by the device.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

6. The "Regular Expression Digitmaps" MSCML feature is not supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3.5 Networking Constraints

This release includes the following known networking constraints:

1. Enabling the UDP checksum calculation is not applied to CALEA and IP-to-IP calls with UDP connections. The UDP checksum field is set to zero in these cases.

Product	
☐ MP-11x	☒ MP-124
☐ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

2. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3. 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).

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

4. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3.6 Security Constraints

This release includes the following known security constraint:

1. IPSec tunnels work with pre-shared secrets but not with certificates. The option for certificate authentication exists on the IPSec configuration Web page, but the IKE negotiation does not proceed beyond ISAKMP Main Mode. A workaround for this constraint is to use pre-shared key authentication.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

2. The following CLI commands don’t function with SHDSL-ATM interfaces:
   - show data interfaces
   - show data ip interface
   - show data qos match-map
   - show data hosts

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3. Once SecureStartup mode is enabled, it can't be disabled correctly thereafter. Attempting to revert to non-Secure startup causes all parameters to return to defaults.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

4. The SSH session closes when issuing the **cf get** CLI command to write the entire configuration file to the SSH session. A workaround for this constraint is to use the **cf view** CLI command to view the configuration file with page breaks.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3.7 High Availability Constraints

This release includes the following known Mediant 3000 High Availability (HA) constraints:

1. The Graceful Lock feature does not function when HA is enabled. Attempting to do so causes errors in the Syslog.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

2. When using IPSec for control protocol transport, the device may experience a large bulk of Syslog error messages during switchover. These messages can be ignored as the switchover should succeed and the connection with the softswitch is restored.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3. During HA switchover, the APS active interface status (e.g., PSTN-B is currently "Active" and PSTN-A is "Inactive") is not transferred to the redundant blade. As a result, if the PSTN-B interface was active before switchover, PSTN-A can be active after switchover. The information regarding which interface is active is not maintained after switchover.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

4. The Voice Prompt file needs be reloaded to the device after the Hitless software upgrade has completed.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3.8 Infrastructure Constraints

This release includes the following known infrastructure constraints:

1. When configuring the Syslog parameters through the WAN interface (i.e., Syslog server IP address and enable/disable Syslog messages), error, notice, or debug messages may appear in the log (e.g., syslog/rs232). These messages should be ignored.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

2. When using BITS with line-synch mode, only APS protected mode is supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3. 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

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

4. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

5. Files loaded to the device must not contain spaces in their file name. Including spaces in the name prevents the file from being saved to the device's flash memory (or copied to the redundant blade – for Mediant 3000 HA).

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3.9 Management Constraints

3.9.1 Web Constraints

This release includes the following known Web constraints:

1. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

2. Caller ID types that are not supported appear in the list. The DTMF Caller ID types appear in the list of possible caller IDs even though they are not supported for these products. A workaround for this constraint is to ensure that the selected caller ID is indeed supported

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3. The Trunk Settings page has some graphic issues. For example, the **Submit** button appears in the middle of the page.

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

4. 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.

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

5. When performing a software upgrade using the Software Upgrade wizard, if the user selects the check box for using the existing file, the **Send File** button should become unavailable. However, it remains active. A workaround for this constraint is not to click this button.

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

6. On the Home page, when only the digital module is assembled, the analog legend describing the icon color codes also appears.

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

7. The **Help** icon on the toolbar is applicable only for the non-data pages. Clicking it when a data page is displayed will show the last help topic that was opened.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

8. A monitoring-only Web user ("User Monitor") is a read-only user that cannot perform any configuration or actions. However, some of the action buttons such as **Burn** and **Submit** are not disabled when in this mode. Note that clicking these buttons results in an error message, and the action will not be performed.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

9. The horizontal scroll bar is missing in the Connection Status page (**Status & Diagnostics** tab > **Data Status** menu > **Connection Statistics**). This results in some loss of information at the end of the line.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

10. When creating a scenario, some of the Web pages cannot be added to it.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

11. 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.

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

12. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

13. On the Configuration > SS7 Configuration > SN > Linkset > Linkset-link > View link, an incorrect link appears. Sometimes a non-configured link is displayed or a link that is connected to another linkset is displayed.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

14. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

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

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

16. On some SS7 Web pages, all available buttons become visible for a split second while the page is loaded, even though they should not appear.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

17. On the 'IP Settings' page, adding an interface with invalid characters (e.g., <, >, ", and ') may result in a corrupted Web page. Submitting the corrupted Web page may result in unexpected behavior such as no response from the device.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

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

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3.9.2 SNMP Constraints

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

1. When configuring acSysInterfaceTable using SNMP or the Web interface, validation is performed only after device reset.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

2. The DS3 ifAdmin-State field cannot be changed in the IF-Table, using SNMP.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

3. When setting snmpTargetAddrTagList to NULL (by removing a row in the snmpTargetAddrTable) without changing the corresponding entry in the snmpCommunityTable, an inconsistency occurs when a switchover occurs between the Active and Redundant blades. In the Active blade, the object appears with a NULL value; in the Redundant blade, a non-NULL value appears.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

4. In the DS3/E3 Current Table, the objects dsx3CurrentSEFSs and dsx3CurrentUASs are not supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

5. In the DS3/E3 Interval Table, the following objects are not supported: dsx3IntervalPSESs and dsx3IntervalSEFSs.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

6. The dsx3Total Table is not supported.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

7. 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.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

8. The Admin State does not change to “Redundant”.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

3.9.3 CLI Constraints

This release includes the following known command-line interface (CLI) constraints:

1. When connecting to the device using Telnet (CLI), Syslog messages do not appear by default. The **Show Log** command can be used to enable this feature.

Product	
☒ MP-11x	☒ MP-124
☒ Mediant 600	☒ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

4 Resolved Constraints

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

4.1 SIP Resolved Constraints

The following SIP constraints from previous releases have been resolved:

1. The On-Board, Three-Way Conferencing feature is not supported when using SRTP.

Product	
☒ MP-11x	☒ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

2. The device does not support On-Board Three-Way Conferencing and three-way conferencing using a third-party Conference server, simultaneously.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☒ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☐ Mediant 2000	
☐ Mediant 3000/TP-6310	☐ Mediant 3000 HA/TP-6310
☐ Mediant 3000/TP-8410	☐ Mediant 3000 HA/TP-8410

4.2 Web Resolved Constraints

The following Web constraints from previous releases have been resolved:

1. The AnalogSignalTransportType parameter appears.

Product	
☐ MP-11x	☐ MP-124
☐ Mediant 600	☐ Mediant 1000
☐ Mediant 800 MSBG	☐ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

2. Clicking the **Submit** button in the 'CAS State Machines' page sometimes causes a "Page Not Found" error.

Product	
☐ MP-11x	☐ MP-124
☒ Mediant 600	☒ Mediant 1000
☒ Mediant 800 MSBG	☒ Mediant 1000 MSBG
☒ Mediant 2000	
☒ Mediant 3000/TP-6310	☒ Mediant 3000 HA/TP-6310
☒ Mediant 3000/TP-8410	☒ Mediant 3000 HA/TP-8410

Reader's Notes

AudioCodes

Release Notes Ver. 6.2

www.audiocodes.com