Enterprise Session Border Controllers (E-SBC)

Multi-Service Business Gateways

VoIP Media Gateways

SIP CPE Release Notes

Release 6.4, Version 13.5

SAS
Stand Alone Survivability
Continuous VoIP Service

MSBG
AudioCodes
Multi-Service
Business Gateway

HD VoIP
Sounds Better

March 2012

Document #: LTRT-26905

AudioCodes

Table of Contents

List of Tables

Reader's Notes

Notice

This document describes the features of Release 6.4 for AudioCodes SIP CPE products, as well as features of Release Version 13.5 for the Mediant 4000 E-SBC and Mediant Software E-BSC.

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: March-15-2012

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 generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), 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
Mediant 600 SIP Installation Manual
Mediant 800 MSBG SIP Installation Manual
Mediant 800 MSBG SIP User's Manual
Mediant 800 Gateway and E-SBC SIP Installation Manual
Mediant 800 Gateway and E-SBC SIP User's Manual
Mediant 1000 SIP Installation Manual
Mediant 600 & Mediant 1000 SIP User's Manual
Mediant 1000 MSBG SIP Installation Manual
Mediant 1000 MSBG SIP User's Manual
Mediant 1000 Gateway and E-SBC SIP Installation Manual
Mediant 1000 Gateway and E-SBC SIP User's Manual
Mediant 3000 SIP Installation Manual
Mediant 3000 SIP User's Manual
Mediant 4000 E-SBC Installation Manual
Mediant 4000 E-SBC User's Manual
Mediant 4000 E-SBC Quick Guide
Mediant Software E-SBC Installation Manual
Mediant Software E-SBC User's Manual
MSBG Series CLI Reference Guide

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

1 Introduction

This document describes the release of Version 6.4. This includes new products, existing products and their hardware features (existing and new), products not supported in this release, and new software-related features.

It describes new and existing products and hardware platforms, as well as new, modified, and obsolete features and configuration parameters. It also provides the known constraints for this release and constraints from the previous release that have now been resolved.

Notes:

- Some of the features mentioned in this document are available only if the relevant software License Key has been purchased from AudioCodes and is installed on the device. For a list of available software license keys that can be purchased, consult your AudioCodes sales representative.
- For Mediant 800 MSBG and Mediant 1000 MSBG, open source software may have been added and/or amended for this product. For further information, visit our web site at: http://audiocodes.com/support or contact your AudioCodes sales representative.
- Updates to this document may be made due to significant information discovered after the release or too late in the release cycle to be otherwise included in the this release documentation. You can check for an updated version on our Web site as a registered customer at http://www.audiocodes.com/downloads.

Reader's Notes

2 New and Existing Products and Hardware Platforms

This section describes the supported products and hardware configurations in Release 6.4.

2.1 New Products

2.1.1 Mediant 800 Gateway & E-SBC

The Mediant 800 media gateway and session border controller (SBC) enables connectivity and security between small and medium businesses (SMB) and service providers' VoIP networks. The Mediant 800 SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and service assurance for service quality and manageability.

The Mediant 800 media gateway functionality is based on field-proven VoIP services and provides the following telephony interfaces:

- Up to 6 RJ-45 E&M port interfaces
- 1 x E1/T1 port interface (over single copper wire pair)
- Up to 4 BRI ports (supporting up to 8 voice channels)
- Up to 12 FXS port interfaces
- Up to 8 FXO port interfaces

The Mediant 800 also offers up to 12 LAN Ethernet interfaces (up to 4 Gigabit Ethernet ports and up to 8 Fast Ethernet ports). These ports operate in port-pair redundancy, providing up to 6 port-pair groups.

The Mediant 800 provides an Open Solutions Network (OSN) server platform for hosting third-party applications such as IP PBX.

The available Mediant 800 models are listed in the table below:

Table 2-1: Available Models for Mediant 800

Model	FXS	FXO	BRI	E&M	E1/T1	LAN [1] GbE/FE	OSN (CPU) / Storage / RAM
M800-ESBC-12L	-	-	-	-	-	12 (4/8)	-
M800-6E&M-2L-X1	-	-	-	6	-	2 (2/0)	Atom / 160 GB HDD / 2 GB
M800-E-4S-2L	4	-	-	-	-	2 (2/0)	-
M800-E-4S4O-12L-P-X1	4	4	-	-	-	12 (4/8)	Atom / 160 GB HDD / 1 GB
M800-E-4S8O-2L-X1	4	8	-	-	-	2 (2/0)	Atom / 8 GB ASX / 1 GB
M800-E-12S-12L-P	12	-	-	-	-	12 (4/8)	-
M800-E-4O-2L-X1	-	4	-	-	-	2 (2/0)	Atom / 160 GB HDD / 2 GB

[1] The LAN ports operate in pairs, providing LAN port redundancy.

Model	FXS	FXO	BRI	E&M	E1/T1	LAN [1] GbE/FE	OSN (CPU) / Storage / RAM
M800-E-12S-2L-P-2U12	12	-	-	-	-	2 (2/0)[2]	-
M800-E-4S40-2L-P-X1-2U12	4	4	-	-	-	2 (2/0)[2]	Atom
M800-E-1B-12L-P	-	-	1[3]	-	-	12 (4/8)	-
M800-E-2B-12L-P	-	-	2[3]	-	-	12 (4/8)	-
M800-E-3B-12L-P	-	-	3[3]	-	-	12 (4/8)	-
M800-E-4B-12L-P	-	-	4	-	-	12 (4/8)	-
M800-E-4B-12L-P-X1	-	-	4	-	-	12 (4/8)	Atom / 160 GB HDD / 1 GB
M800-E-4B-2L-P-X1-2U12	-	-	4	-	-	2 (2/0)[2]	Atom / 160 GB HDD / 1 GB
M800-E-1B-2L-P-2U12	-	-	1[3]	-	-	2 (2/0)[2]	-
M800-E-2B-2L-P-2U12	-	-	2[3]	-	-	2 (2/0)[2]	-
M800-E-3B-2L-P-2U12	-	-	3[3]	-	-	2 (2/0)[2]	-
M800-E-4B-2L-P-2U12	-	-	4	-	-	2 (2/0)[2]	-
M800-E-1ET-12L-P	-	-	-	-	1	12 (4/8)	-
M800-E-1ET-2L-P-2U12	-	-	-	-	1	2 (2/0)[2]	-
M800-E-1ET8S-12L-P	8	-	-	-	1	12 (4/8)	-
M800-E-1ET4S4O-12L-P	4	4	-	-	1	12 (4/8)	-

[2] Software upgradable to 12 LANs (4/8) by ordering relevant Feature Key (once enabled, the additional 10 LAN ports can be used by removing their protective plastic covers).

[3] Software upgradable to 4 BRI ports by ordering relevant Feature Key (once enabled, the additional BRI ports can be used by removing their protective plastic covers).

2.1.2 Mediant 1000B Gateway & E-SBC

The Mediant 1000B media gateway and session border controller (SBC) enables connectivity and security between small and medium businesses (SMB) and service providers' VoIP networks.

The Mediant 1000B SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and service assurance for service quality and manageability.

The Mediant 1000B media gateway functionality is based on field-proven VoIP services, providing the following telephony modules:

- Up to 4 TRUNKS modules (1, 2, or 4 E1/T1/J1 PRI spans per module).
- Up to 5 BRI modules (4 BRI ports per module)
- Up to 6 FXO modules (4 FXO ports per module)
- Up to 6 FXS modules (4 FXS ports per module)
- Up to 3 MPM modules for media processing such as announcements and conferencing
- Up to 6 LAN Ethernet interfaces (2 interfaces on a CRMX module and an additional 4 interfaces provided by a LAN Expansion module). These ports provide up to 3 port-pair redundancy groups.

The Mediant 1000B also supports an Open Solutions Network (OSN) server platform for hosting third-party applications such as IP PBX.

2.1.3 Mediant 4000 E-SBC

The Mediant 4000 is a member of AudioCodes family of Enterprise Session Border Controllers (E-SBC), enabling connectivity and security between enterprises and voice-over-IP (VoIP) networks of Internet Telephony Service Providers (ITSP).

This release supports the following existing hardware:

- The Mediant 4000 is designed as a modular, 1U chassis.
- A single AudioCodes Full-Height AMC module running the session border controller (SBC) application, consisting of the following:
  - 1.25 GHz multi-core CPU
  - Eight Ethernet 10/100/1000Base-T ports, supporting four groups of redundant pairs (1+1), auto-negotiation, half- and full-duplex modes, and straight-through and crossover cable detection
  - DSP module (will be applicable only in the next release)
- 1+1 power load-sharing and redundancy using two Power Supply modules
- 1+1 High Availability using two Mediant 4000 devices

2.1.4 Mediant Software E-SBC

AudioCodes' Mediant Software Enterprise Session Border Controller (E-SBC) is a pure-software, server-based product enabling connectivity and security between Enterprises' and Service Providers' Voice-over-IP (VoIP) networks. The Mediant Software E-SBC provides perimeter defense as a way of protecting companies from malicious VoIP attacks; mediation for allowing the connection of any PBX and / or IP-PBX to any Service Provider; and service assurance for service quality and manageability.

The Mediant Software E-SBC package shipped to customers includes a CD containing Mediant Software E-SBC, AudioCodes utilities, and related documentation. The installation of the E-SBC software must be done according to the instructions in the *Mediant Software E-SBC Installation Manual*.

Software is to be installed on the following server:

- **Platform:** HP ProLiant DL120 G7
- **Processor:** Intel Xeon E3-1220 (8M Cache, 3.10 GHz), 4 Cores
- **Memory:** 8 GB
- **Disk space:** 72 GB or more
- **CD-ROM:** Local
- **CLI support:**
  - VGA monitor and keyboard
  - RS-232 serial port (optional

2.2 Existing Products

This section lists the products from the previous release that are also supported in Release 6.4. In addition, this section describes their new hardware configurations (if any).

2.2.1 Mediant 600

Mediant 600 continues to be supported in Release 6.4.

2.2.1.1 New Hardware

This release introduces no new hardware configurations for Mediant 600.

2.2.1.2 Existing Hardware

This release supports the following existing hardware:

- Up to 2 digital Trunk modules (1 or 2 E1/T1/J1 PRI spans, including fractional E1/T1)
- Up to 2 BRI modules (where each module provides 4 to 8 BRI ports)
- Up to 2 FXS modules (where each module provides 4 FXS interfaces)
- Up to 2 FXO modules (where each module provides 4 FXO interfaces)

These interfaces are available in one of the following hardware 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

2.2.2 Mediant 800 MSBG

Mediant 800 MSBG continues to be supported in Release 6.4.

2.2.2.1 New Hardware

This release introduces the following new hardware features:

- Various power budgets (120 and 50 Watt) for Power over Ethernet (PoE IEEE 802.3af-2003) on the LAN ports – see Section 3.2.10 on page 52 for more information on this new feature
- ADSL / VDSL WAN port interface – see Section 3.2.8 on page 50 for more information on this new feature
- 3G Cellular WAN access (primary or backup) using a USB modem – see Section 3.2.8 on page 50 for more information on this new feature

Table 2-2: New Available Models for Mediant 800 MSBG

Model	FXS	FXO	BRI	T1/E1	LAN GE/FE	WAN	PoE	OSN (CPU) / Storage / RAM
M800-4S4O4B-12L-P-AVDSL-A	4	4	4	-	12 (4/8)	AVDSL-A	120W	-
M800-1ET8S-12L-P-2T	8	-	-	1	12 (4/8)	2 x T1	120W	-
M800-1ET4S4O-12L-P-2T	4	4	-	1	12 (4/8)	2 x T1	120W	-
M800-1ET8S-12L-P-4SHDSL	8	-	-	1	12 (4/8)	4 x SHDSL	120W	-
M800-8B-12L-P-AVDSL-A	-	-	8	-	12 (4/8)	AVDSL-A	120W	-
M800-4S4O4B-12L-P-AVDSL-B	4	4	4	-	12 (4/8)	AVDSL-B	120W	-

2.2.2.2 Existing Hardware

This release supports the following existing hardware:

- 1 x E1/T1 port interface (over single copper wire pair)
- Up to 4 BRI ports (supporting up to 8 voice channels)
- Up to 12 FXS port interfaces
- Up to 12 FXO port interfaces
- FXS 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.
- Up to 12 Ethernet LAN ports:
  - Up to 4 RJ-45 10/100/1000Base-T (Gigabit) ports
  - Up to 8 RJ-45 10/100Base-TX (Fast Ethernet) ports

- Available WAN interface types:
  - 1 x Ethernet copper WAN port (10/100/1000Base-T).
  - 1 x Symmetric High-Speed Digital Subscriber Line (SHDSL) WAN port (providing 4 SHDSL WAN ports housed on a single R-J45 connector):
    - ATM:
      - ✓ RFC 2684 in Routed (IPoA) and Bridged (ETHoA) modes, supporting LLC-SNAP and VC-Multiplexed encapsulations over AAL5
      - ✓ ATM UNI 4.1 compliant
      - ✓ UBR, CBR, VBR classes of service
      - ✓ 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
      - ✓ 802.1q VLANs over EFM
      - ✓ PPPoE
  - 1 x T1 WAN DSU/CSU port
- Power over Ethernet (PoE) supported on all LAN ports, complying with IEEE 802.3af-2003.
- OSN server platform (OSN3 and HDMX modules) for hosting third-party applications (such as an IP PBX).
- 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).

The available Mediant 800 MSBG models from the previous release with continued support in Release 6.4 are listed in the table below:

Table 2-3: Existing Available Models for Mediant 800 MSBG

Model	FXS	FXO	BRI	T1/E1	LAN GbE/FE	WAN	PoE	OSN (CPU) / Storage / RAM
M800-4S-2L	4	-	-	-	2 (2/0)	GbE	-	-
M800-4S4O-12L-P-X1	4	4	-	-	12 (4/8)	GbE	50W	Atom / 160 GB HDD / 1 GB
M800-4S8O-2L-X1	4	8	-	-	2 (2/0)	GbE	-	Atom / 8 GB ASX / 1 GB
M800-12S-12L-P	12	-	-	-	12 (4/8)	GbE	120W	-
M800-4O-2L-X1	-	4	-	-	2 (2/0)	GbE	-	Atom / 160 GB HDD / 2 GB
M800-12S-2L-P-2U12	12	-	-	-	2 (2/0)[4]	GbE	120W	-
M800-4S40-2L-P-X1-2U12	4	4	-	-	2 (2/0)[4]	GbE	50W	Atom

[4] Software upgradable to 12 LANs (4/8) by ordering relevant Feature Key (once enabled, the additional 10 LAN ports can be used by removing their protective plastic covers).

Model	FXS	FXO	BRI	T1/E1	LAN GbE/FE	WAN	PoE	OSN (CPU) / Storage / RAM
M800-1B-12L-P	-	-	1[5]	-	12 (4/8)	GbE	120W	-
M800-2B-12L-P	-	-	2[5]	-	12 (4/8)	GbE	120W	-
M800-3B-12L-P	-	-	3[5]	-	12 (4/8)	GbE	120W	-
M800-4B-12L-P	-	-	4	-	12 (4/8)	GbE	120W	-
M800-4B-12L-P-X1	-	-	4	-	12 (4/8)	GbE	120W	Atom / 160 GB HDD / 1 GB
M800-4B-2L-P-X1-2U12	-	-	4	-	2 (2/0)[4]	GbE	120W	Atom / 160 GB HDD / 1 GB
M800-1B-2L-P-2U12	-	-	1[5]	-	2 (2/0)[4]	GbE	120W	-
M800-2B-2L-P-2U12	-	-	2[5]	-	2 (2/0)[4]	GbE	120W	-
M800-3B-2L-P-2U12	-	-	3[5]	-	2 (2/0)[4]	GbE	120W	-
M800-4B-2L-P-2U12	-	-	4	-	2 (2/0)[4]	GbE	120W	-
M800-1ET-12L-P	-	-	-	1	12 (4/8)	GbE	120W	-
M800-1ET-2L-P-2U12	-	-	-	1	2 (2/0)[4]	GbE	120W	-
M800-4B-12L-P-4SHDSL	-	-	4	-	12 (4/8)	4 x SHDSL	120W	-
M800-4B-2L-P-4SHDSL-2U12	-	-	4	-	2 (2/0)[4]	4 x SHDSL	120W	-
M800-1B-12L-P-4SHDSL	-	-	1[5]	-	12 (4/8)	4 x SHDSL	120W	-
M800-2B-12L-P-4SHDSL	-	-	2[5]	-	12 (4/8)	4 x SHDSL	120W	-
M800-3B-12L-P-4SHDSL	-	-	3[5]	-	12 (4/8)	4 x SHDSL	120W	-
M800-1B-2L-P-4SHDSL-2U12	-	-	1[5]	-	2 (2/0)[4]	4 x SHDSL	120W	-
M800-2B-2L-P-4SHDSL-2U12	-	-	2[5]	-	2 (2/0)[4]	4 x SHDSL	120W	-
M800-3B-2L-P-4SHDSL-2U12	-	-	3	-	2 (2/0)[4]	4 x SHDSL	120W	-
M800-12L-P-4SHDSL	-	-	-	-	12 (4/8)	4 x SHDSL	120W	-
M800-2L-P-4SHDSL-2U12	-	-	-	-	2 (2/0)[4]	4 x SHDSL	120W	-

[5] Software upgradable to 4 BRI ports by ordering relevant Feature Key (once enabled, the additional BRI ports can be used by removing their protective plastic covers).

2.2.3 Mediant 1000

Mediant 1000 continues to be supported in Release 6.4.

2.2.3.1 New Hardware

No new hardware has been introduced in this release for Mediant 1000.

2.2.3.2 Existing Hardware

This release supports the following existing hardware:

- Up to 4 digital Trunks modules (1, 2, or 4 E1/T1/J1 PRI spans)
- Up to 5 BRI modules (where each module provides 4 BRI ports)
- Up to 6 FXS modules (where each module provides 4 FXS interfaces)
- Up to 6 FXO modules (where each module provides 4 FXO interfaces)
- Up to 3 MPM modules for media processing such as announcements and conferencing
- OSN server platform for hosting third-party applications (such as an IP PBX), available in one of the following types:
  - OSN1 (Ver. 1) - Intel™ Celeron™ 600 MHz
  - OSN2 (Ver. 2) - Intel™ Pentium™ M 1.4 GHz

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

2.2.4 Mediant 1000 MSBG

Mediant 1000 MSBG continues to be supported in Release 6.4.

2.2.4.1 New Hardware

No new hardware has been introduced in this release for Mediant 1000 MSBG.

2.2.4.2 Existing Hardware

This release supports the following existing hardware:

- Up to 4 digital Trunks modules (1, 2, or 4 E1/T1/J1 PRI spans)
- Up to 5 BRI modules (where each module provides 4 BRI ports)
- Up to 6 FXS modules (where each module provides 4 FXS interfaces)
- Up to 6 FXO modules (where each module provides 4 FXO interfaces)
- Up to 3 MPM modules for media processing such as announcements and conferencing
- CRMX module:
  - 3 x Ethernet LAN 10/100/1000Base-T ports
  - 1 x WAN port, available in one of the following configurations, depending on CRMX module type:
    - CRMX-C: RJ-45 port (4-twisted pair copper cabling) providing 1 Gigabit Ethernet (GbE) interface
    - CRMX-S: 1000Base-SX optical fiber port (multi-mode fiber)
    - CRMS-L: 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: SHDS port (providing 4 SHDSL ports on a single physical connector):
  - ✓ ATM:
    - → RFC 2684 in Routed (IPoA) and Bridged (ETHoA) modes, supporting LLC-SNAP and VC-Multiplexed encapsulations over AAL5
    - → ATM UNI 4.1 compliant
    - → UBR, CBR, VBR classes of service
    - → 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
    - → 802.1q VLANs over EFM
    - → PPPoE

- OSN server platform for hosting third-party applications (such as an IP PBX), available in one of the following types:
  - OSN1 (Ver. 1) - Intel™ Celeron™ 600 MHz
  - OSN2 (Ver. 2) - Intel™ Pentium™ M 1.4 GHz
  - OSN3 (Ver. 3) - Intel® Core™ 2 Duo 1.5 GHz processors L7400 with Intel 3100 Chipset (64-bit). Note that this is supported only on the Mediant 1000B chassis.
- Chassis types:
  - Mediant 1000
  - Mediant 1000B - based on the incumbent Mediant 1000 chassis, but provides 8 Advanced Mezzanine Card (AMC) form-factor 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.

2.2.5 Mediant 2000

Mediant 2000 continues to be supported in Release 6.4.

2.2.5.1 New Hardware

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

2.2.5.2 Existing Hardware

This release supports the following existing hardware:

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

2.2.6 Mediant 3000

Mediant 3000 continues to be supported in Release 6.4.

2.2.6.1 New Hardware

This release introduces the following new hardware:

- Depopulated TP-6310 with single DS3 configuration including eight DSPs. This is offered on the following models:
  - M3K1/DC (AC)
  - M3K3/DC (AC)
  - M3K40/ESBC/AC (DC)
  - M3K42/ESBC/AC (DC)

2.2.6.2 Existing Hardware

This release supports the following existing hardware:

- Mediant 3000 hosting a single TP-6310 blade, providing 1+1 SONET/SDH or 3 x T3 PSTN interfaces.
- Mediant 3000 hosting two TP-6310 blades for 1+1 High Availability (HA), providing 1+1 SONET / SDH or 3 x 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 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) for 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) for hosting third-party applications (such as SS7 GWC).

2.3 Products Not Supported in this Release

The following products are not supported in Release 6.4:

- MediaPack Series (MP-11x and MP-124)
- IPmedia 2000
- IPmedia 3000

3 New Software Features

This section describes the new features introduced in Release 6.4 Version 13.5 and the initial Release 6.4.

3.1 Release 6.4 (Version 13.5) SBC Features

Note: The Release 6.4, Version 13.5 is applicable only to **Mediant 4000 E-SBC** and **Mediant Software E-SBC**.

1. **Increase in Maximum SBC Sessions:**

   The maximum number of SBC sessions has been increased:

   - RTP-RTP Sessions:1,800
   - SRTP-RTP Sessions: 900

   Applicable Products: Mediant 4000 E-SBC.

2. **Symmetric SRTP MKI Negotiation per IP Profile:**

   This feature provides support for enabling symmetric MKI negotiation per IP Profile for SBC sessions. This allows the handling of MKI negotiation for calls pertaining to specific entities (e.g., IP Groups).

   A new field has been added in the IP Profile table to support this feature:

   - Enable Symmetric MKI – enables symmetric MKI negotiation

3. **SIP REFER Handling (Call Transfer):**

   SIP UAs may support different versions of the REFER standard and some may not support REFER. This results in interoperability problems, which this feature resolves. It enables configuring specific IP Groups that do not support REFER. For such IP Groups, when the E-SBC receives a REFER request, instead of forwarding it to the IP Group, it handles it locally.

   This feature supports the following:

   - Attended, Unattended, and Semi-attended call transfers
   - Sending INVITE, REFER-notifications, BYE, PRACK and Session Timer on behalf of peer PBXs
   - Advanced routing rules for the new, initiated INVITE
   - Forwarding early media after REFER while trying to avoid transcoding (by sending session update)
   - Interoperate with environments were the different SIP UAs lack basic SIP functionality such as Re-INVITE, UPDATE, PRACK, Delayed Offer, Re-INVITE without SDP.
   - Session updates after connect in order to avoid transcoding

   The new INVITE is sent to the alternative destination according to the IP2IP Routing table. The IP2IP Routing table has been enhanced to route such "re-route" INVITEs differently to regular INVITE routing. For the E-SBC to route INVITEs triggered by REFER, the Call Trigger field must be set to "REFER".

   It is also possible to specify the IP Group that sent the REFER request as matching criteria for the re-routing rule. This is done in the IP2IP Routing table in the Re-Route IP Group ID field. For more information on this feature, see feature number 0.

The existing global parameter, SBCReferBehavior (which defines how the E-SBC handles SIP REFER requests), can now be configured per IP Profile and a new option value, "Handle Locally" was added to this IP Profile parameter to enable this feature:

- **SBCRemoteReferBehavior:**
  - [-1] Not Configured (default) = Handling is according to the settings of the SBCReferBehavior global parameter.
  - [0] Regular = Refer-To header is unchanged.
  - [1] Reroute through SBC = SBC changes the Refer-to header so that the re-routed INVITE is sent through the SBC.
  - [2] Group Name = Sets the host part to the name defined for the IP Group in the IP Group table.
  - [3] Handle Locally = Device handles the REFER request itself without forwarding the REFER request.

4. **Interworking of SIP PRACK Requests:**

This feature provides support to resolve the interoperability problem of inconsistent support for SIP reliable provisional responses (18x), encountered when the E-SBC communicates with different SIP networks. While some endpoints do not support PRACK (RFC 3262), others require it. The E-SBC can be configured to enable sessions between these endpoints.

A new field was added to the IP Profile table to support this feature:

- **SBCPrackMode:** Determines the PRACK mode required at the remote side:
  - [1] Optional = PRACK is optional for these endpoints. For calls destined to these endpoints, PRACK is optional. If required, the E-SBC performs the PRACK process on behalf of the destination endpoint.
  - [2] Mandatory = PRACK is required for these endpoints. Calls from endpoints that do not support PRACK are rejected. Calls destined to these endpoints are also required to support PRACK.
  - [3] Transparent (default) = E-SBC does not intervene with the PRACK process and forwards the request as is.

5. **Handling of SIP 3xx Redirect Responses:**

The E-SBC can handle SIP 3xx responses on behalf of the dialog-initiating UA, and retry the request (e.g., INVITE) using one or more alternative URIs included in the 3xx response. The new request includes SIP headers from the initial request. These include headers such as Diversion, History-Info, P-Asserted-Id, and Priority. The source and destination URIs can be manipulated, using the regular manipulation mechanism.

The new request is sent to the alternative destination according to the IP2IP Routing table. The IP2IP Routing table has been enhanced to route such "re-route" requests differently to regular request routing. For the E-SBC to route requests triggered by 3xx, the Call Trigger field must be set to "3xx".

It is also possible to specify the IP Group that sent the 3xx response as matching criteria for the re-routing rule. This is done in the IP2IP Routing table in the Re-Route IP Group ID field. For more information on this feature, see feature number 0.

The existing global parameter, SBC3xxBehavior (which defines how the E-SBC handles SIP 3xx responses), can now be configured per IP Profile and a new option value, "Handle Locally" was added to this IP Profile parameter to enable this feature:

- **IPProfile_SBCRemote3xxBehavior:**
    - [-1] Not Configured (default) = According to the settings of the SBC3xxBehavior parameter.
    - [0] Transparent = Forwards the SIP Contact header as is.
    - [1] Reroute through SBC = SBC changes the Contact header so that the re-route request is sent through the SBC.
    - [2] Handle Locally = E-SBC handles the 3xx response forwarding the 3xx response.

6. **Interworking of Session Timer Mismatches:**

The SIP standard provides a signaling keep-alive mechanism using Re-INVITES and UPDATES. In certain setups, keep alive may be required by some SIP devices, while for others it may not be supported. This feature enables the E-SBC to resolve this type of mismatch, by performing the keep-alive process on behalf of devices that do not support it.

A new field was added to the IP Profile table to support this feature:

- **SBCSessionExpiresMode:** Determines the required session expires mode at the remote side:
    - [0] Transparent (default) = E-SBC does not interfere with the session expires negotiation.
    - [1] Observer = If the session-expires is present, the E-SBC does not interfere, but maintains an independent timer (for each leg) to monitor the session and disconnects the call if the session is not refreshed on time.
    - [2] Supported = E-SBC enables the session timer with endpoints belonging to this IP Group even if the peer endpoint does not support this capability.
    - [3] Not supported = E-SBC does not allow a session timer with endpoints belonging to this IP Group.

7. **Interworking of SIP Early Media Interworking**:

This feature relates to the handling of SIP early media.

- **Early Media Enabling:**

  Early media can arrive in provisional responses to an INVITE request. This feature determines whether an IP Group can accept early media. The SBC forwards the request for early media for IP Groups that support this capability; otherwise, the SBC terminates it. The SBC refers to this parameter also for features that require early media such as playing ring back tone.

  Provisional responses whose SDP are suppressed are changed to a SIP 180 response. This feature is also supported for delayed offers.

  A new field was added to the IP Profile table to support this feature:

  SBCRemoteEarlyMediaSupport: Determines whether a remote side can accept early media or not.

    - [0] Not Supported = Early media is not supported.
    - [1] Supported = (Default) Early media is supported.

- **Early Media Response Type:**

  This feature determines in which provisional response type (180 or 183) to forward the early media to the caller.

  A new field was added to the IP Profile table to support this feature:

  SBCEarlyMediaResponseType:

  - [0] Transparent = (Default) All early media response types are supported; the E-SBC forwards all responses as is (unchanged).
  - [1] 180 = Early media is sent as 180 response only.
  - [2] 183 = Early media is sent as 183 response only.

- **Multiple 18x support:**

  Determines whether multiple 18x responses (including 180 Ringing, 181 Call is Being Forwarded, 182 Call Queued, and 183 Session Progress) are forwarded to the caller.

  A new field was added to the IP Profile table to support this feature:

  SBCRemoteMultiple18xSupport:

  - [0] Not Supported = Only the first 18x response is forwarded to the caller.
  - [1] Supported = (Default) Multiple 18x responses are forwarded to the caller.

8. **Interworking of Re-INVITE:**

   This feature relates to the handling of SIP Re-INVITE messages.

   - **Interworking of Re-INVITE Method:**

     This feature enables communication between endpoints that generate Re-INVITE requests and those that do not support the receipt of Re-INVITEs. The E-SBC does not forward Re-INVITE requests to IP Groups that do not support it. In such cases, the E-SBC sends a SIP response to the Re-INVITE request, which can be either a success or a failure, depending on whether the E-SBC can bridge the media between the endpoints. The E-SBC can handle Re-INVITEs with or without an SDP body.

   - **Interworking of Re-INVITE SDP:**

     This feature enables communication between endpoints that do not support Re-INVITE requests without SDP and those that require it. The E-SBC generates an SDP offer and inserts it into the incoming Re-INVITE request if it does not contain an SDP, and only then forwards it to the destination endpoint.

   A new field was added to the IP Profile table to support these features:

   SBCRemoteReinviteSupport: Determines whether the destination of the Re-INVITE request supports Re-INVITE messages and if so, whether it supports Re-INVITE with or without SDP:

   - [0] Not Supported = Re-INVITE is not supported.
   - [1] Supported with SDP = Re-INVITE is supported, but only with SDP. If the Re-INVITE arrives without SDP, the E-SBC creates an SDP and adds it to the Re-INVITE.
   - [2] Supported = (Default) Re-INVITE is supported with or without SDP.

9. **Interworking of SIP UPDATE Requests:**

   This feature can enable communication between endpoints that generate UPDATE requests and those that do not support the receipt of UPDATE requests. The E-SBC does not forward UPDATE requests to IP Groups that do not support it. In such cases, the E-SBC sends a SIP response to the UPDATE request, which can be either a success or a failure, depending on whether the E-SBC can bridge the media between the endpoints.

   A new field was added to the IP Profile table to support this feature:

   SBCRemoteUpdateSupport: Determines whether endpoints belonging to a certain IP Profile support the UPDATE method.

   - [0] Not Supported = UPDATE method is not supported.
   - [1] Supported Only After Connect = UPDATE method is supported only after the call is connected.
   - [2] Supported (default) = UPDATE method is supported during call setup and after call establishment.

10. **Interworking Re-INVITE to UPDATE Requests:**

    This feature can enable communication between endpoints that do not support Re-INVITE requests, but that do support the UPDATE method or vice versa. The E-SBC translates the Re-INVITE request to UPDATE request, or vice versa.

    Note that if a Re-INVITE request arrives without SDP, the E-SBC generates SDP and inserts it into the outgoing UPDATE request.

    To enable this feature, each IP Group needs to be configured with its capabilities, using the IP Profile table (which is associated with the IP Group). For example, an IP Group that supports UPDATE requests but not Re-INVITEs, would be configured as follows:

    - SBCRemoteUpdateSupport = 2 (Supported)
    - SBCRemoteReinviteSupport = 0 (Not Supported)

    If a Re-INVITE request needs to be forwarded to this IP Group, it will be translated to an UPDATE request.

11. **Interworking of Delayed Offer:**

    This feature allows sessions between endpoints that send INVITEs without SDP (delayed media) and endpoints that do not support receipt of INVITEs without SDP. The E-SBC creates an SDP and adds it to INVITEs that arrive without SDP. This intervention in the SDP offer/answer process may require transcoding (currently, not supported). Delayed offer is also supported when early media is present.

    A new field was added to the IP Profile table to support this feature:

    SBCRemoteDelayedOfferSupport: Determines whether the remote endpoints support delayed offer (i.e., initial INVITEs without an SDP offer):

    - [0] Not Supported = Initial INVITE requests without SDP are not supported.
    - [1] Supported = (Default) Initial INVITE requests without SDP are supported.

    Note: For this feature to function properly, a valid Extension Coders Group ID needs to be configured for IP Profiles that do not support delayed offer.

12. **Re-Routing SIP Requests using IP2IP Routing Table Rules:**

    This feature complements the features that enable the re-routing of requests (e.g., INVITE) after SIP 3xx or REFER, using different routing rules than for regular requests. The following new fields have been added to the IP2IP Routing table to support this re-routing of requests:

    - **Call Trigger:** Defines the reason (trigger) for re-routing the request:
        - Any (default) – This routing rule is used for all scenarios (re-routes and non-re-routes)
        - 3xx - The re-route rule is used to route the request if it was triggered as a result of a SIP 3xx response
        - REFER – The re-route rule is used to route the INVITE if it was triggered as a result of a REFER request
        - 3xx or REFER – same as above for 3xx and REFER options
        - Initial Only – This routing rule is used for regular requests that the E-SBC forwards to destination. This rule is not used for re-routing of requests triggered by the receipt of REFER or 3xx.
    - **Reroute IP Group ID:** Specifies the IP Group that initiated (sent) the Redirect (e.g., 3xx) / REFER. The default is -1 (i.e., not configured).

13. **SDP Insertion:**

    For certain mid-call media negotiations (such as interworking of Re-INVITEs and 18x responses with or without SDP), the E-SBC needs to insert an SDP offer or answer into requests/responses. For this insertion to function correctly, a valid Extension Coders Group ID needs to be configured for the relevant IP Profile. The extension assists the E-SBC in generating an SDP that optimizes the offer/answer process and reduces the chances for transcoding. (Transcoding is not supported in this Release version, since it requires DSP resources.)

3.2 Major 6.4 Release Features

This section describes the main features that were introduced in the initial release of 6.4.

3.2.1 SIP General Features

The device supports the following new SIP general features:

Note: The SIP general features are applicable to all the applications supported by the device (i.e., GW / IP2IP, SAS, and SBC).

1. **VoIP Configuration through the Command Line Interface (CLI):**

   This feature provides support for configuring the VoIP-related parameters through the CLI (including all the SIP parameters). Until now, only Data-Router configuration could be configured through CLI. The VoIP-related CLI commands are accessed through the command, **`configure voip`**. The current VoIP settings can be displayed using the CLI **`show`** commands.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

2. **SIP Message Manipulation using Wildcards to Remove Headers:**

   This feature provides support for using wildcards to remove headers when configuring SIP message manipulations in the existing Message Manipulations table. For example, to remove all SIP Via headers, you can use the asterisk (*) wildcard, for example, “header.Via*”.

   Applicable Products: This feature is applicable to all devices.

3. **Full SIP Manipulation on History-Info and Privacy Headers:**

   This feature provides support for configuring full manipulation (addition, modification, and removal) capabilities on the SIP History-Info and Privacy headers. This is configured in the existing Message Manipulations table.

   Applicable Products: This feature is applicable to all devices.

4. **SIP Message Manipulation Rules using Variables:**

   This feature provides enhanced SIP message manipulation by which information can be copied between messages. It does this by using variables in the existing Message Manipulations table. Information from one message is copied to a variable and then information from that variable is copied to any subsequent message. Examples of this feature are shown below:

   - Example 1:

     Storing a value in a call variable: Stores the subject URI parameter from the To header:

     ```
     MessageManipulations 0 = 0, Invite.Request, ,
     var.call.dst.1, 2, header.to.url.param.subject, 0;
     ```

     Using the stored value: Allocates a Subject header for the 200 OK response for the same call and assigns it the stored value:

     ```
     MessageManipulations 0 = 0, Invite.response.200, ,
     header.subject, 0, var.call.dst.1, 0;
     ```

- Example 2:

  Storing a value in a global variable: Stores the Priority header of the INVITE with ‘company’ in the host part of the From header:

  ```
  MessageManipulations 0 = 0, Invite.Request,
  header.from.url.host == ‘company’, var.global.1, 2,
  header.priority, 0;
  ```

  Using the stored value: Assigns the same priority as the INVITE request to SUBSCRIBE requests arriving with 'company' in the host part of the From header:

  ```
  MessageManipulations 0 = 0, Subscribe.request,
  header.from.url.host == ‘company’, header.priority, 0,
  var.global.1, 0;
  ```

Applicable Products: This feature is applicable to all devices.

5. **SIP Message Manipulation of Elements for Supported, Required and Unsupported Headers:**

   This feature provides support for modifying the following elements in SIP Supported, Required, and Unsupported headers using the existing Message Manipulations table:

- EarlyMedia,
- ReliableResponse
- Timer
- EarlySession
- Path
- Privacy
- Replaces
- History
- Unknown
- GRUU
- ResourcePriority
- TargetDialog
- SdpAnat

Examples of this feature are shown below:

- Adding the path capability to the Supported header of INVITE requests:

  ```
  MessageManipulations 0 = 0, Invite.Request, ,
  header.supported.capabilities.path, 2, ‘true’, 0;
  ```

- Adding a Subject header if the privacy capability appears in the Required header:

  ```
  MessageManipulations 0 = 0, Invite.Request,
  header.required.capabilities.privacy == 'true',
  header.subject, 2, ‘Privacy is a required capability’, 0;
  ```

Applicable Products: This feature is applicable to all devices.

6. SIP Message Manipulation Rules using Random Strings:

This feature provides support for adding randomly generated strings to header manipulations configured in the existing Message Manipulations table. The random string can be configured with up to 298 characters and include a range of, for example, from a to z or 1 to 10. This string is used in the table's 'Action Value' field.

The syntax of this option is shown below:

- rand.string.<number of characters in string>.<low value>.<maximum value>
- rand.number.<low number>.<high number>

The syntax variations can be written as follows:

- rand.string.5.a.z: generates a 5-character string using characters a through z
- rand.string.8.0.z: generates an 8-character string using characters and digits
- rand.number.5.32: generates an integer between 5 and 32

An example of such a manipulation rule is shown below.

```
MessageManipulations 4 = 1, Invite.Request, , Header.john, 0,
rand.string.56.A.Z, 0;
```

In this example, a header called "john" is added to all INVITE messages received by the device and a random string of 56 characters containing characters A through Z is added to the header.

Applicable Products: This feature is applicable to all devices.

7. SIP Message Manipulation Rules using Source or Destination IP Group:

This feature provides support for configuring SIP message manipulation rules using specific parameters from the source or destination IP Group to which the message belongs. The following IP Group parameters (defined in the IP Group table) can be used in the manipulation rule:

- 'Contact User': used as the Request-URI user part
- 'SIP Group Name': used as the Request-URI host part
- 'Type': used as the IP Group type (i.e., SERVER or USER)

These values can be used in the manipulation rule as follows:

- For matching rule conditions. For example, SIP messages belonging to an IP Group whose 'Contact User' field value is set to "username"
- For operation (actions). If the message matches the condition, then use an IP Group parameter value (listed above) in the outgoing Request-URI.

This feature is configured in the existing Message Manipulations table, using the new manipulation parameter, *param.ipg.<src|dst>.<user|host|type>*. To define a matching condition for indicating source or destination Request-URI (without using IP Group parameters), the manipulation parameter, *param.call.<src|dst>.<user|host>* can be used.

For example, the following manipulation rule uses the *param.ipg* syntax to check the source IP Group type. If it is a USER-type IP Group, then an XML message body is added in all REGISTER messages:

```
MessageManipulations 0 = 1, REGISTER.response,
"PARAM.IPG.src.TYPE=='user'", body.application/xml, 0,
'<?xml\\version="1.0"\\encoding="utf-
8"\\?>\\<LMIDocument\\version="1.0">\\<LocalModeStatus>\\<Loca
lModeActive>\\true\\</LocalModeActive>\\<LocalModeDisplay>\\"S
tandAloneModeActive"\\</LocalModeDisplay>\\</LocalModeStatus>\
\</LMIDocument>', 0;
```

Applicable Products: This feature is applicable to all devices.

8. **Voice Quality Reporting of TIA/TSB-116-A Ie and TCLw:**

This feature provides support for reporting the TIA/TSB-116-A Equipment Impairment factor (Ie) and Weighted Terminal Coupling Loss (TCLw) voice quality parameters. The reporting is done through RTCP-XR factors in SIP BYE messages, and 200 OK responses to BYE, using the existing proprietary SIP header, X-RTP-Stat (shown in the example below).

```
X-Audiocodes-RTP-Stat:
PS=1783,OS=285280,PR=1784,OR=285440,PL=0,JI=3,LA=0, IE=50,
TCLW=20
```

To support this feature, the following needs to be done:

- Enable RTCP XR using the existing parameter, *VQMonEnable*.
- Enable the proprietary SIP header, X-RTP-Stat using the existing parameter, *QoSStatistics*.
- RTCP XR Feature Key must be installed on the device.

Applicable Products: This feature is applicable to all devices.

9. **Quality of Experience Reporting to EMS Session Experience Manager:**

This feature provides support for reporting voice quality of experience to AudioCodes Session Experience Manager (SEM) plug-in for the EMS. This feature is configured using the following new parameters:

- *QOEServerIP* – defines the IP address of the SEM server
- *QOEPort* – defines the port of the SEM server
- *QOEInterfaceName* – defines the IP interface on which the SEM reports are sent
- *QOEConnectionMode* – defines the connection type (client or server)
- *QOEInformationLevel* – defines the level (i.e., amount of information) of information sent in the reports
- *QOEUseMosLQ* – defines the reported MOS type (listening or conversational)

To support this feature, the device must be installed with the relevant Software Upgrade Feature Key.

Applicable Products: Mediant 600, Mediant 800, Mediant 800 MSBG, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B, and Mediant 3000.

3.2.2 SIP Gateway / IP-to-IP Features

The device supports the following new features for the SIP Gateway / IP-to-IP application:

1. **Denial of Collect Calls:**

   This feature supports the ability to reject (disconnect) incoming Tel (FXO)-to-IP collect calls and to signal this denial to the PSTN. This capability is required, for example, in the Brazilian telecommunication system to deny collect calls.

   This feature can be enabled for all calls or per FXO port, using the new parameter, *EnableFXODoubleAnswer*. The sequence of signals that the device sends to the PSTN side is an off-hook, on-hook after one second, and then off-hook after two seconds (i.e., double-answer sequence). In addition to enabling this feature, the PSTN side must be configured to identify this double-answer signal and automatic dialing must not be configured for the FXO ports.

   Applicable Products: Mediant 600, Mediant 1000, Mediant 800 MSBG, and Mediant 1000 MSBG.

2. **Least Cost Routing per Call Destination:**

   This feature provides support for least cost routing (LCR) whereby the device selects the IP destination routing rule based on lowest call cost. The device sends the calculated cost of the call to a Syslog server (as Information messages).

   LCR is implemented by defining *Cost Groups* and assigning them to routing rules in the Outbound IP Routing table. When routing a call using the LCR feature, the device searches the routing table for matching routing rules, and then selects the one with the lowest call cost. If two routing rules have identical costs, then the route appearing higher up in the table (i.e., first-matched rule) is used. If a selected route is unavailable, the device uses the next least-cost routing rule. However, even if a matched routing rule is not assigned a Cost Group, the device can select it as the preferred route over other matched routing rules with Cost Groups, according to the settings of an LCR-related parameter, *LCRDefaultCost* (see below).

   The Cost Group defines a default call connection cost and charge per minute. However, the Cost Group can be assigned *time bands,* which define call connection costs and charges per minute based on specific days of the week and time intervals (for example, 0.17 units between Saturday and Sunday and between 18:00 and 6:00).

   In addition to time bands, the device calculates the cost of the call using a user-defined average call duration value: Call cost = call connection cost + (minute cost * average call duration). A basic example of four defined Cost Groups (without time bands) and their total cost if the average call duration is 10 minutes is shown below:

Cost Group	Connection Cost	Minute Cost	Cost for 1 Minute	Cost for 10 Minutes
A	1	6	7	61
B	0	10	10	100
C	0.3	8	8.3	80.3
D	6	1	7	**16**

   In the example above, if four matching routing rules are located in the routing table and each one is assigned a different Cost Group, then the rule assigned with Cost Group D (i.e., lowest call cost) is used. Note that for 1 minute, Cost Groups A and D are identical, but due to the average call duration, Cost Group D is cheaper.

   The LCR feature is configured using the following new parameters: *LCREnable*, *CostGroupTable, CostGroupTimebands*, *LCRDefaultCost*, and *LCRAvgCallLength*. To associate Cost Groups to routing rules, the new field, 'Cost Group' has been added to the Outbound IP Routing table.

   Applicable Products: This feature is applicable to all devices.

3. **SIP Message Manipulation for Gateway/IP-to-IP Application:**

   This feature provides support for SIP INVITE message manipulation for the Gateway / IP2IP applications. This is similar to the existing SIP message manipulation capabilities supported for the SBC application.

   The message manipulation rules are configured in the Message Manipulation table (*MessageManipulations*) and the logic for applying message manipulation rules (*Manipulation Set ID*) are as follows:

   - For manipulation on all inbound SIP INVITE messages, the Manipulation Set ID is selected (and enabled), using the new "global" parameter, *GWInboundManipulationSet*.
   - For manipulation on outbound SIP INVITE messages, the Manipulation Set ID is selected (and enabled) using the following logic:

     a. According to the settings of the Outbound Message Manipulation Set parameter of the destination IP Group. In other words, manipulation can be done per destination IP Group. If this parameter is not configured, see Step b below.

     b. According to the settings of the new "global" parameter, *GWOutboundManipulationSet*. If this parameter is also not configured, no manipulation is done.

     Note that for the IP-to-IP application, the outgoing message is re-created and consequently, SIP headers not relevant to the outgoing SIP session (e.g., Referred-By) are not included in the outgoing message. Therefore, if required, manipulations on such headers should be handled in inbound manipulation.

   Currently, this feature is configurable only through the *ini* file.

   Applicable Products: This feature is applicable to all devices.

4. **Routing and Manipulation Based on Suffix of Source / Destination Number:**

   This feature provides support for routing and manipulation according to the suffix of the source and/or destination number. This is in addition to the existing support for using prefix numbers. The suffix can be a specific number or a range of numbers. This capability is used in the call routing and manipulation tables. For example, a value entered as "[100-199](100,101,105)" depicts a number that starts (i.e., prefix) with a number from 100 through 199, and ends (i.e., suffix) with 100, 101, or 105.

   Applicable Products: This feature is applicable to all devices.

5. **SIP Calling Name Manipulations:**

   This feature provides support for manipulating the calling name (caller ID) for Tel-to-IP and IP-to-Tel calls. This can include modifying or removing the Calling Name.

   For example, assume that an incoming SIP INVITE message includes the following header:

   ```
   P-Asserted-Identity: "company:john" sip:6666@78.97.79.104
   ```

   Using the IP-to-Tel calling name manipulation, the text, "company" can be changed to "worker" in the outgoing INVITE, as shown below:

   ```
   P-Asserted-Identity: "worker:john" sip:996666@10.13.83.10
   ```

   This feature is configured using the following new tables:

   - Calling Name Manipulations IP2Tel (CallingNameMapIp2Tel *ini* file parameter)
   - Calling Name Manipulations Tel2IP (CallingNameMapTel2Ip *ini* file parameter)

   Applicable Products: This feature is applicable to all devices.

6. **Calling Number with "ext=<xxx>" Parameter in From or P-Asserted-ID Headers:**

   This feature provides support for handling calling numbers with the "ext=<xxx>" parameter in From or P-Asserted-ID headers in incoming INVITE messages.

   This feature adds the value of the "ext" parameter as a suffix to the calling number and the character "e" as a prefix to the calling number. For example, if the From header, "From: sip:622125519100;**ext=1010**@10.1.10.12" is received, the device changes the calling number to "e6221255191001010". Once this number is changed, it is possible to configure number manipulation rules to modify the calling number, for example, to leave only the four last digits.

   The feature is enabled using the existing parameter, *EnableMicrosoftExt*.

   Applicable Products: This feature is applicable to all devices.

7. **Obtaining Calling Number from P-Asserted-Identity Header:**

   This feature provides support for configuring from where the device obtains the calling (source) number in the incoming INVITE request. This can be obtained from one of the following headers:

   - First P-Asserted-Identity
   - Second P-Asserted-Identity (if exists)
   - From

   This feature is configured using the existing parameter, *SourceNumberPreference*. If not configured, the URI is taken from the first P-Asserted-Identity header.

   Applicable Products: This feature is applicable to all devices.

8. **Destination Number and Ascending Channel Select Mode:**

   This feature provides an additional method for allocating a channel of a Trunk Group to an incoming IP-to-Tel call. For this new method, the device selects the channel as follows:

   a. The device attempts to route the call to the channel that is associated with the destination (called) number. If located, the call is sent to that channel.

   b. If the number is not located or the channel is unavailable (e.g., busy), the device searches, in ascending order, the next available channel in the Trunk Group. If located, the call is sent to that channel.

   c. If the device reaches the highest channel in the Trunk Group and all the channels are unavailable, the call is released.

   This new feature is configured using the new channel select mode option, “Dest Number + Ascending” (11), for the following existing parameters:

   - *ChannelSelectMode* – “global” parameter for channel select method for all Trunk Groups
   - *TrunkGroupSettings* – channel select method per Trunk Group (in the Trunk Group Settings table)

   Applicable Products: This feature is applicable to all devices.

9. **B-Channel Number for Calling Party Number in Q.931 Setup:**

   This feature provides support for replacing the original source phone number with the B-channel number. This feature is applicable to CAS and ISDN protocols.

   The device handles this support as follows:

   - **For IP-to-Tel calls:** The B-channel's number (according to the Channel Select Mode in the 'Trunk Group' table) is sent as the calling party number to the Tel side (instead of the phone number received in the SIP INVITE’s From header). For example, if the incoming INVITE From header contains "12345" and the destined B-channel number is 17, then the outgoing calling party number in the Q.931 Setup message is set to "17" instead of "12345". Note that this feature is applied after routing and manipulation (before sending to the PSTN).
   - **For Tel-to-IP calls:** The B-channel's number is sent in the INVITE’s From header to the IP side (instead of the phone number received in the Q.931 Setup message). For example, if the incoming calling party number in the Q.931 Setup message is "12345" and the B-channel number is 17, then the outgoing INVITE From header is set to "17" instead of "12345". Note that this feature is applied before routing or manipulation on the source number.

   This feature can be enabled (in the Web, *ini* file, SNMP and EMS), using the following new parameters:

   - *UseEPNumAsCallingNumTel2IP*
   - *UseEPNumAsCallingNumIP2Tel*

   Applicable Products: This feature is applicable to all devices.

10. **QSIG Tunneling for All ISDN Variants:**

    This feature provides support for QSIG tunneling (according to ECMA-355) on all ISDN variants (in addition to the already supported QSIG protocol).

    Applicable Products: This feature is applicable to all devices.

11. **QSIG Tunneling-over-SIP per Call:**

    This feature provides support for QSIG tunneling-over-SIP per IP call. This feature is enabled using the new IP Profile table parameter, *EnableQSIGTunneling*. This IP Profile is then assigned to the relevant call routing rule. In the previous release, QSIG tunneling over SIP could be applied only for all calls (not per call), using the *EnableQSIGTunneling* "global" parameter.

    Applicable Products: This feature is applicable to all devices.

12. **Interworking QSIG Path Replacement for IP-to-ISDN Calls:**

    This feature provides support for handling consultation call transfer requests for ISDN (QSIG) to IP calls. When a request for a consultation call transfer is received by the device (from the PBX), the device sends a SIP REFER message with a Replaces header to the SIP UA to transfer it to another SIP UA. Once the two IP parties are successfully connected, the device requests the PBX to disconnect the ISDN call (thereby, freeing resources on the PBX).

    For example, assume legacy PBX user A has two established calls (connected through the device) – one with remote SIP user agent B and the other with SIP user agent C. In this scenario, user A initiates a consultation call transfer to connect B to C. The device receives the consultation call transfer request from the PBX and then connects B to C by sending a REFER message with a Replaces header (i.e., replace caller A with C) to B. Upon receipt of a SIP NOTIFY 200 message in response to the REFER, the device sends a Q.931 DISCONNECT messages to the PBX notifying the PBX that it can disconnect the ISDN calls (of user A).

    This feature is enabled by the new parameter, *ISDNTransferMode*.

    Applicable Products: This feature is applicable to all devices.

13. **AT&T Toll Free Out-Of-Band Blind Transfer for 4ESS Protocol:**

    This feature provides support for AT&T toll free out-of-band blind transfer for trunks configured with the 4ESS ISDN protocol. This trunk transfer method is done when a SIP REFER message is received. AT&T courtesy transfer is a supplementary service which enables a user (e.g., A) to transform an existing call between it and another user (e.g., B) into a new call between user B and a third user (e.g., C), whereby A does not have a call established with C prior to call transfer.

    The device handles this feature as follows:

    - **IP-to-Tel (user side):** When a SIP REFER message is received, the device initiates the call transfer by sending a Facility message to the PBX.
    - **Tel-to-IP (network side):** When a Facility message initiating an out-of-band blind transfer is received from the PBX, the device sends a SIP REFER message to the IP side if the *EnableNetworkISDNTransfer* parameter is set to 1.

    This feature is configured by setting the existing *TrunkTransferMode* parameter to the new option value, 6.

    Applicable Products: Mediant 600, Mediant 800 MSBG, Mediant 1000, Mediant 1000 MSBG, Mediant 2000, and Mediant 3000.

14. **Three-Way Conferencing for BRI Interfaces:**

    This feature provides support for three-way conferencing on the ISDN Basic Rate Interface (BRI) phones that are connected to the device. This feature complies with ETS 300 185.

    Three-way conferencing is enabled using the existing parameters *Enable3WayConference* (set to 1) and *3WayConferenceMode* (set to 2). Establishing a three-way conference is done by pressing the relevant conference button on the BRI phone.

    For Mediant 1000, the MPM module is required for three-way conferencing.

    Applicable Products: Mediant 1000, Mediant 800 MSBG, and Mediant 1000 MSBG.

15. **BRI Supplementary Services for ETSI Variant using a Single BRI B-Channel:**

    This feature provides support for BRI supplementary services of the ETSI variant, using only a single BRI B-channel. In the previous release, a second B-channel was required.

    This feature supports the following supplementary services:

    - Call waiting (ETS 300 058-1 and Q.953)
    - Call hold / retrieve (ETS 300 141)
    - Call transfer

    The BRI supplementary services are initiated by the BRI phones connected to the device.

    Applicable Products: Mediant 600, Mediant 1000, Mediant 800 MSBG, and Mediant 1000 MSBG.

16. **V.150.1 Modem-Relay Handling:**

    This feature provides support for V.150.1 modem relay coder negotiation in initial INVITE and 200 OK, using the SDP body. This eliminates the need for sending a re-INVITE (as was done in the previous release) to negotiate V.150.1. This is according to the UCR-2008, Change 2 specification.

    Applicable Products: Mediant 800 MSBG and Mediant 3000.

17. **Negotiating T.38 Version in Re-INVITE for V.34 Fax Relay:**

    This feature provides support for negotiating T.38 Version 3 capability using SIP re-INVITE. The device negotiates T.38 Version 3 as follows:

    a. The device receives an INVITE from a remote party with an audio coder in the SDP and responds with a 200 OK from the termination fax answer.

b. Upon fax answer tone detection, the device sends a re-INVITE to the remote party, negotiating the use of T.38 Version 3.

c. If the remote party supports only T.38 Version 0, the device “downgrades” the T.38 Version 3, to T.38 Version 0.

To enable this feature, the existing parameter, *IsFaxUsed* is used (set to 1 or 3). In addition, the T.38 coder must not be defined (in the Coder table).

Applicable Products: Mediant 800 MSBG and Mediant 3000.

18. **Using Destination IP Group for MWI SIP SUBSCRIBE Messages:**

This feature provides support for using settings of a specific IP Group (and associated Proxy Set) when sending a SIP SUBSCRIBE message to an MWI server. This is done as follows:

- The IP Group table parameter, 'SIP Group Name' is used for the host name in the Request-URI of the SUBSCRIBE message.
- Sends the SUBSCRIBE to the address defined for the Proxy Set associated with the IP Group, and uses the Proxy Set's capabilities such as proxy redundancy and load balancing.

For example, if the 'SIP Group Name' field of the IP Group is set to "company.com", the device sends the following SUBSCRIBE message:

```
SUBSCRIBE sip:company.com...
```

Instead of:

```
SUBSCRIBE sip:10.33.10.10...
```

This feature is configured using the new parameter, *MWISubscribeIPGroupID*. This parameter defines the IP Group ID used for this feature. If this feature is not configured, the MWI SUBSCRIBE message is sent to the MWI server as defined by the existing parameter, *MWIServerIP*.

Applicable Products: This feature is applicable to all devices.

19. **Registration per Entity:**

This new feature provides support for initiating registration per the following entities through the Web interface:

- FXS / FXO endpoints - using the **Register** button in the Endpoint Phone Number table
- Trunk Groups - using the **Register** button in the Trunk Group table
- BRI endpoints - using the **Register** button in the ISDN Supp Services table
- Accounts - using the **Register** button in the 'Account Table' page

The registration method for each endpoint in the above pages is determined according to the existing parameter, 'Registration Mode' (Per Gateway, Per Endpoint, Per Account, No register) in the 'Trunk Group Settings' page.

In the previous release, only registration per device was supported (by clicking the **Register** button in the Proxy & Registration page).

Applicable Products: This feature is applicable to all devices.

20. **Excluding SIP "resource-priority" Tag from Required Header:**

This feature provides support for configuring the device to exclude the "resource-priority” tag from the SIP Require header in the INVITE, for Tel-to-IP calls. This feature is used for MLPP priority call handling (when the *CallPriorityMode* parameter is set to 1). This feature is configured using the new parameter, *RPRequired*.

Applicable Products: This feature is applicable to all devices.

21. **RTCP XR Voice Quality Monitoring:**

This feature provides support for publishing RTCP XR information according to RFC 6035. 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.

The device can send RTCP XR reports to an external server, using SIP PUBLISH messages.

To support this feature, RTCP XR must be enabled (using the existing, *VQMonEnable* parameter) and the RTCP XR feature key must be installed on the device.

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

Applicable Products: Mediant 800 and Mediant 800 MSBG (existing support on Mediant 600, Mediant 1000, Mediant 1000 MSBG, Mediant 2000, and Mediant 3000).

22. **Additional CDR Fields for Gateway Application:**

This feature provides additional call detail record (CDR) fields for the Gateway application:

Field	Description
SrcHost	Source host name
SrcHostBeforeMap	Source host name before manipulation
DstHost	Destination host name
DstHostBeforeMap	Destination host name before manipulation
IPG	IP Group description
LocalRtpIp	Remote RTP IP address
LocalRtpPort	Local RTP port
TrmReasonCategory	Termination reason category
RedirectNumBeforeMap	Redirect number before manipulation
SrdId	SRD ID
SIPInterfaceId	SIP interface ID
TransportType	SIP transport type (UDP, TCP, TLS)
TxRTPIPDiffServ	Media IP DiffServ
TxSigIPDiffServ	Signaling IP DiffServ
LocalRFactor	Local R-factor
RemoteRFactor	Remote R-factor
LocalMosCQ	Local MOS for conversation quality
RemoteMosCQ	Remote MOS for conversation quality
SourcePort	Source RTP port
DestPort	Destination RTP port

Applicable Products: This feature is applicable to all devices.

23. **Trunk Group Settings and Inbound IP Routing Web Tables Increased to 120:**

This feature provides support for increased table row size for the Trunk Group Settings table and the Inbound IP Routing table in the Web interface. This has been increased to 120 entries (compared to 24 entries in the previous release).

Applicable Products: Mediant 1000, Mediant 1000 MSBG, Mediant 2000, and Mediant 3000.

24. **E&M Line Signaling Interfaces:**

This feature provides support for up to six E&M (earth & magneto, or ear & mouth) signaling interfaces (offered in groups of two E&M interfaces). E&M is a type of supervisory line signaling that uses DC signals on separate leads, called the "E" lead and "M" lead, traditionally used in the telecommunications industry between telephone switches.

This support allows the device to be integrated into various applications requiring E&M signaling interfaces. For example, the device can operate in a radio-over-IP (RoIP) gateway solution for two-way radio systems. In such a solution, the device interfaces between the analog radio station (servicing the land mobile radios) and the IP-based push-to-talk (PTT) server.

The device's E&M interfaces support the following:

- Dial Type: DTMF touch-tone dialer; pulse dialer
- Impedance: 600R and TBR21
- Operation: two- or four-wire. 4-wire E&M uses a 4-wire (2-pair) transmission path for the voice signal. 2-wire E&M uses a single pair for both transmit and receive voice signal. This is configured using the new parameter, *enmVoiceType*.
- Hook Signaling: LMR immediate (without DTMF / MF dialing).
- Interface Type V (selectable by the new parameter, *enmSignalingType*): Type V is the most common variant in use outside United States. Both ends of the connection indicate a call by grounding the relevant lead. This means that it is easy to interconnect two PABXs "back-to-back" by crossing over the E&M leads and transmit and receive pairs.

Additional E&M parameters are listed below:

- *EnmSystemType* – sets E&M interfaces to signaling or trunking unit.
- *EnmHookDebounceTiming* – E&M standard requires hook detection after 70 milliseconds of hook status change. This parameter modifies the hook detection time for integrating E&M into other systems.
- *EnmOffHookGlareEnable* – E&M interface can detect hook events from the PSTN side and generate hook signals toward the PSTN side. Situations were generation of hook command toward the PSTN side and detection of hook events from the PSTN side is unavoidable. Since the device supports only the LMR hook type, there is no way to signal the PSTN side for busy status. When both event and command collide and this parameter is ON (1), the hook command is rejected and returns the hook command request for busy signal.
- *EnmCountryCoefficients* – sets the E&M internal filters and line impedance to USA 600 Ohm or Europe TBR21.

The following call flow example describes how E&M signaling is implemented:

d. On power up, the device registers its E&M endpoints by sending SIP REGISTER messages to the PTT server.

e. The PTT server sends INVITE messages to the device's E&M endpoints with 'a=inactive' in the SDP.

f. The device responds immediately with a 200 OK to the PTT server.

g. Once the call is established, re-INVITEs can be sent by the device or PTT server, as described below:

- ♦ PTT server can send re-INVITE messages to the device to control the radio transmission:
  - ✓ SDP with 'a=sendonly' activates the E-lead (starts radio transmission)
  - ✓ SDP with 'a=inactive' idles the E-lead (stops radio transmission)
- ♦ Change in M-lead triggers the device to send re-INVITE messages to the PTT server:
  - ✓ When M-lead goes active, the device sends re-INVITE with 'a=sendonly' in SDP (radio is in receiving mode)
  - ✓ When M-lead goes idle, the device sends re-INVITE with 'a=inactive' in SDP (radio is in idle mode)

Applicable Products: Mediant 800.

3.2.3 SIP Stand-Alone Survivability (SAS) Features

The device supports the following new SIP Stand-Alone Survivability (SAS) application feature:

1. **Destination Number Manipulation in Incoming INVITE in SAS Emergency State:**

   This feature provides support for manipulating the destination number in the Request-URI of incoming INVITE messages when SAS is in emergency state. This is required, for example, if the call is destined to a registered user, but the destination number in the received INVITE is not the number assigned to the registered user in the SAS registration database. To overcome this and successfully route the call, this feature allows you to define manipulation rules to change the INVITE's destination number so that it matches that of the registered user in the database.

   For example, in SAS emergency state, assume an incoming INVITE has a destination number "7001234" which is destined to a user registered in the SAS database as "552155551234". In this scenario, the received destination number therefore, needs to be manipulated to the number "552155551234". Once manipulated, the outgoing INVITE sent by the device also contains this number in the Request-URI user part.

   This feature is enabled using the new parameter, *SASInboundManipulationMode*. The manipulation rule is defined in the existing IP to IP Inbound Manipulation table (under the **SBC** menu).

   Applicable Products: This feature is applicable to all devices.

3.2.4 Session Border Controller Features

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

1. **Increase in SBC Sessions to 50 for Mediant 800 and Mediant 800 MSBG:**

   This feature provides support for up to 50 concurrent SBC sessions (as opposed to 25 in the previous release).

   Applicable Products: Mediant 800 and Mediant 800 MSBG.

2. **SIP BYE Response Authentication:**

   This feature provides support for authenticating a SIP BYE request prior to the disconnection of a call. This feature prevents, for example, a scenario in which the SBC SIP client receives a BYE request from a third-party imposer assuming the identity of a participant in the call and as a consequence, the call between the first and second parties is inappropriately disconnected.

   When this feature is enabled, the device forwards the SIP authentication response (for the BYE request) to the request sender and waits for the user to authenticate it. The call is disconnected only if the authenticating server responds with a 200 OK.

   This feature is enabled (disabled by default) using the new parameter, *SBCEnableByeAuthentication*.

   Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

3. **User Information File for SBC Users:**

   This feature provides support for creating an SBC users database from a loaded User Information file. The same text-based User Information file for the GW / IP2IP application is used for this feature, enabled by the existing parameter, *EnableUserInfoUsage*.

   The User Information file lists the SBC users under the "[SBC]" section and the Gateway PBX users under the "[GW]" section, as shown below:

   ```
   [ GW ]
   FORMAT
   PBXExtensionNum,GlobalPhoneNum,DisplayName,UserName,Password
   4000,039764000,lee,lee_user,lee_pass
   4001,0547771234,mike,mike_user,mike_pass
   [ SBC ]
   FORMAT LocalUser,UserName,Password,IPGroupID
   john,john_user,john_pass,2
   sue,sue_user,sue_pass,1
   ```

   where:

   - *LocalUser* - identifies the user and is used as the URI user part for the AOR in the database
   - *UserName* -user's authentication username
   - *Password* - user's authentication password
   - *IPGroupID* - IP Group to which the user belongs and is used as the URI source host part for the AOR in the database

   The user database can later be used for the following functionalities:

   - Register to an external registrar server on behalf of a specific user.
   - Authenticate (for any SIP request and as a client) on behalf of a specific user if challenged by an external server
   - Authenticate (as a server) incoming user requests (used for SBC security)

   Two new IP Group table parameters have been added to configure the handling of user registration and authentication - Registration Mode and Authentication Mode.

If the SBC registers on behalf of users and the users don't perform registration at all, any SIP request destined to the user is routed to the Proxy Set associated with the user's IP Group (associating a Proxy Set was not supported in the previous release).

The maximum number of users that can be defined in the User Information file is:

- Mediant 800 – 200 users
- Mediant 1000 MSBG – 600 users
- Mediant 3000 – 3,000 users

Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

4. **SIP Server Authentication:**

This feature provides support for the device to function as an authentication server for SIP SBC message requests. Until now, such requests were authenticated by an external, third-party server. The SIP authentication method is based on HTTP authentication DIGEST with MD5.

When functioning as an authentication server (set by the new IP Group table parameter, *AuthenticationMode*), the device authenticates only users that belong to a USER-type IP Group. When the client (e.g., SIP phone) sends an INVITE or REGISTER to the device for SIP message authorization, the device (as a server) processes the authorization as follows:

a. The device verifies the type of incoming SIP method (e.g., INVITE) that must be challenged for authorization. This is configured using the new IP Group table parameter, *MethodList*.

b. If the message is received without an Authorization header, the device "challenges" the client by sending a 401 or 407 SIP response. The client then resends the request with an Authorization header (containing user name and password).

c. The device validates the SIP message according to the settings of the new parameters, *AuthNonceDuration*, *AuthChallengeMethod* and *AuthQOP*. If validation fails, the message is rejected and the device sends a 403 "Forbidden" response.

d. If the SIP message is validated, the device verifies identification of the SBC user by checking whether the user name and password received from the user is correct. The user name and password in the database is obtained from the User Information file. If after three attempts the SIP SBC user is not successfully authenticated, the device sends a 403 "Forbidden" response.

e. If the user is successfully identified, the SIP message request is processed.

Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000 TP-6310 (Simplex).

5. **SIP Message Security Rules:**

This feature provides support for defining SIP message policies for blocking (blacklist) unwanted incoming SIP messages and allowing (whitelist) receipt of desired messages. This feature allows you to define legal and illegal characteristics of a SIP message. The message policy can apply globally (default) or per signaling domain (i.e., assigned to a SIP interface in the SIP Interface table).

This feature is helpful against VoIP fuzzing (also known as robustness testing), which sends different types of packets to its "victims" for finding bugs and vulnerabilities. For example, the attacker might try sending a SIP message containing either an oversized parameter or too many occurrences of a parameter.

SIP message security rules are configured in the new Message Policy table (MessagePolicy). Each policy can be defined with the following:

- Maximum message length
- Maximum SIP header length
- Maximum message body length

- Maximum number of headers
- Maximum number of bodies
- Option to send 400 "Bad Request" response if message request is rejected
- Blacklist and whitelist for defined SIP methods (e.g., INVITE)
- Blacklist and whitelist for defined SIP bodies

Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

6. **Enhanced Classification Process using Condition Rules:**

   This feature provides support for enhancing the process of classifying an incoming SIP dialog to an IP Group, based on SIP message conditions. The condition rule is defined in the new Condition table. This table allows you to define SIP message conditions using the same syntax (match-condition) as in the Message Manipulations table (for example, `header.to.host contains “company”`). If a classification rule in the Classification table (using a new field, MessageCondition) is associated with a condition rule, the classification is used only if the classification rule and its associated condition rule are matched. You can also define a more complex rule using the "AND" or "OR" Boolean operands

   Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

7. **Enhanced Classification Process using Source Port and Transport Type:**

   This feature provides support for enhancing the process of classifying an incoming SIP dialog to an IP Group, by using source port number and SIP transport type. This feature is accommodated by two new fields in the Classification table (SrcPort and SrcTransportType).

   Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

8. **SIP Access List using Classification Rules:**

   This feature provides support for configuring SIP application-layer access lists. This includes blocking unwanted SIP dialogs by using classification rules. The Classification table (existing support) provides a new field that when set to "Deny", incoming SIP dialogs matching the specific classification rule are rejected.

   This feature offers greater flexibility in the security mechanism of the SBC by allowing the user to configure whitelists (allowed messages) and blacklists (deny messages) based on classification rules. If the incoming SIP dialog cannot be classified according to the Classification table, the call is accepted or rejected based on the settings of the existing parameter. *AllowUnclassifiedCalls*.

   Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

9. **Maximum SBC Call Duration:**

   This feature provides support for defining the maximum allowed duration (in minutes) of an SBC call. If an established call reaches this user-defined limit, the device terminates the call. This feature is configured using the parameter, *MaxCallDuration* (used in the previous release for the Gateway application). This feature is useful for ensuring available resources for new calls, by ensuring calls are properly terminated.

   Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

10. **Alternative Routing upon Reaching Call Admission Control Limit:**

    This feature provides support for alternative routing when the initial route of an SRD or IP Group has reached its call admission control limit (i.e., maximum concurrent calls and / or call rate) as set in the Admission Control table.

    Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

11. **Preference Order of Extension Coders in SDP:**

    This feature provides support for configuring the order of preference of the Extension coders in the SDP of the outgoing SIP message. This new feature arranges the Extension coders and Allowed coders (according to the Allowed Coders Group). This is enabled using the new parameter, *SBCPreferencesMode.* If this feature is disabled (default), the Extension coders are added at the end of the list in the SDP.

    A review of the existing Allowed Coders and Extension Coders feature:

    - The device restricts coders by allowing only the use of coders defined in the Allowed Coders Group table (i.e., only coders common between the SDP offered coders and Allowed Coders are used).
    - The device can add coders (i.e., Extension coders) to the SDP, which can result in transcoding.

    In the previous release, the device arranged only the Allowed coders in the SDP. This was based on the settings of the 'Allowed Coders Mode' parameter in the IP Profile table. When set to 'Preference', the order of the coders was arranged according to their order of appearance in the Allowed Coders Group table; the Extension coders were added at the end.

    Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

12. **Fax Negotiation and Transcoding:**

    This feature provides support for handling fax transmissions. This feature allows fax transmissions to traverse the device transparently (i.e., without transcoding) or handles the fax as follows:

    - Allows interoperability between different fax devices, supporting fax transcoding if required.
    - Restricts usage of specific fax coders to save bandwidth, enhance performance, or comply with supported coders: G.711 (A-Law or Mu-Law), VBD (G.711 A-Law or G.711 Mu-Law), and T38.

    Fax configuration is done in the IP Profile and Coder Group Settings tables. The IP Profile table now includes a list of supported fax coders and defines how the device handles the negotiation between the incoming and outgoing fax legs, using the following new fax-related parameters:

    - *SBCFaxBehavior:* defines the offer negotiation method - pass fax transparently, negotiate fax according to fax settings in IP Profile, or enforce remote UA to first establish a voice channel before fax negotiation.
    - *SBCFaxCodersGroupID:* selects supported fax coders (from the Coders Group Settings table).
    - *SBCFaxOfferMode:* determines the fax coders sent in the outgoing SDP offer.
    - *SBCFaxAnswerMode:* determines the fax coders sent in the outgoing SDP answer.

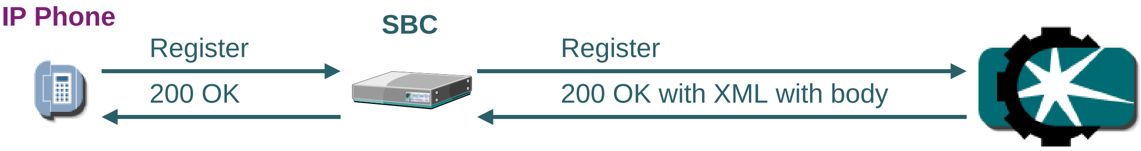
    Note that the voice-related coder configuration (Allowed and Extended coders) is independent of the fax-related coder configuration, with the exception of the G.711 coder. If the G.711 coder is restricted by the Allowed Coders Group table, it is not used for fax processing even if it is listed in the Coders Group Settings table for faxes. However, support for G.711 coders for voice is not dependent upon which fax coders are listed in the Coders Group Settings table.

    Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

13. **BroadSoft support for Auto-Provisioning of Subscriber-Specific Information:**

    This feature enhances the support for call survivability when connectivity with BroadSoft's BroadWorks server is lost (due to, for example, WAN failure). This feature enables local users to dial a local extension of (or any other configured alias) that identifies another local user in survivability mode. This feature is enabled using the new parameter, *SBCExtensionsProvisioningMode*.

    In normal operation, when subscribers (e.g., IP phones) register to the BroadWorks server through the SBC, the SBC includes the Allow-Events header in the sent REGISTER message. In response, the BroadWorks server sends the SBC a SIP 200 OK containing an XML body with subscriber information such as extension number, phone number, and URIs (aliases). The SBC forwards the 200 OK to the subscriber (without the XML body).



    The SBC saves these users with their phone numbers and extensions in its registration database, thus enabling routing to these destinations during survivability mode. When in survivability mode, the device routes the call to the Contact associated with the dialed phone number or extension number in the registration database.

    Below is an example of an XML body received from the BroadWorks server:

```
<?xml version="1.0" encoding="utf-8"?>
  <BroadsoftDocument version="1.0" content="subscriberData">
    <phoneNumbers>
      <phoneNumber>2403645317</phoneNumber>
      <phoneNumber>4482541321</phoneNumber>
    </phoneNumbers>
    <aliases>
      <alias>sip:bob@broadsoft.com</alias>
      <alias>sip:rhughes@broadsoft.com</alias>
    </aliases>
    <extensions>
      <extension>5317</extension>
      <extension>1321</extension>
    </extensions>
  </BroadSoftDocument>
```

    Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

14. **Enhanced Detection of SIP Connectivity Failure:**

    This feature provides support for detecting a failure in receiving SIP responses (e.g., TCP timeout, and UDP ICMP) and consequently, re-sending the responses to an alternative destination. (In the previous release, only detection of failed SIP requests was supported.)

    For example, assume the device sends a SIP 200 OK in response to a received INVITE request. If the device does not receive an ACK in response to this, it sends a new 200 OK to the next optional destination (e.g., to the next given IP address resolved from a DNS from the Contact or Record-Route header in the request related to the response).

    Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

15. **Call Forking:**

    This feature provides support for call forking. This enables an incoming call to be forked to multiple SBC user destinations. In such a scenario, all the extensions of a user ring simultaneously. The first extension to pick up the call receives the call and all other extensions stop ringing.

    To support this feature, the device's database can now register multiple SIP client user phone contacts (mobile and fixed-line extensions) to the same Address of Record (AOR). This enhancement allows an incoming call to ring simultaneously at multiple phone contacts. This saves significant time on the line for the caller compared to a serial calling configuration, where an incoming call is forwarded from extension to extension until the call is answered. This feature can be implemented in the following example scenarios:

    - An enterprise Help Desk, where an incoming customer call is simultaneously sent to multiple customer service agent extensions.
    - An employee's phone devices, where the incoming call is simultaneously sent to multiple devices (e.g., to the employee's office phone and mobile SIP phone).
    - An enterprise reception desk, where an incoming call is simultaneously sent to multiple receptionists.

    The Call Forking feature is configured by creating a USER-type IP Group with Call Forking enabled, using the new parameter, *EnableSBCClientForking*.

    Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

16. **Handling SIP Forking Initiated by SIP / Proxy Server:**

    This feature supports the handling of SIP forking responses received from a proxy server in response to an INVITE sent by the device from a UA (i.e., responses with a different SIP To header 'tag' parameter for the request forwarded by the device). This occurs in scenarios where, for example, a proxy server forks the INVITE request to several UAs, and hence, the SBC may receive several replies for a single request.

    Forked SIP responses may result in a single SDP offer with two or more SDP answers during call setup. The SBC handles this scenario by "hiding" the forked responses from the INVITE-initiating UA. This is achieved by marking the UA that responded first to the INVITE as the active UA, and only requests/responses from that UA are subsequently forwarded. All other requests/responses from other UAs are handled by the SBC (SDP offers from these users are answered with an 'inactive' media).

    If the active UA is the first one to send the final response (e.g., 200 OK), the call is established and all other final responses are acknowledged and a BYE is sent if needed. If another UA sends the first final response, then it is possible that the SDP answer that was forwarded to the INVITE initiating UA is not relevant, and media synchronization is needed between the two UAs. Media synchronization is done by sending a re-INVITE request immediately after the call is established. The re-INVITE is sent without an offer to the INVITE initiating UA. This causes the UA to send an offer which is forwarded to the UA that confirmed the call. The media synchronization process is enabled by the new parameter, *EnableSBCMediaSync*.

    Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

17. **Shared Phone Line Call Appearance for SBC Survivability:**

This feature provides support for redundancy of the BroadSoft Shared Call Appearance feature. When the BroadSoft application server (AS) switch fails or does not respond, or when the network connection between the device and the BroadSoft AS is down, the device manages the Shared Call Appearance feature for the SIP clients.

This feature is supported by configuring a primary extension and associating it with secondary extensions. For example, assume primary extension 600 is shared with secondary extensions 601 and 602. In the case of an incoming call to 600, all three phones ring simultaneously (using the above mentioned forking feature). Note that incoming calls specific to 601 or 602 ring only at these specific extensions respectively.

This feature is configured in the existing SBC Inbound Manipulation table, using the new ‘Manipulation Purpose’ option, 'Shared Line'. An inbound manipulation call rule (for registration requests) must be defined to change the destination number of the secondary extensions (e.g. 601 and 602) to the primary extension (e.g., 600). In addition, the Call Forking feature must also be enabled, by defining a USER-type IP Group with call forking enabled, using the new parameter, *EnableSBCClientForking*.

The following limitations currently exist:

- The SBC enables outgoing calls from all equipment that share the same line simultaneously (usually only one simultaneous call is allowed per a specific shared line).
- A shared line LED indicator may display the wrong current state.

Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

18. **Enhanced SBC CDRs:**

This feature provides enhanced call detail record (CDR) fields for the SBC application. This feature provides CDR fields for signaling and media. The signaling CDRs are published for each SBC leg. The media CDRs are published for each active media stream, thereby allowing multiple media CDRs where each media CDR has a unique call ID corresponding to the signaling CDR.

Signaling CDR		Media CDR	
Field	**Description**	**Field**	**Description**
SBCReportType	Report Type (call start, connect, end)	**MediaReportType**	Report type (media start, update, end)
EPTyp	Endpoint type	**SIPCallId**	Unique call ID
SIPCallId	Unique ID of call	**Cid**	Channel CID
SessionId	Unique Session ID	**MediaType**	Media type - audio/video/text
Orig	Call originator (local/remote)	**Coder**	Coder name
SourceIp	Source IP address	**PacketInterval**	Coder packet interval
SourcePort	Source UDP port	**LocalRtpIp**	Local RTP IP address
DestIp	Destination IP address	**LocalRtpPort**	Local RTP port
DestPort	Destination UDP port	**RemoteRtpIp**	Remote RTP IP address
TransportType	Transport type (UDP, TCP, TLS)	**RemoteRtpPort**	Remote RTP port

Signaling CDR		Media CDR	
Field	**Description**	**Field**	**Description**
SrcURI	Source URI	**InPackets**	Number of received packets
SrcURIBeforeMap	Source URI before manipulation	**OutPackets**	Number of sent packets
DstURI	Destination URI	**LocalPackLoss**	Local packet loss
DstURIBeforeMap	Destination URI before manipulation	**RemotePackLoss**	Remote packet loss
Durat	Call duration	**RTPdelay**	RTP delay
TrmSd	Termination side (local / remote)	**RTPjitter**	RTP jitter
TrmReason	Termination reason	**TxRTPssrc**	Tx RTP SSRC
TrmReasonCategory	Termination reason category	**RxRTPssrc**	Local RTP SSRC
SetupTime	Call setup time	**LocalRFactor**	Conversation quality
ConnectTime	Call connect time	**RemoteRFactor**	Conversation quality
ReleaseTime	Call release time	**LocalMosCQ**	Local MOS for conversation
RedirectReason	Redirect reason	**RemoteMosCQ**	Remote MOS for conversation
RedirectURINum	Redirection URI	**TxRTPIPDiffServ**	Media IP DiffServ
RedirectURINumBeforeMap	Redirect URI number before manipulation	-	-
TxSigIPDiffServ	Signaling IP DiffServ	-	-
IPGroup	IP Group description	-	-
SrdId	SRD name	-	-
SIPInterfaceId	SIP Interface ID	-	-
ProxySetId	Proxy Set ID	-	-
IpProfileId	IP Profile ID	-	-
MediaRealm	Media Realm name	-	-
DirectMedia	Direct media or traversing SBC (yes / no)	-	-

Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

3.2.5 Media Features

The device supports the following new media features:

1. **Acoustic Echo Cancellation:**

   This feature provides support for acoustic echo cancellation (ACE) on SBC calls. These echoes are composed of undesirable acoustical reflections (non-linear) of the received signal (i.e., speaker) which find their way from multiple reflections such as walls and windows into the transmitted signal (i.e., microphone). Therefore, the party at the far end hears his / her echo. The device's ACE removes these echoes and sends only the near-end's desired speech signal to the network (i.e., to the far-end party).

   This feature is enabled by setting the existing IP Profile table parameter, *EnableEchoCanceller* to the new option, "Acoustic". Note that the option, "Line" is for linear echo (handled by the device's Line Echo Canceller). The ACE configuration is also done using the following new parameters: Network Echo Suppressor Enable, Echo Canceller Type, Attenuation Intensity, Max ERL Threshold – DB, Min Reference Delay x10 msec, Max Reference Delay x10 msec.

   To support this feature, the Forced Transcoding feature must be enabled so that the device uses DSPs.

   Applicable Products: Mediant 3000.

2. **Skype SILK Audio Codec:**

   This feature provides support for SILK, Skype's default audio codec used for Skype-to-Skype calls. The following SILK codec specifications are supported:

   - Sampling frequencies: 8 kHz (narrowband) and 16 kHz (wideband)
   - Bit rates: 6-20 Kbps (default 20,000) for 8 KHz and 8-30 Kbps (default 30,000) for 16 KHz
   - Basic frame size: 20 ms
   - Packetization time intervals (ptime): 20 (default), 40, 60, 80, and 100 ms
   - Payload type: dynamic
   - Forward error correction

   The SILK codec is configured using the existing *CodersGroup* parameter and the following new parameters:

   - *SilkTxInbandFEC* – enables forward error correction
   - *SilkMaxAverageBitRate* - defines the maximum average bit rate

   Applicable Products: Mediant 800 and Mediant 800 MSBG.

3. **Disabling RTCP when RTP is Inactive:**

   This feature provides support for disabling Real-Time Transport Control Protocol (RTCP) traffic when there is no RTP traffic. In the previous release, RTCP was active even during inactive RTP periods (i.e., when the media is in 'recvonly' or 'inactive' mode). For example, this scenario can occur if the call is put on hold by an INVITE with 'a=inactive' in the SDP.

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

   Applicable Products: This feature is applicable to all devices.

4. **RTCP XR for SBC Calls:**

   This feature provides support for calculating RTCP XR voice quality metrics on SBC calls and distributing these metrics to the OAM&P layer. To support this feature, RTCP XR must be enabled (using the existing parameter, *VQMonEnable*) and the RTCP XR feature key must be installed on the device.

   Applicable Products: Mediant 1000 MSBG, Mediant 1000B, and Mediant 3000.

5. **Five-Level RTP Redundancy:**

   This feature provides support for five levels of RTP redundancy (according to RFC 2198). This is required for wireless networks such as Wi-Fi where a high percentage (up to 50%) of packet loss can be observed.

   This feature is configured by setting the existing parameter, *RTPRedundancyDepth* to the new option, 5. To use RTP redundancy level 5, you need to set the DSPVersionTemplateNumber parameter to 4 or 7. The coders that support 5-level RTP redundancy include:

   - DSPVersionTemplateNumber = 4 (all coders)
   - DSPVersionTemplateNumber = 7 (only G.729 and iLBC coders)

   Applicable Products: Mediant 3000.

6. **Automatic Gain Control:**

   This feature provides support for Automatic Gain Control (AGC). The AGC feature can be used to maintain stable voice energy levels on any call and during the call, by automatically converging to pre-defined energy levels.

   The AGC requires the installation of the IP Media Detectors feature key. In addition, the following existing parameters are used to enable the feature: *EnableDspIPMDetectors*, *EnableAGC*, and *AGCTargetEnergy*.

   Applicable Products: Mediant 800 MSBG and Mediant 800.

3.2.6 PSTN Features

The device supports the following new PSTN feature:

1. **New Behavior Bit for ISDNIBehavior:**

   This feature provides support for an additional behavior bit for the ISDNIBehavior parameter. The ISDN Q931 Layer Response Behavior field determines several behavior options which influence how the Q.931 protocol behaves. A new behavior bit has been added: NS_ACCEPT_ANY_CAUSE (67108864). The default value is 0. When this bit is set, the device accepts any Cause information element (IE) value.

   This behavior bit is applicable only to the ETSI protocol.

   Applicable Products: This feature is applicable to all devices.

3.2.7 Networking Features

The device supports the following new networking features:

1. **Physical Port Separation:**

   This feature provides support for selecting the Ethernet physical port group that the device must use. This is done in the existing Multiple Interface table using the new field, ‘Underlying Interface’. For each Ethernet port, the port speed and native VLAN (PVID) can be configured. This feature can also be used to set trusted and un-trusted networks on different physical ports.

   This feature also provides support for LAN port redundancy (protection). The device’s LAN ports operate in pairs, where one port is active and the other is redundant (standby). This is configured in the new Web page table, ‘Physical Ports Settings’.

   - For Mediant 800, up to 6 port-pair redundancy groups are supported
   - For Mediant 1000B, up to 3 port-pair redundancy groups is supported (2 ports on the CRMX module and 4 GB ports on the new LAN Expansion module)

   Applicable Products: Mediant 800 and Mediant 1000B.

2. **Virtual Routing and Forwarding for OAMP Interface:**

   This feature provides support for configuring OAMP Virtual Routing and Forwarding (VRF). This is done by binding OAMP applications to a specific interface which can then be associated with a VRF.

   This feature can be configured using the new parameter, *OAMPWanInterfaceName*. This feature can be configured in the Web interface and the CLI.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

3. **Adding SRV / NAPTR Capabilities for Data-Router DNS Server:**

   This feature provides support for configuring the internal Name System (DNS) server with Service (SRV) and Name Authority Pointer (NAPTR) records. This feature is configured using the CLI.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

3.2.8 Data-Router Features

The device supports the following new data-router features:

1. **3G/3.5G Cellular for Primary or Backup WAN Access:**

   This feature provides support for a 3G cellular WAN connection using a USB modem. The 3G cellular WAN interface can be used as the primary WAN interface or as an optional WAN backup when the primary WAN (e.g., WAN Ethernet) fails. The WAN connection type is a point-to-point protocol (PPP) over cellular.

   The device supports the following 3G cellular USB modems:

   - ZTE MF626
   - ZTE MF637
   - Alcatel X220
   - Huawei E182E
   - Sierra Wireless AirCard 308

   The 3G cellular WAN connection can be configured using the Web interface or the CLI (**`configure data`** > **`interface cellular 0/0`**).

   Applicable Products: Mediant 800 MSBG.

2. **ADSL and VDSL WAN Access:**

   This feature provides support for the following xDSL WAN access types:

   - Asymmetric Digital Subscriber Line (ADSL):
     - RFC 2684 in Routed (IPoA) and Bridged (ETHoA) modes, supporting LLC-SNAP and VC-Multiplexed encapsulations over AAL5
     - ATM UNI 4.1 compliant
     - UBR, CBR, VBR classes of service
     - RFC 2364 PPPoA
     - RFC 2516 PPPoE over ATM
     - Up to 8 PVCs
   - Very High-speed Digital Subscriber Line (VDSL):
     - ITU G.991.2 Annex E for Ethernet, also known as EFM or 2Base-TL, as defined in IEEE 802.3ah
     - 802.1q VLANs over EFM
     - PPPoE

   The ADSL and VDSL WAN connections can be configured using the Web interface or the CLI (**`configure data`** > **`interface dsl`**).

   Applicable Products: Mediant 800 MSBG.

3. **Enhanced RIP Support:**

   This feature provides enhanced support for Routing Information Protocol (RIP). RIP can be configured using the Web interface or the CLI.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

4. **GRE Configuration through CLI:**

   This feature provides support for configuring General Routing Encapsulation (GRE) tunneling interfaces through the CLI. Configuration of GRE was supported only through the Web interface in the previous release.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

5. **Capturing VoIP and Data-Routing Traffic:**

   This feature provides support for capturing VoIP and Data-Routing network traffic by sending traces to the CLI or to a file (later sent to a TFTP server). The traffic can be captured using the following new CLI commands to start the debug capture process:

   - **`debug capture voip`**
   - **`debug capture data`**

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

3.2.9 Security Features

The device supports the following new security feature:

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

   This feature provides support for the ARIA algorithm cipher encryption for Secure Real-time Transport Protocol (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 configured by the following parameters:

   - *AriaProtocolSupport* – enables ARIA encryption
   - *SRTPofferedSuites* – using the new options, AES_CM_128_HMAC_SHA1_32 and ARIA_128_BIT

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

   Applicable Products: Mediant 800 MSBG and Mediant 800 (existing support on Mediant 3000).

2. **Reporting of Data-Networking Security Events:**

   This feature provides support for enabling the reporting of security-related events for data-router networking. This feature is configured using the new *ini* file parameter, *EnableSecSyslog*. When enabled, access list rules (configured using the CLI command **`access-list`**) set to "log", issue Syslog messages whenever traffic matching the access list is encountered.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

3. **VoIP Firewall Rules Based on Source Port:**

   This feature provides support for specifying source TCP / UDP port when configuring VoIP firewall rules.

   This feature can be configured in the existing Web interface’s Firewall Settings page, using the new field, “Source Port”. It can also be configured in the CLI, using the new command, **`configure voip > access-list`**.

   Applicable Products: Mediant 600, Mediant 1000, Mediant 2000, and Mediant 3000.

3.2.10 Infrastructure Features

The device supports the following new infrastructure features:

1. **Loop-Current Limiter for FXO Line:**

   This feature provides support for limiting the FXO loop current for the FXO interfaces to a maximum of 60 mA, according to the TBR21 standard. This feature is disabled by default, but can be enabled using the new parameter, *EnableFXOCurrentLimit*.

   Applicable Products: Mediant 600, Mediant 800 MSBG, Mediant 800, Mediant 1000, Mediant 1000 MSBG, and Mediant 1000B.

2. **DC Termination for FXO Line:**

   This new feature allows you to configure the DC termination (resistance) of the FXO line. By default, the line is set to 50 Ohms, but it can be configured to 800 Ohms using the new parameter, *FXODCTermination*.

   Applicable Products: Mediant 600, Mediant 800 MSBG, Mediant 800, Mediant 1000, Mediant 1000 MSBG, and Mediant 1000B.

3. **Power over Ethernet Configuration**:

   This feature provides support for configuring Power over Ethernet (PoE). PoE was supported in the previous release, but without the ability to configure it. This feature can be configured using the new Web page, ‘Power Over Ethernet Settings’ (or CLI).

   PoE provides power on the Ethernet lines through all the device’s LAN ports. It is fully compliant with the IEEE802.3af-2003 standard, providing up to 15.4W per port, and a total budget of 50W or 120W for all ports. PoE is supplied on Pins 4,5: (+), pins 7,8: (-).

   This feature allows you to perform the following PoE configuration:

   - Enable or disable PoE per port (PoE is enabled on all ports upon device startup)
   - Define maximum port power consumption (up to 15.4W) – used when the plugged-in client is detected to be of Class 0 (see following description)

   Upon plugging in a PoE client to one of the ports, the device automatically detects the class to which the client belongs and therefore, the maximum power allowed:

   - Class 0 – user-defined max. power (up to 15.4W)
   - Class 1 – up to 4W max. power
   - Class 2 – up to 7W max. power
   - Class 3 – up to 15.4W max. power

   If the plugged-in client is detected as Class 0, the device saves the user-defined wattage from the total wattage budget (default is 15.4W). If the plugged-in client is detected as Class 1, Class 2, or Class 3, the device saves 4W, 7W, or 15.4W respectively from the total wattage budget. Power budget may vary from 50W to 120W, depending on Mediant 800 MSBG model.

   If the power budget has been exhausted and a new client is plugged in, no power is available to this client.

   Note that the power is always taken off the total budget according to the class detected, regardless of what is actually consumed per port.

   Applicable Products: Mediant 800 MSBG.

3.2.11 Management and Provisioning Features

This subsection describes the new management and provisioning new features.

3.2.11.1 Web Features

The device supports the following new Web interface features:

1. **Web Login Authentication using Smart Cards:**

   This feature provides support for Web login authentication using a third-party, smart card with user identification. When enabled and the user attempts to access the device through the Web browser (HTTPS), the device retrieves the Web user's login username (and other information, if required) from the smart card and the user is then required to provide only the correct login password. Typically, a TLS connection is established between the smart card and the device's Web interface, and a RADIUS server is implemented to authenticate the password with the username. Thus, this feature implements a two-factor authentication - what the user has (i.e., the physical card) and what the user knows (i.e., the login user name).

   This feature can be enabled using the new parameter, *EnableMgmtTwoFactorAuthentication*. Depending on customer requirements, specific device configuration and integration may also be required.

   Applicable Products: This feature is applicable to all devices.

2. **Alarm History Display:**

   This feature provides support for displaying a list of historical alarms. This support is in addition to the already supported display of current alarms. The historical alarms are displayed in the new Web page, 'Alarms History'.

   Applicable Products: This feature is applicable to all devices.

3. **Logged Login Attempts to Management Interface:**

   This feature provides support for enhanced logging (additional event notifications) of attempts made to log in to the device's management interfaces. Each authentication attempt at the device's management port is logged. This is configured using the existing parameter, *ActivityListToLog*.

   Applicable Products: This feature is applicable to all devices.

4. **Performance Monitoring of Trunk Utilization:**

   This feature provides support for real-time display of the number of calls per trunk. This is displayed in the new Web page, 'Trunk Utilization'.

   Applicable Products: This feature is applicable to all devices.

5. **Menu Name "BGP & OSPF" Modified in Web Navigation Tree:**

   This feature changes the menu name, "BGP & OSPF" displayed in the Web Navigation tree to "Dynamic Routing".

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

6. **Selection Method of Default Media Realm Modification:**

   This feature enables the user to determine whether or not a Media Realm is default when configuring a Media Realm. For this support, the Media Realm table now includes a new field, 'Is Default'. In the previous release, the global parameter, cpDefaultMediaRealmName was used to configure the default Media Realm. This parameter is now obsolete.

   Applicable Products: This feature is applicable to all devices.

3.2.11.2 SNMP Features

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

1. **Host Resources MIB (RFC 2790):**

   This feature provides support for the Host Resources MIB, which is used for managing host systems. The term *host* is any computer that communicates with other similar computers connected to the Internet and that is directly used by one or more human beings.

   The following Host Resources MIB objects have been added:

   - hrSystem group
   - hrStorage group (basic only)
   - hrDevice group (CPU, RAM, Flash - basic only)
   - hrSWRunPerf (basic only)
   - hrSWInstalled (OS only)

   Applicable Products: This feature is applicable to all devices.

2. **VoIP Configuration File Download without Parsing:**

   This feature provides support for a new SNMP object, acSysActionSetApplyINImethodthat that enables the EMS to perform VoIP *ini* file download without parsing (similar to the wizard mode). This object is located under the system MIB.

   Applicable Products: This feature is applicable to all devices.

3. **SNMP Trap upon Power Over-Allocation for Power Over Ethernet:**

   This feature provides support for the new SNMP trap, acPowerOverEthernetStatus (OID:1.3.6.1.4.1.5003.9.10.1.21.2.0.80). This trap is sent when insufficient power is available for a plugged-in PoE client in a PoE-enabled LAN port.

   Applicable Products: Mediant 800 MSBG.

4. **SNMP Trap for Detection of Attacks on Media Interfaces:**

   This feature provides support for a new SNMP trap, acMediaProcessOverloadAlarm OID:1.3.6.1.4.1.5003.9.10.1.21.2.0.81 that is sent upon overload of the device's media processing and interfaces.

   Applicable Products: Mediant 800 MSBG, Mediant 800, Mediant 1000 MSBG, Mediant 1000B, Mediant 2000, and Mediant 3000.

5. **SONET Alarms Consolidation:**

   This feature provides support for sending trunk alarms only on the DS3 level. This is in addition to the already supported alarms on the trunk level. The alarm level is configured by the parameter, *DS3AlarmConsolidation*. When enabled, only SDH alarms are raised and no alarms are raised for trunks (even if they exist). When the SDH alarm is cleared, trunk alarms are raised (if they exist).

   Applicable Products: Mediant 3000 with TP-6310.

3.2.11.3 CLI Features

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

1. **Full VoIP Entity Configuration through the CLI Interface:**

   This feature provides support for configuring the VoIP-related parameters through the CLI. Until now, only Data-Routing configuration could be configured through CLI. Thus, the CLI is now a fully supported management tool for the device, providing the following main CLI command paths:

   - **`config voip`** for configuring the VoIP-related parameters such as the following:
     - Network
     - PSTN and TDM
     - Security
     - SIP signaling
     - Media
     - Services (e.g., LDAP and LCR)
     - SIP application enabling
     - SIP control network
     - SIP definitions
     - Coders and profiles
     - GW and IP2IP
     - SBC
     - SAS
     - IP Media
   - **`config system`** for configuring the system-related parameters:
     - Applications (e.g., NTP and DHCP)
     - Syslog
     - Regional settings
     - Certificates
     - Management (e.g., Web, Telnet, and SNMP)
   - **`config data`** – for configuring the data-routing parameters:
     - Routing protocols
     - Interfaces (e.g., Ethernet, T1, and SHDSL)
     - QoS
     - Crypto command
     - NAT

   For more information on configuring the device using CLI, refer to the CLI Reference Manual.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

2. **Display of Current Configuration through CLI:**

   This feature provides support for displaying the current configuration running on the device. This feature also enables saving the current configuration to a file on a computer.

   This feature is done using the new CLI command, **`show running-config`**.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

3. **TACACS+ for CLI Login:**

   This feature provides support for the Terminal Access Controller Access-Control System (TACACS+) remote authentication protocol and user authentication for CLI login. This feature can be configured through the *ini* file (*TacPlusEnable*, *TacPlusServerIp*, *TacPlusSecondaryServerIp*, *TacPlusPort*, *TacPlusTimeout*, and *TacPlusSharedSecretand*) and CLI (**`configure data`** > **`aaa authentication`** and **`configure data`** > **`tacacs-server`**).

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

3.2.12 New Parameters

This section describes the new parameters for Release 6.4. These parameters pertain to the relevant features described in previous sections.

In this section, the *ini* file parameters corresponding to the Web interface name are enclosed in square brackets.

3.2.12.1 SIP General Parameters

The table below describes the new general SIP parameters for Release 6.4. These parameters are applicable to the device's Gateway / IP2IP and SBC applications.

Table 3-1: New SIP General Parameters for Release 6.4

Parameter	Description
Silk Tx Inband FEC **[SilkTxInbandFEC]**	Enables forward error correction (FEC) for the SILK coder. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Silk Max Average Bit Rate **[SilkMaxAverageBitRate]**	Defines the maximum average bit rate for the SILK coder. The valid value range is 5000 to 30000. The default is 16000.
LCR Parameters **Note:** This feature is applicable only to the Gateway application.	
Cost Group Table **[CostGroupTable]**	Defines Cost Groups, where each Cost Group is defined with a fixed call connection charge and a call rate (charge per minute). ▪ Index = Cost Group table entry index. ▪ Cost Group Name = Defines an arbitrary name for the Cost Group. ▪ Default Connect Cost = Defines the call connection cost (added as a fixed charge to the call). This is used if a time band is not defined. The valid range is 0-65533 (the default is 0). ▪ Default Time Cost = Defines the call charge per minute. This is used if a time band is not defined. The valid range is 0-65533 (the default is 0). **Note:** When calculating the cost of a call, if the current time is not within a time band, then the default connection cost and minute charge are used.
[CostGroupTimebands]	Defines time bands and associates them with Cost Groups. The time band defines the day and time range for which the time band is applicable (e.g., from Saturday 05:00 to Sunday 24:00) as well as the fixed call connection charge and call rate per minute for this interval. ▪ CostGroup = Associates a Cost Group with this time band. Up to 21 time bands can be associated with a Cost Group. ▪ TimebandIndex = Defines the timeband index. ▪ StartTime = Defines the start day and time from when this time band is applicable. The format is *day:hr:min* (e.g., SUN:06:00), where: ✓ day = SUN, MON, TUE, WED, THUR, FRI, SAT ✓ hr = 0-23 ✓ min = 0-59

Parameter	Description
	▪ EndTime = Defines the end day and time to when this time band is applicable. ▪ ConnectCost = Defines the call connection cost. This is added as a fixed charge to the call. The valid range is 0-65533 (default is 0). ▪ TimeCost = Defines the call cost per minute charge. The valid range is 0-65533 (default is 0). **Note:** You cannot define overlapping time bands.
Routing Rule Groups Table **[RoutingRuleGroups]**	This table allows you to enable the LCR feature, define the average call duration, and default call cost. [RoutingRuleGroups] FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable, RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost; [\RoutingRuleGroups] Where: ▪ LCREnable = Enables the LCR feature: ✓ **[0]** Disable (default) ✓ **[1]** Enable ▪ LCRAverageCallLength = Defines the average call duration (in minutes) and is used to calculate the variable portion of the call cost. This is useful, for example, when the average call duration spans over multiple time bands. The LCR is calculated as follows: cost = call connect cost + (minute cost * average call duration) The valid range is 0-65533 (default is 1). For example, assume the following Cost Groups: ✓ "Weekend A": call connection cost is 1 and charge per minute is 6. Therefore, a call of 1 minute cost 7 units. ✓ "Weekend_ B": call connection cost is 6 and charge per minute is 1. Therefore, a call of 1 minute cost 7 units. Therefore, for calls under one minute, "Weekend A" carries the lower cost. However, if the average call duration is more than one minute, then "Weekend B" carries the lower cost. ▪ LCRDefaultCost = Determines whether routing rules without a defined Cost Group are considered as a higher cost or lower cost route compared to other matched routing rules with LCR. ✓ **[0]** Min = If the device locates other matching LCR routing rules, this routing rule is considered the lowest cost route and therefore, it is selected as the appropriate route to use (default.) ✓ **[1]** Max = If the device locates other matching LCR routing rules, this routing rule is considered as the highest cost route (and therefore, is not used). **Note:** If more than one valid routing rule without a defined Cost Group exists, the device selects the first-matched rule.
Quality of Experience (QoE) Parameters for SEM	
[QOEServerIP]	Defines the IP address of the Session Experience Manager (SEM) server. Note: For this parameter to take effect, a device reset is required.

Parameter	Description
[QOEPort]	Defines the port of the SEM server. The valid value range is 0 to 65534. The default is 5000.
[QOEInterfaceName]	Defines the IP interface on which the quality experience reports are sent. The default is “DEFAULT”. Note: For this parameter to take effect, a device reset is required.
[QOEConnectionMode]	Defines whether the device connects to the SEM (client) or receives connection from the server (server). The default is client. Note: Currently, only client connection is supported.
[QOEInformationLevel]	Defines the level (i.e., amount of detail) of voice quality information sent to the server. ▪ Standard (default) ▪ Enhanced ▪ Debug
[QOEUseMosLQ]	Enables reporting of the MOS-LQ (listening quality). If disabled, the MOS-CQ is reported (conversational quality). MOS-LQ measures the quality of audio for listening purposes only. MOS-LQ does not take into account bidirectional effects such as delay and echo. MOS-CQ takes into account listening quality in each direction, as well as the bidirectional effects.

3.2.12.2 SIP Gateway Parameters

The table below describes the new SIP Gateway / IP2IP application parameters for Release 6.4.

Table 3-2: New SIP Gateway Parameters for Release 6.4

Parameter	Description
Use EndPoint Number As Calling Number Tel2IP **[UseEPNumAsCallingNumTel2IP]**	Enables the use of the B-channel number as the calling number (sent in the INVITE From field) instead of the phone number (received in the Q.931 Setup message) for Tel-to-IP calls. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** When enabled, this feature is applied before routing and manipulation is done on the source number.
Use EndPoint Number As Calling Number IP2Tel **[UseEPNumAsCallingNumIP2Tel]**	Enables the use of the B-channel number as the calling party number (sent in the Q.931 Setup message) instead of the phone number (received in the SIP INVITE‘s From header) for IP-to-Tel calls. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** When enabled, this feature is applied after routing and manipulation is done on the source number (before sending to the PSTN).

Parameter	Description
ISDN Transfer Mode **[ISDNTransferMode]**	Enables support for QSIG path replacement for IP-to-Tel calls. ▪ **[0]** Slave – disable (default) ▪ **[1]** Master – enable = If a request for a consultation call transfer is received from a PBX (user that has established calls with two SIP UAs), the device sends a SIP REFER message with a Replaces header to the SIP UA to connect it to the second SIP UA (i.e., transfer the call). Once the two SIP UAs are successfully connected (i.e., device receives a SIP NOTIFY 200 message in response to the REFER), the device sends a Q.931 Disconnect message to the PBX notifying the PBX that it can disconnect the ISDN call (thereby, freeing resources on the PBX).
FXO Double Answer **[EnableFXODoubleAnswer]**	Enables the “FXO Double Answer” feature, which rejects (disconnects) incoming Tel (FXO)-to-IP collect calls and signals (informs) this call denial to the PSTN. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Aria Protocol Support **[AriaProtocolSupport]**	Enables ARIA algorithm cipher encryption for SRTP. ARIA is a symmetric key block cipher algorithm standard developed by the Korean National Security Research Institute. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Notes:** ▪ To configure the ARIA bit-key encryption size (128 or 192 bit) with HMAC SHA-1 cryptographic hash function, use the SRTPOfferedSuites parameter. ▪ For ARIA encryption support, the device must be installed with the relevant Software Upgrade Feature Key.

Calling Name Manipulations IP2Tel
[CallingNameMapIp2Tel]
	Configures rules for manipulating the calling name (caller ID) for IP-to-Tel calls. This can include modifying or removing the calling name.
	For example, assume an incoming SIP INVITE message includes the following caller ID:
	`P-Asserted-Identity: "company:john" sip:6666@78.97.79.104`
	Using the calling name manipulation feature, the text, "company" can be modified to "worker" in the outgoing INVITE, as shown below:
	`P-Asserted-Identity: "worker:john" sip:996666@10.13.83.10`
	The format of this *ini* file parameter table is as follows:
	[CallingNameMapIp2Tel]
	FORMAT CallingNameMapIp2Tel_Index = CallingNameMapIp2Tel_DestinationPrefix, CallingNameMapIp2Tel_SourcePrefix, CallingNameMapIp2Tel_CallingNamePrefix, CallingNameMapIp2Tel_SourceAddress, CallingNameMapIp2Tel_RemoveFromLeft, CallingNameMapIp2Tel_RemoveFromRight, CallingNameMapIp2Tel_LeaveFromRight, CallingNameMapIp2Tel_Prefix2Add, CallingNameMapIp2Tel_Suffix2Add;

Parameter	Description
	[\CallingNameMapIp2Tel]
Calling name manipulations Tel2IP **[CallingNameMapTel2Ip]**	Configures rules for manipulating the calling name (caller ID) for Tel-to-IP calls. This can include modifying or removing the calling name. [CallingNameMapTel2Ip] FORMAT CallingNameMapTel2Ip_Index = CallingNameMapTel2Ip_DestinationPrefix, CallingNameMapTel2Ip_SourcePrefix, CallingNameMapTel2Ip_CallingNamePrefix, CallingNameMapTel2Ip_SrcTrunkGroupID, CallingNameMapTel2Ip_SrcIPGroupID, CallingNameMapTel2Ip_RemoveFromLeft, CallingNameMapTel2Ip_RemoveFromRight, CallingNameMapTel2Ip_LeaveFromRight, CallingNameMapTel2Ip_Prefix2Add, CallingNameMapTel2Ip_Suffix2Add; [\CallingNameMapTel2Ip]

MWI Subscribe IP Group ID **[MWISubscribeIPGroupID]**	Defines the IP Group ID used for MWI subscription. The 'SIP Group Name' field value of the IP Group table is used for the Request-URI host name in the outgoing MWI SIP SUBSCRIBE message. The request is sent to the IP address of the Proxy Set that is associated with the IP Group. In addition, the Proxy Set's capabilities such as proxy redundancy and load balancing are also applied to the message.
	For example, if the 'SIP Group Name' field of the IP Group is set to "company.com", the device sends the following SUBSCRIBE message:
	`SUBSCRIBE sip:company.com...`
	Instead of:
	`SUBSCRIBE sip:10.33.10.10...`
	Note: If this feature is not configured, the MWI SUBSCRIBE message is sent to the MWI server as defined by the parameter, *MWIServerIP.*

RTCP Activation Mode **[RTCPActivationMode]**	Disables RTCP traffic when there is no RTP traffic. ▪ **[0]** Active Always (default) = RTCP is active even during inactive RTP periods. ▪ **[1]** Inactive Only If RTP Inactive = No RTCP is sent when RTP is inactive.
Resource-Priority Required **[RPRequired]**	Determines whether the SIP resource-priority tag is added in the SIP Require header in the INVITE message, for Tel-to-IP calls. ▪ **[0]** Disable = Excludes the SIP resource-priority tag from the SIP Require header. ▪ **[1]** Enable (default) = Adds the SIP resource-priority tag in the SIP Require header. Note: This parameter is applicable only to MLPP priority call handling (i.e., only when the *CallPriorityMode* parameter is set to 1).
E&M Parameters	
Voice Type **[EnMVoiceType]**	Defines the E&M voice interface type. ▪ **[0]** Two Wire ▪ **[1]** Four Wire (default)

Parameter	Description
	Note: For this parameter to take effect, a device reset is required.
System Type **[EnmSystemType]**	Defines the E&M signaling type. ▪ **[0]** Signaling (default) ▪ **[1]** Trunking **Note:** For this parameter to take effect, a device reset is required.
Signaling Type **[EnmSignalingType]**	Defines the E&M interfaces hook-signaling type, according to the E&M TIA/EIA-464C standard. The valid value range is 1 to 5. The default is 5. **Note:** For this parameter to take effect, a device reset is required.
Hook Debounce Timing **[EnmHookDebounceTiming]**	Defines the hook detection time. E&M standard requires hook detection after 70 milliseconds of hook status change. The valid value range is 0 to 150. The default is 75. **Note:** For this parameter to take effect, a device reset is required.
Off Hook Glare **[EnmOffHookGlareEnable]**	Enables protection of E&M port from Rx and Tx hook collision. E&M interface can detect hook events from the PSTN side and generate hook signals toward the PSTN side. Situations were generation of hook command toward the PSTN side and detection of hook events from the PSTN side is unavoidable. Since the device supports only the LMR hook type, the device cannot signal a busy condition to the PSTN side. When both event and command collide and EnMOffHookGlareEnable parameter is ON (1), the hook command is rejected and the hook command request is returned for busy signal. ▪ **[0]** Off (default) ▪ **[1]** On **Note:** For this parameter to take effect, a device reset is required.
[EnmCountryCoefficients]	Defines the E&M internal filters and line impedance to USA 600 Ohm or Europe TBR21. When operating with two-wire voice interface type, line impedance is automatically set to 600 Ohm. ▪ **[0]** Disable (default) ▪ **[1]** Enable = loads E&M country coefficient file from the *ini* file. **Note:** For this parameter to take effect, a device reset is required.
[GWInboundManipulationSet]	Defines the Manipulation Set ID for manipulating all inbound INVITE messages. The Manipulation Set is defined using the *MessageManipulations* parameter. By default, no manipulation is done (i.e. Manipulation Set ID is set to -1). **Note:** This parameter is applicable only for the Gateway/IP2IP application.
[GWOutboundManipulationSet]	Defines the Manipulation Set ID for manipulating all outbound INVITE messages. The Manipulation Set is defined using the *MessageManipulations* parameter. By default, no manipulation is done (i.e. Manipulation Set ID is set to -1). **Notes:** ▪ This parameter is used only if the Outbound Message Manipulation Set parameter of the destination IP Group is not set. ▪ This parameter is applicable only for the Gateway/IP2IP application.

3.2.12.3 SIP SAS Parameters

The table below describes the new SIP SAS application parameter for Release 6.4.

Table 3-3: New SIP SAS Parameters for Release 6.4

Parameter	Description
[SASInboundManipulation Mode]	Enables destination number manipulation in incoming INVITE messages when SAS is in Emergency the state: - **[0]** = None (default) - **[1]** = Emergency only – enables manipulating the destination number in the Request-URI of incoming INVITE messages when SAS is in emergency state. This is required, for example, if the call is destined to a registered user, but the destination number in the received INVITE is not the number assigned to the registered user in the SAS registration database. To overcome this and successfully route the call, this feature allows you to define manipulation rules (in the IP to IP Inbound Manipulation table) to change the INVITE's destination number so that it matches that of the registered user in the database.

3.2.12.4 SBC Parameters

The table below describes the new SBC application parameters for Release 6.4.

Table 3-4: New SBC Parameters for Release 6.4

Parameter	Description
Enable Bye Authentication **[SBCEnableByeAuthentication]**	Enables authenticating a SIP BYE request prior to the disconnection of a call. This feature prevents, for example, a scenario in which the SBC SIP client receives a BYE request from a third-party imposer assuming the identity of a participant in the call and as a consequence, the call between the first and second parties is inappropriately disconnected. - **[0]** Disable (default) - **[1]** Enable = The SIP client issues an authentication request to the sender of the BYE request, who then needs to identify itself. The call (i.e., media) is disconnected only if the sender of the BYE request is successfully authenticated (i.e., upon receipt of a SIP 401 “Unauthorized” response for user agents or 407 “Proxy Authentication Required” for proxy servers).
Message Policy Table **[MessagePolicy]**	Configures SIP message rules for blocking (blacklist) unwanted incoming SIP messages and allowing (whitelist) receipt of desired messages. The message policy can apply globally (default) or per signaling domain (i.e., assigned to a SIP interface in the SIP Interface table). The policy can be assigned a reject, ignore, or allow action. This feature is helpful against VoIP fuzzing (also known as robustness testing), which sends different types of packets to its "victims" for finding bugs and vulnerabilities. For

Parameter	Description
	example, the attacker might try sending a SIP message containing either an oversized parameter or too many occurrences of a parameter. [MessagePolicy] FORMAT MessagePolicy_Index = MessagePolicy_Policy, MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength, MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders, MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection, MessagePolicy_MethodListType, MessagePolicy_MethodList, MessagePolicy_BodyListType, MessagePolicy_BodyList; [/MessagePolicy] Where: ▪ MaxMessageLength = Maximum message length (up to 32768 characters) ▪ MaxHeaderLength = Maximum SIP header length (up to 256 characters) ▪ MaxBodyLength = Maximum message body length – value of the Content-Length header (up to 512 characters) ▪ MaxNumHeaders = Maximum number of headers (up to 16) ▪ MaxNumBodies = Maximum number of bodies (up to 2) ▪ SendRejection = Send response if message request is rejected – sends a 400 Bad Request response ▪ MethodListType = Policy for defined SIP methods - blacklist or whitelist ▪ MethodList = Rule applies to defined SIP methods (e.g., “INVITE/BYE”) ▪ BodyListType = Policy for defined SIP body - blacklist or whitelist ▪ BodyList = Rule applies to defined SIP body (i.e., value of the Content-Type header) For example: MessagPolicy 0 = 0, 32768, 256, 512, 16, 2, 0, 0, “INVITE,BYE”, 0, “” The policy defined above limits messages to 32768 characters, headers to 256 characters, bodies to 512 characters, limits number of headers to 16, and only permits two bodies. Invalid requests are rejected. Only INVITE and BYE requests are permitted and there are no restrictions on bodies.

Parameter	Description
Condition Table **[ConditionTable]**	Configures Conditions for SIP messages and supports the same syntax used in the SIP Message Manipulation table. These Condition rules are later assigned to Classification rules in the Classification table for enhancing the process for classifying an incoming SIP dialog to an IP Group. [ConditionTable] FORMAT ConditionTable_Index = ConditionTable_Condition, ConditionTable_Description; [\ConditionTable]
SBC Preferences Mode **[SBCPreferencesMode]**	Determines the order of the Extension coders (coders added if there are no common coders between SDP offered coders and Allowed coders) and Allowed coders (defined in the Allowed Coders Group table) in the outgoing SIP message (in the SDP section). ▪ **[0]** Doesn't Include Extensions = Extension coders are added at the end of the list (default). ▪ **[1]** Include Extensions =
[SBCExtensionsProvisioningMode]	Enables SBC user registration for interoperability with BroadSoft BroadWorks server to provide call survivability in case of connectivity failure with the BroadWorks server. ▪ **[0]** = Normal processing of REGISTER messages (default). ▪ **[1]** = Registration method for BroadWorks server. In a failure scenario with BroadWorks, the device acts as a backup SIP proxy server, maintaining call continuity between the enterprise LAN users (subscribers), and between the subscribers and the PSTN (if provided). In normal operation, when subscribers (e.g., IP phones) register to the BroadWorks server through the SBC, the SBC includes the Allow-Events header in the sent REGISTER message. In response, the BroadWorks server sends the SBC a SIP 200 OK with an XML body containing subscriber information such as extension number, phone number, and URIs (aliases). The SBC forwards the 200 OK to the subscriber (without the XML body). The SBC saves these users with their phone numbers and extensions in its registration database, thus enabling routing to these destinations during survivability mode. When in survivability mode, the device routes the call to the Contact associated with the dialed phone number or extension number in the registration database.
Lifetime of the nonce in seconds **[AuthNonceDuration]**	Defines the lifetime (in seconds) that the current nonce is valid. The device challenges a message that attempts to use a server nonce beyond this period. This parameter is used to provide replay protection (i.e., ensures that old communication streams cannot be used in replay attacks). The valid value range is 30 to 600. The default value is 300.

Parameter	Description
Authentication Challenge Method **[AuthChallengeMethod]**	Defines the type of authentication challenge. - **[0]** 0 = Send SIP 401 "Unauthorized" with a WWW-Authenticate header, as the authentication challenge response. (default) - **[1]** 1 = Send SIP 407 "Proxy Authentication Required" with a Proxy-Authenticate header, as the authentication challenge response.
Authentication Quality of Protection **[AuthQOP]**	Specifies the authentication and/or integrity level of quality of protection (QOP) for digest authentication offered to the client. When the device challenges a SIP request (e.g., INVITE), it sends a 401 response with the Authorization header containing the 'qop' parameter indicating the level of QoP of the message to be authenticated. In response, the SBC client needs to send the device another INVITE with the MD5 hash of the INVITE message and indicates its auth or auth-int support. - **[0]** Auth = The device sends 'qop=auth' in the SIP response, requesting authentication required (i.e., validates user by checking user name and password). This option does not authenticate the message body (i.e., SDP). - **[1]** auth-int = = The device sends 'qop=auth-int' in the SIP response, indicating authentication and authentication with integrity (e.g., checksum) required. This option restricts the client to authenticating the entire SIP message, including the body, if present. - **[2]** Auth-Int and Auth = The device sends 'qop=auth, auth-int' in the SIP response, indicating either authentication or integrity (default). Allows the client to choose auth or auth-int. If the client chooses auth-int, the body is included in the authentication. If the client chooses auth, then the body is not authenticated. (default)
[EnableSBCMediaSync]	Enables SBC media synchronization process for calls established from SIP forking initiated by external proxy servers. It is possible that a call is established with the media not synchronized between the SBC legs. The media synchronization process solves this issue. - **[0]** Disable - **[1]** Enable (default)

3.2.12.5 Media Parameters

The table below describes the new media parameters for Release 6.4.

Table 3-5: New Media Parameters for Release 6.4

Parameter	Description
Acoustic Echo Cancellation Parameters	
Network Echo Suppressor Enable **[AcousticEchoSuppressorSupport]**	Enables the network Acoustic Echo Suppressor feature on SBC calls. This feature removes echoes and sends only the near-end's desired speech signal to the network (i.e., to the far-end party). ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** For this parameter to take effect, a device reset is required.
Echo Canceller Type **[EchoCancellerType]**	Defines the echo canceller type. ▪ **[0]** Line echo canceller = Echo canceller for Tel side (default) ▪ **[1]** acoustic echo suppressor = Echo canceller for IP side
Attenuation Intensity **[AcousticEchoSuppAttenuationIntensity]**	Defines the acoustic echo suppressor signals identified as echo attenuation intensity. The valid range is 0 to 3. The default is 0.
Max ERL Threshold - DB **[AcousticEchoSuppMaxERLThreshold]**	Defines the acoustic echo suppressor maximum ratio between signal level and returned echo from the phone (in decibels). The valid range is 0 to 60. The default is 10.
Min Reference Delay x10 msec **[AcousticEchoSuppMinRefDelayx10ms]**	Defines the acoustic echo suppressor minimum reference delay (in 10-ms units). The valid range is 0 to 40. The default is 0.
Max Reference Delay x10 msec **[AcousticEchoSuppMaxRefDelayx10ms]**	Defines the acoustic echo suppressor maximum reference delay (in 10-ms units). The valid range is 0 to 40. The default is 40 (i.e., 40 x 10 = 400 ms).

3.2.12.6 Networking Parameters

The table below describes the new networking parameter for Release 6.4.

Table 3-6: New Networking Parameters for Release 6.4

Parameter	Description
WAN OAMP Interface **[OAMPWanInterfaceName]**	Binds the OAMP interface to a WAN interface, which can later be associated with a Virtual Routing and Forwarding (VRF).

3.2.12.7 Security Parameters

The table below describes the new security parameters for Release 6.4.

Table 3-7: New Security Parameters for Release 6.4

Parameter	Description
[EnableSecSyslog]	Enables the reporting of security-related events for data networking. When enabled, access list rules (configured using the CLI command **access-list**) set to "log", issue Syslog messages whenever traffic matching the access list is encountered. ▪ **[0]** = Disabled (default) ▪ **[1]** = Enabled
TACACS+ for CLI Login	
[TacPlusEnable]	Enables Terminal Access Controller Access-Control System (TACACS+) remote authentication protocol and user authentication for CLI login. ▪ **[0]** = Disabled (default) ▪ **[1]** = Enabled **Note:** For this parameter to take effect, a device reset is required.
[TacPlusServerIp]	Defines the IP address (in dotted decimal notation) of the TACACS+ primary authentication server.
[TacPlusSecondaryServerIp]	Defines the IP address (in dotted decimal notation) of the TACACS+ secondary authentication server.
[TacPlusPort]	Defines the TACACS+ authentication port (UDP) for authenticating with the RADIUS server. The valid value range is 1 to 15. The default is 49.
[TacPlusTimeout]	Defines the TACACS+ response timeout (in seconds). If no response is received within this period, retransmission is required. The valid value range is 1 to 15. The default is 5.
[TacPlusSharedSecretand]	Defines the TACACS+ shared secret between client and server. The valid value can be a string of up to 64 characters. The default value is “msbg”.

3.2.12.8 Infrastructure Parameters

The table below describes the new infrastructure parameters for Release 6.4.

Table 3-8: New Infrastructure Parameters for Release 6.4

Parameter	Description
[EnableFXOCurrentLimit]	Enables limiting the FXO loop current to a maximum of 60 mA (according to the TBR21 standard). - **[0]** = FXO line current limit is disabled (default). - **[1]** = FXO loop current is limited to a maximum of 60 mA. **Note:** For this parameter to take effect, a device reset is required.
[FXODCTermination]	Defines the DC termination (i.e., resistance) of the FXO line. - **[0]** = Line is set to 50 Ohms (default). - **[1]** = Line is set to 800 Ohms. **Note:** For this parameter to take effect, a device reset is required.

Power over Ethernet Settings
[POETable]
	This table enables PoE per port and configures the maximum power consumption allowed per LAN port for Class 0 clients connected to it. This is done in the Power Over Ethernet Settings table.
	[POETable]
	FORMAT POETable_Index = POETable_PortEnable, POETable_PortPower;
	POETable 0 = 1, 15400;
	POETable 1 = 1, 15400;
	POETable 2 = 1, 15400;
	POETable 3 = 1, 15400;
	POETable 4 = 1, 15400;
	POETable 5 = 1, 15400;
	POETable 6 = 0, 15400;
	POETable 7 = 1, 15400;
	POETable 8 = 1, 15400;
	POETable 9 = 1, 15400;
	POETable 10 = 1, 15400;
	POETable 11 = 1, 15400;
	[\POETable]
	Where:
	- Index = Port number (0 is port 1)
	- PortEnable = enables [1] or disables [0] PoE
	- PortPower = defines maximum power consumption
	Notes:
	- PoE is enabled on all ports upon a device reset.
	- The maximum port power consumption is 15.4W (depending on the class type of the client connected to the LAN port)

3.2.12.9 Management and Provisioning Parameters

The table below describes the new management and provisioning parameter for Release 6.4.

Table 3-9: New Management and Provisioning Parameters for Release 6.4

Parameter	Description
[EnableMgmtTwoFactorAuthentication]	Enables Web login authentication using a third-party, smart card. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable When enabled, the device retrieves the Web user's login username from the smart card, which is automatically displayed (read-only) in the Web Login screen; the user is then required to provide only the login password. Typically, a TLS connection is established between the smart card and the device's Web interface, and a RADIUS server is implemented to authenticate the password with the username. Thus, this feature implements a two-factor authentication - what the user has (the physical card) and what the user knows (i.e., the login user name).

3.2.13 Modified Parameters

This section describes parameters from the previous release that have been modified in Release 6.4. These parameters pertain to the relevant features described in previous sections.

3.2.13.1 SIP General Parameters

The table below describes the SIP general parameters from the previous release that have been modified in Release 6.4.

Table 3-10: Modified SIP General Parameters for Release 6.4

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Coders Table / Coder Group Settings Table
<b>[CodersGroup]</b></td><td><b>Modification:</b> SILK coder added.
<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>silk-nb
<b>[Silk-8Khz]</b></td><td>20 (default), 40, 60, 80, and 100</td><td>8</td><td>Dynamic (default is 76)</td><td>N/A</td></tr>
<tr><td>silk-wb
<b>[Silk-16Khz]</b></td><td>20 (default), 40, 60, 80, and 100</td><td>16</td><td>Dynamic (default is 77)</td><td>N/A</td></tr>
</table></td></tr>
<tr><td>Outbound IP Routing Table
<b>[Prefix]</b></td><td><b>Modification:</b> New field, “CostGroup” – associates an LCR Cost Group with a routing rule.
[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<b>_CostGroup</b>;
[\PREFIX]</td></tr>
</table>

3.2.13.2 SIP Gateway Parameters

The table below describes the SIP Gateway parameters from the previous release that have been modified in Release 6.4.

Table 3-11: Modified SIP Gateway Parameters for Release 6.4

Parameter	Description
IP Profile Table **[IPProfile]**	**Modifications:** ▪ EnableEchoCanceller – existing field with new option, “Acoustic” for enabling the Acoustic Echo Cancellation feature.*EnableQSIGTunneling* – new field, enabling QSIG tunneling over SIP per IP call SBCFaxCodersGroupID – selects supported fax coders (from the Coders Group Settings table) ▪ SBCFaxBehavior – defines negotiation method for fax offer: ✓ **[0]** Pass fax transparently, without interference (default).

Parameter	Description
	✓ **[1]** Handle fax according to fax settings in the IP Profile for all offer-answer transactions (including the initial INVITE). ✓ **[2]** Handle fax according to fax settings in the IP Profile for all re-INVITE offer-answer transactions (excluding initial INVITE). ▪ SBCFaxOfferMode – determines the coders included in the outgoing SDP offer (sent to the called "fax"): ✓ **[0]** All = use only (and all) the coders of the selected Coders Group Settings table (SCFaxCodersGroupID). (default) ✓ **[1]** Single = use only one coder. If a coder in the incoming offer (from the calling "fax") matches a coder in the SBCFaxCodersGroupID, then the device uses this coder. If no match exists, then the device uses the first coder in the Coders Group Settings table (SCFaxCodersGroupID). ▪ SBCFaxAnswerMode - determines the coders included in the outgoing SDP answer (sent to the calling "fax"):**[0]** All = use matched coders between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group Settings table (SBCFaxCodersGroupID). ✓ **[1]** Single = use only one coder. If the incoming answer (from the called "fax") includes a coder that matches a coder match between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group Settings table (SCFaxCodersGroupID, then the device uses this coder. If no match exists, the device uses the first listed coder of the matched coders between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group Settings table (SCFaxCodersGroupID. (default). [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,

Parameter	Description
	IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID, IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode; [\IpProfile]
Web/EMS: SRTP offered Suites **[SRTPofferedSuites]**	**Modification:** New options. ▪ **[4]** CIPHER SUITES ARIA CM 128 HMAC SHA1 80 = device uses ARIA encryption algorithm with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag. ▪ **[8]** CIPHER SUITES ARIA CM 192 HMAC SHA1 80 = device uses ARIA encryption algorithm with a 192-bit key and HMAC-SHA1 message authentication with a 32-bit tag. **Note:** For enabling ARIA encryption, use the AriaProtocolSupport parameter.
Channel Select Mode **[ChannelSelectMode]**	**Modification:** New option. ▪ **[11]** Dest Number + Ascending = This channel select method for allocating a Trunk Group channel to an incoming IP-to-Tel call is as follows: **a.** The device attempts to route the call to the channel that is associated with the destination (called) number. If located, the call is sent to that channel. **b.** If the number is not located or the channel is unavailable (e.g., busy), the device searches in ascending order for the next available channel in the Trunk Group. If located, the call is sent to that channel. **c.** If the device reaches the highest channel in the Trunk Group and all the channels are unavailable, the call is released.

Parameter	Description
Trunk Transfer Mode **[TrunkTransferMode]**	**Modification:** New option. ▪ **[6]** = Supports AT&T toll free out-of-band blind transfer for trunks configured with the 4ESS ISDN protocol. This trunk transfer method is done when a SIP REFER message is received. AT&T courtesy transfer is a supplementary service which enables a user (e.g., user A) to transform an existing call between user A and user B into a new call between user B and user C, whereby user A does not have a call established with user C prior to call transfer. The device handles this feature as follows: ✓ IP-to-Tel (user side): When a SIP REFER message is received, the device performs a transfer by sending a Facility message to the PBX, initiating a transfer. ✓ Tel-to-IP (network side): When a Facility message initiating an out-of-band blind transfer is received from the PBX, the device sends a SIP REFER message to the IP side (if the EnableNetworkISDNTransfer parameter is set to 1).
Source Number Preference **[SourceNumberPreference]**	**Modification:** Ability to select header. Defines from where the device obtains the calling (source) number in incoming INVITE requests. This can be obtained from one of the following headers: ▪ The first P-Asserted-Identity header ▪ The second P-Asserted-Identity header (if exists) ▪ The From header If not configured (default), the Request-URI is obtained from the first P-Asserted-Identity header.

3.2.13.3 SBC Parameters

The table below describes SBC parameters from the previous release that have been modified in Release 6.4.

Table 3-12: Modified SBC Parameters for Release 6.4

Parameter	Description
Classification Table **[Classification]**	**Modifications:** New fields: ▪ MessageCondition = Assigns a Condition rule (defined in the Condition table) that is also used to classify the incoming SIP dialog to an IP Group. ▪ SrcPort = Defines the source port of the incoming SIP dialog used for classifying it to an IP Group. ▪ SrcTransportType = Defines the source transport type (UDP, TCP, or TLS) of the incoming SIP dialog used for classifying it to an IP Group. ▪ ActionType = Defines a whitelist or blacklist that allows or denies, respectively an incoming SIP dialog that matches the classification characteristics. [Classification] FORMAT Classification_Index = Classification_MessageCondition, Classification_SrcSRDID, Classification_SrcAddress, Classification_SrcPort, Classification_SrcTransportType, Classification_SrcUsernamePrefix, Classification_SrcHost,

Parameter	Description
	Classification_DestUsernamePrefix, Classification_DestHost, Classification_ActionType, Classification_SrcIPGroupID; [\Classification]
IP Group Table **[IPGroup]**	**Modifications:** New fields: ▪ RegistrationMode: ✓ **[0]** User initiates registrations (default) ✓ **[1]** SBC initiate registrations (works only with User Info file) = Used when the device serves as a client (with, for example, and IP PBX) ✓ **[2]** No registrations needed = The device adds users to its database in active state. ▪ AuthenticationMode: ✓ **[0]** User Authenticates (default) = The device does not handle the authentication, but simply passes the authentication messages between the SIP user agents. ✓ **[1]** SBC Authenticates (as Client) = The device authenticates as a client. It receives the 401/407 response from the proxy requesting for authentication. The device sends the proxy the authorization credentials (i.e., user name and password) according to one of the following: 1) account defined in the Account table (only if authenticating SERVER-type IP Group), 2) global username and password parameters (only if authenticating SERVER-type IP Group), 3) User Information file, or 4) sends request to users requesting credentials (only if authenticating USER-type IP Group). ✓ **[2]** SBC Authenticates (as Server) = The device authenticates as a server (using the User Information file). ▪ MethodList = SIP methods to challenge. Multiple entries are separated by "/". If none are defined (default), no methods are challenged. ▪ EnableSBCClientForking: ✓ [0] No (default) ✓ [1] Yes = The device forks INVITE messages (to up to five separate SIP outgoing legs). [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_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList, IPGroup_EnableSBCClientForking, IPGroup_ContactName; IPGroup 1 = 0, , -1, , , 0, -1, 0, 0, -1, 0, , 1, 0, -1, -1, -1, 2, 2, INVITE, 0, ; [\IPGroup]

3.2.13.4 Media Parameters

The table below describes a media parameter from the previous release that has been modified in Release 6.4.

Table 3-13: Modified Media Parameter for Release 6.4

Parameter	Description
Media Realm Table **[CpMediaRealm]**	**Modifications:** New fields. ▪ IsDefault = Defines the default Media Realm: ✓ **[0]** No ✓ **[1]** Yes [CpMediaRealm] FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd, CpMediaRealm_TransRateRatio, CpMediaRealm_**IsDefault**; [\CpMediaRealm]

3.2.13.5 Networking Parameters

The table below describes networking parameters from the previous release that have been modified in Release 6.4.

Table 3-14: Modified Networking Parameters for Release 6.4

Parameter	Description
RTP Redundancy Depth **[RTPRedundancyDepth]**	**Modification:** New option. - **[5]** 5 = five levels of RTP redundancy (according to RFC 2198)
Multiple Interface Table **[InterfaceTable]**	**Modification:** New field: - UnderlyingInterface = Assigns the Ethernet ports to an IP network interface [InterfaceTable] FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID, InterfaceTable_InterfaceName, InterfaceTable_**UnderlyingInterface**; [\InterfaceTable]

3.2.13.6 Security Parameters

The table below describes security parameters from the previous release that have been modified in Release 6.4.

Table 3-15: Modified Security Parameter for Release 6.4

Parameter	Description
Firewall Settings Table **[AccessList]**	**Modification:** New field. - Source_Port = Defines the source UDP or TCP port (on the remote host) from where packets are sent to the device. The valid range is 0 to 65535. [AccessList] FORMAT AccessList_Index = AccessList_Source_IP, AccessList_**Source_Port**, 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]

3.2.14 Obsolete Parameters

Parameters from the previous release that are now obsolete in Release 6.4 are listed in the table below.

Table 3-16: Obsolete Parameters

Obsolete Parameter	Description
[AMDDetectionDirection]	AMD detection direction (from PSTN or IP) is no longer supported.
[cpDefaultMediaRealmName]	This parameter has been replaced by the new Media Realm table field, 'Is Default'.
[WANMgmtHTTPSPort]	This parameter has been replaced by the AllowWanHTTPS parameter. **Note:** Applicable only to Mediant 800 MSBG and Mediant 1000 MSBG.
[WANMgmtHTTPPort]	This parameter has been replaced by the AllowWanHTTP parameter. **Note:** Applicable only to Mediant 800 MSBG and Mediant 1000 MSBG.
[WanMgmtSSHPort]	This parameter has been replaced by the AllowWanSSH parameter. **Note:** Applicable only to Mediant 800 MSBG and Mediant 1000 MSBG.
[WANMgmtSNMPPort]	This parameter has been replaced by the AllowWanSNMP parameter. **Note:** Applicable only to Mediant 800 MSBG and Mediant 1000 MSBG.
[WanMgmtTelnetPort]	This parameter has been replaced by the AllowWanTelnet parameter. **Note:** Applicable only to Mediant 800 MSBG and Mediant 1000 MSBG.

4 DSP Firmware Templates and Channel Capacity

This section lists the DSP firmware templates for Release 6.4. These DSP templates indicated the maximum number of channels supported for various supplementary capabilities and voice coders.

Notes:

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

4.1 Mediant 800 and Mediant 800 MSBG

The Mediant 800 and Mediant 800 MSBG DSP templates for Release 6.4 are shown in the table below.

Table 4-1: Channel Capacity Templates for Mediant 800 and Mediant 800 MSBG

Telephony Interfaces Assembly[6]	Number of DSP Channels on Physical Interface	Advanced DSP Capabilities[7]							
		IPM Detectors[8]	AMR WB	SILK	SILK WB	V.150.1[9]	Transcoding Sessions	Conference Participants[10]	SBC Sessions
1 x E1/T1	31 / 24	-	-	-	-	-	6	-	19 / 26
	31 / 24	Yes		Yes		Yes	-	-	19 / 26
1 x E1/T1 & FXS / FXO Combination x 8	39 / 32	Yes	-	-	-	-	-	-	11 / 28
	0 / 32	Yes	-	Yes	-	-	-	-	0 / 18
12 x FXS	12	-	-	Yes	-	-	-	-	38
	12	Yes	-	-	-	Yes	-	-	38
	11	Yes	-	Yes	-	-	-	-	39
4 x FXS & 8 x FXO	12	Yes	-	-	-	-	-	-	38
	11	Yes	-	Yes	-	-	-	-	39

[6] For the relevant model, see Table 2-1 on page 11, Table 2-2 on page 13, and Table 2-3 on page 14. For example, for the "1 x E1/T1" assembly, the relevant model includes **M800-1ET-12L-P**.

[7] All hardware assemblies also support the following DSP channel capabilities: IBS, echo cancellation (EC), CID (caller ID), silence compression (SC), T.38, G.711, G.726, G.729, G.723.1, G.722, AMR, RTCP XR reporting, SRTP.

[8] IPM Detectors include Automatic Gain Control (AGC) and Answer Detector (AD).

[9] V.150.1 is supported only for the US Department of Defense (DOD).

[10] The number of available three-way conferences (bridges) is the number of conference participants divided by three.

Telephony Interfaces Assembly[6]	Number of DSP Channels on Physical Interface	Advanced DSP Capabilities[7]							
		IPM Detectors[8]	AMR WB	SILK	SILK WB	V.150.1[9]	Transcoding Sessions	Conference Participants[10]	SBC Sessions
4 x FXS & 4 x FXO	8	Yes	-	Yes	-	-	-	-	42
4 x BRI	8	Yes	-	Yes	-	-	-	-	42
8 x BRI	16	-	-	-	-	-	-	-	34
	14	-	-	Yes	-	-	-	-	36
	12	Yes	-		-	-	-	-	38
	10	Yes	-	Yes	-	-	-	-	40
4 x BRI & 4 x FXS	12	-	-	Yes	-	-	-	-	38
	12	Yes	-	-	-	-	-	-	38
	11	Yes	-	Yes	-	-	-	-	39
4 x BRI & 4 x FXS & 4 x FXO	16	-	-	-	-	-	-	-	34
	14	-	-	Yes	-	-	-	-	36
	12	Yes	-	-	-	-	-	-	38
	10	Yes	-	Yes	-	-	-	-	40
6 x E&M[11]	6	-	-	-	-	-	-	-	44
4 x FXS or 4 x FXO	4	-	-	Yes	-	Yes	-	-	46
	4	-	-		-	-	3	7	46
	4	-	-	Yes	-	-	2	6	46
	4	Yes	Yes	Yes	-	-	1	4	46
	4	Yes	Yes	Yes	Yes	-	1	3	46
SBC (telephony interfaces may be present, but inactive)	-	-	-	-	-	-	-	-	50
Without Telephony Interfaces	-	-	-	-	-	-	16	-	50
	-	-	-	Yes	-	-	15	-	50
	-	-	Yes	Yes	Yes	-	10	-	50

[11] E&M signaling interfaces are applicable only to Mediant 800.

4.2 Mediant 600, Mediant 1000 and Mediant 1000 MSBG

This section lists the Mediant 600, Mediant 1000, and Mediant 1000 MSBG DSP templates for the following interfaces:

- Analog (FXS/FXO) – see Section 4.2.1 on page 81
- Digital interfaces – see Section 4.2.2 on page 82
- Media processing interfaces (MPM module) – see Section 4.2.3 on page 83

Note: The maximum number of channels on any form of analog, digital, and MPM modules assembly is 120.

4.2.1 Analog Interfaces

The DSP templates for analog interfaces are shown in the table below.

Table 4-2: DSP Firmware Templates for 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.723.1	Yes	Yes
G.729 A, B	Yes	Yes
G.722	-	Yes

4.2.2 Digital Interfaces

The DSP templates for digital interfaces are shown in the table below.

Table 4-3: DSP Firmware Templates for Digital Interfaces

	DSP Template														
	0 or 10			**1 or 11**			**2 or 12**			**5 or 15**			**6 or 16**		
	Number of Spans														
	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	24	36	60	31	60	100
With 128 ms EC	31	60	100	31	48	80	24	36	60	24	36	60	31	60	100
With SRTP	31	60	100	NA	NA	NA	24	36	60	24	36	60	31	48	80
With IPM Features[12]	31	60	100	NA	NA	NA	NA	NA	NA	NA	NA	NA	31	60	100
With IPM Features & SRTP	31	48	80	NA	NA	NA	NA	NA	NA	NA	NA	NA	31	48	80
Voice Coder															
G.711 A-law/Mμ-law PCM	✓			✓			✓			✓			✓		
G.726 ADPCM	✓			✓			✓			✓			-		
G.723.1	✓			-			-			-			-		
G.729 A, B	✓			✓			✓			✓			✓		
GSM FR	✓			✓			-			-			-		
MS GSM	✓			✓			-			-			-		
iLBC	-			-			-			✓			-		
EVRC	-			-			✓			-			-		
QCELP	-			-			✓			-			-		
AMR	-			✓			-			-			-		
GSM EFR	-			✓			-			-			-		
G.722	-			-			-			-			✓		
Transparent	✓			✓			✓			✓			✓		

[12] IPM Features refers to the configuration that includes at least one of the following:

- Mounted MPM module in Slot #6 for conference applications.
- IPM detectors (e.g., Answer Detector) are enabled.
- The IP Media Channels featured is enabled.

4.2.3 Media Processing Interfaces

The DSP templates for the media processing interfaces (i.e., MPM module) are shown in the table below.

Notes:

- The MPM module DSP templates are applicable only to Mediant 1000 and Mediant 1000 MSBG.
- Assembly of the MPM module in Slot #6 enables DSP conferencing capabilities.
- To use the MPM module, the IP Media Channels feature key must be installed on the device.

Table 4-4: DSP Firmware Templates for MPM Module

			DSP Template									
			0 or 10		1 or 11		2 or 12		5 or 15		6 or 16	
			Assembly Slot no.									
			1-5	6	1-5	6	1-5	6	1-5	6	1-5	6
Supplementary Capabilities			Number of Channels									
SRTP	IPM Detectors	Conference										
-	-	-	40	20	32	16	24	12	24	12	40	20
✓	-	-	40	20	NA	NA	24	12	24	12	40	20
-	✓	-	40	20	NA	NA	NA	NA	NA	NA	40	20
✓	✓	-	32	16	NA	NA	NA	NA	NA	NA	32	16
-	-	✓	40	20	32	16	24	12	24	12	40	20
✓	-	✓	32	16	NA	NA	24	12	24	12	32	16
✓	✓	✓	32	16	NA	NA	NA	NA	NA	NA	32	16
Voice Coder												
G.711 A-law/Mμ-law PCM			✓		✓		✓		✓		✓	
G.726 ADPCM			✓		✓		✓		✓		-	
G.723.1			✓		-		-		-		-	
G.729 A, B			✓		✓		✓		✓		✓	
GSM FR			✓		✓		-		-		-	
MS GSM			✓		✓		-		-		-	
iLBC			-		-		-		✓		-	
EVRC			-		-		✓		-		-	
QCELP			-		-		✓		-		-	
AMR			-		✓		-		-		-	
GSM EFR			-		✓		-		-		-	
G.722			-		-		-		-		✓	
Transparent			✓		✓		✓		✓		✓	

4.3 Mediant 2000

The DSP templates for Mediant 2000 are shown in the table below.

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

Table 4-5: DSP Firmware Templates for Mediant 2000

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

4.4 Mediant 3000

This section lists the Mediant 3000 DSP templates for the following:

- Mediant 3000 full chassis – see Section 4.4.1 on page 86
- Mediant 3000 with 16 E1 / 21 T1 – see Section 4.4.2 on page 88
- Mediant 3000 with single T3 – see Section 4.4.3 on page 90
- DSP template mix feature – see Section 4.4.3 on page 90

4.4.1 Mediant 3000 Full Chassis

The DSP templates for Mediant 3000 are shown in the table below. For Release 6.4, the following updates were done:

- The following supplementary capabilities were added to the matrix - IPM Detectors and Acoustic Echo Suppressor
- The Enhanced G.711 coder was removed

Table 4-6: 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**	**IPM Detectors**	**Acoustic Echo Suppressor**									
-	-	-	-	-	2016	2016	1764	1260	1260	1638	1008	1512	630
-	-	✓	✓	-	1890	1890	1638	1134	1134	1638	1008	1512	630
-	-	-	-	✓	1134	1260	1134	756	1008	882	252	1134	252
✓	-	-	-	-	1764	-	-	-	-	1638	1008	-	630
✓	-	✓	✓	-	1638	-	-	-	-	1512	1008	-	630
✓	✓	-	-	-	1638	-	-	-	-	1386	1008	-	504
✓	✓	✓	✓	-	1638	-	-	-	-	1386	1008	-	504
✓	✓	✓	✓	✓	1134	-	-	-	-	882	252	-	252
Voice Coder													
AMR					-	✓	-	✓	-	-	-	-	-
AMR-WB					-	-	-	✓	-	-	-	-	-
EVRC					-	-	✓	-	✓	-	-	-	-
EVRC-B					-	-	-	-	✓	-	-	-	-
G.711 A/μ-law PCM					✓	✓	✓	✓	✓	✓	✓	✓	✓
G.722					-	-	-	✓	-	-	-	✓	✓
G.723.1					✓	-	-	-	-	-	-	-	-
G.726 ADPCM					✓	✓	✓	✓	✓	✓	-	-	-
G.729 A, B					✓	✓	✓	✓	✓	✓	✓	✓	✓
G.729.1 (up to 12 kbps)					-	-	-	-	-	-	-	-	-
GSM EFR					-	✓	-	✓	-	-	-	-	-
GSM FR					✓	✓	-	✓	-	-	-	-	-
iLBC					-	-	-	-	-	✓	-	-	-
MS GSM					✓	✓	-	✓	-	-	-	-	-
MS-RTA (NB)					-	-	-	-	-	-	✓	-	✓
MS-RTA (WB)					-	-	-	-	-	-	-	-	✓
T.38 Version 3					-	-	-	-	-	-	-	✓	-

4.4.2 Mediant 3000 16 E1 / 21 T1

The DSP templates for Mediant 3000 16 E1 / 21 T1 are shown in the table below.

Notes:

- For each IP-to-IP transcoding call, two DSP channels are required.
- For each IP-to-IP call, one DSP channel is required.

Table 4-7: DSP Firmware Templates for Mediant 3000 16 E1 / 21 T1

					DSP Template								
					0	1	2	4	5	7	9	10	11
Supplementary Capabilities					Number of Channels								
SRTP	ARIA	RTCP XR	IPM detectors	Acoustic Echo Suppressor									
-	-	-	-	-	504	504	504	360	360	468	288	432	180
-	-	✓	✓	-	504	504	468	324	324	468	288	432	180
-	-	-	-	✓	324	360	324	216	288	252	72	324	72
✓	-	-	-	-	504	-	-	-	-	468	288	-	180
✓	-	✓	✓	-	468	-	-	-	-	432	288	-	180
✓	✓	-	-	-	468	-	-	-	-	396	288	-	144
✓	✓	✓	✓	-	468	-	-	-	-	396	288	-	144
✓	✓	✓	✓	✓	324	-	-	-	-	252	72	-	72
Voice Coder													
AMR					-	✓	-	✓	-	-	-	-	-
AMR-WB					-	-	-	✓	-	-	-	-	-
EVRC					-	-	✓	-	✓	-	-	-	-
EVRC-B					-	-	-	-	✓	-	-	-	-
G.711 A/µ-law PCM					✓	✓	✓	✓	✓	✓	✓	✓	✓
G.722					-	-	-	✓	-	-	-	✓	✓
G.723.1					✓	-	-	-	-	-	-	-	-
G.726 ADPCM					✓	✓	✓	✓	✓	✓	-	-	-
G.729 A, B					✓	✓	✓	✓	✓	✓	✓	✓	✓
G.729.1 (up to 12 kbps)					-	-	-	-	-	-	-	-	-
GSM EFR					-	✓	-	✓	-	-	-	-	-
GSM FR					✓	✓	-	✓	-	-	-	-	-
iLBC					-	-	-	-	-	✓	-	-	-
MS GSM					✓	✓	-	✓	-	-	-	-	-
MS-RTA (NB)					-	-	-	-	-	-	✓	-	✓
MS-RTA (WB)					-	-	-	-	-	-	-	-	✓
T.38 Version 3					-	-	-	-	-	-	-	✓	-

4.4.3 Mediant 3000 with Single T3

The DSP templates for Mediant 3000 with a single T3 interface are shown in the table below. This is a new DSP template matrix for the Mediant 3000.

Table 4-8: DSP Firmware Templates for Mediant 3000 with Single T3

					DSP Template								
					0	**1**	**2**	**4**	**5**	**7**	**9**	**10**	**11**
Supplementary capabilities					**Number of Channels**								
SRTP	**ARIA**	**RTCP XR**	**IPM detectors**	**Acoustic Echo Suppressor**									
-	-	-	-	-	672	672	672	480	480	624	384	576	240
-	-	✓	✓	-	672	672	624	432	432	624	384	576	240
-	-	-	-	✓	432	480	432	288	384	336	96	432	96
✓	-	-	-	-	672	-	-	-	-	624	384	-	240
✓	-	✓	✓	-	624	-	-	-	-	576	384	-	240
✓	✓	-	-	-	624	-	-	-	-	528	384	-	192
✓	✓	✓	✓	-	624	-	-	-	-	528	384	-	192
✓	✓	✓	✓	✓	432	-	-	-	-	336	96	-	96
Voice Coder													
AMR					-	✓	-	✓	-	-	-	-	-
AMR-WB					-	-	-	✓	-	-	-	-	-
EVRC					-	-	✓	-	✓	-	-	-	-
EVRC-B					-	-	-	-	✓	-	-	-	-
G.711 A/μ-law PCM					✓	✓	✓	✓	✓	✓	✓	✓	✓
G.722					-	-	-	✓	-	-	-	✓	✓
G.723.1					✓	-	-	-	-	-	-	-	-
G.726 ADPCM					✓	✓	✓	✓	✓	✓	-	-	-
G.729 A, B					✓	✓	✓	✓	✓	✓	✓	✓	✓
G.729.1 (up to 12 kbps)					-	-	-	-	-	-	-	-	-
GSM EFR					-	✓	-	✓	-	-	-	-	-
GSM FR					✓	✓	-	✓	-	-	-	-	-
iLBC					-	-	-	-	-	✓	-	-	-
MS GSM					✓	✓	-	✓	-	-	-	-	-
MS-RTA (NB)					-	-	-	-	-	-	✓	-	✓
MS-RTA (WB)					-	-	-	-	-	-	-	-	✓
T.38 Version 3					-	-	-	-	-	-	-	✓	-

4.4.4 Mediant 3000 DSP Template Mix Feature

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 4-9: Template Mix Feature Channel Capacity for Mediant 3000

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

4.5 Mediant 4000 E-SBC

Note: This first release of Mediant 4000 does not contain digital signal processing (DSP) resources. As a result, only SBC functionalities that do not require transcoding are supported.

4.6 Mediant Software E-SBC

Note: This first release of Mediant 4000 does not does not implement digital signal processing (DSP). Therefore, only SBC functionalities that do not require media signal processing are supported.

5 Known Constraints in Release 6.4

This section lists known constraints in Release 6.4.

5.1 SIP Constraints

This release includes the following known SIP constraints:

1. The IP-to-IP and Gateway (IP2IP/GW) applications are not supported.

   Applicable Products: This constraint is applicable to Mediant 4000 and SW E-SBC.

2. SIP-registered user database is not replicated as part of the switchover from active to redundant board

   Applicable Products: This constraint is applicable to Mediant 4000 and SW E-SBC.

3. To configure IP-to-IP inbound manipulation for SAS, the IP2IP Inbound Manipulation table used for the SBC application must be used. This table is available in the Web interface only if the SBC application is enabled and the device is installed with the SBC Feature Key.

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

6. The following new features are not supported in the Web interface and can only be configured using the corresponding *ini* file parameter:

   - SIP Calling Name Manipulations table
   - AT&T toll free out-of-band blind transfer for trunks configured with the 4ESS ISDN protocol
   - SBC Registration Time Parameters

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

7. For Mediant 800 MSBG, IP media features such as play and/or record of announcements, and conferencing are not supported.

   Applicable Products: Mediant 800 MSBG.

8. Least Cost Routing is supported only for the Gateway and IP2IP applications and will be supported for the SBC application in the next applicable release

Applicable Products: Mediant 800 MSBG, Mediant 800, Mediant 1000 MSBG, Mediant 3000, Mediant 1000B, Mediant 4000 E-SBC, Mediant Software E-SBC.

9. 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

   Applicable Products: Mediant 1000, Mediant 1000 MSBG, and Mediant 3000.

5.2 Media Constraints

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

1. Transcoding of RTP, DTMF, and fax are not supported.

   Applicable Products: Mediant 4000 and Mediant Software E-SBC.

2. The SILK coder does not support silence compression. If silence compression is enabled on calls based on the SILK coder, the device generates a Syslog warning information message.

   Applicable Products: Mediant 800 MSBG and Mediant 800.

3. When a call uses the SILK coder, fax over T.38 transport cannot be done using the same local UDP port as configured for the RTP session. A workaround is to use only the default setting for T.38 local UDP port as RTP local UDP port +2.

   Applicable Products: Mediant 800 MSBG and Mediant 800.

4. When IP-to-IP or IP-to-PSTN calls use SRTP with ARIA encryption, the number of simultaneous calls is limited to 31.

   Applicable Products: Mediant 800 MSBG and Mediant 800.

5. Dialing of RFC 4733 digits is not functioning. A workaround is to configure the device to dial transparent digits to the network instead of RFC 4733.

   Applicable Products: Mediant 800 MSBG and Mediant 800.

6. SBC RTP forwarding calls using the SRTP tunneling feature cannot monitor parameters for the QoE feature. A workaround is to use SRTP full encryption / decryption on the forwarding calls.

   Applicable Products: Mediant 1000 MSBG and Mediant 1000B.

7. SBC RTP forwarding calls using the SRTP tunneling feature cannot provide RTCP XR monitoring parameters (such as MOS) required for the QoE feature on the following variable bit rate coders: G.723, GSM FR, GSM EFR, and MS RTA. A workaround is to use SRTP full encryption / decryption on the forwarding calls.

   Applicable Products: Mediant 3000.

8. Ethernet packets received on the RTP side of SRTP-RTP SBC sessions must not exceed 1500 bytes. Packets exceeding this size are dropped.

   Applicable Products: Mediant 1000B, Mediant 1000 MSBG, Mediant 800, Mediant 800 MSBG, Mediant 3000, Mediant 4000, Mediant Software E-SBC.

9. Video sessions cannot be transported on SBC RTP forwarding calls.

   Applicable Products: Mediant 3000.

10. The Enhanced G.711 vocoder is no longer supported.

    Applicable Products: Mediant 600, Mediant 1000, Mediant 1000 MSBG, and Mediant 3000.

11. Acoustic Echo Suppression cannot be used together with Wideband transcoding. When Acoustic Echo Suppression is enabled, IP-to-IP calls using Wideband coders such as G.722 or AMR-WB do not maintain the Wideband quality and consequently, is degraded to Narrowband quality.

    Applicable Products: Mediant 3000.

12. 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.

    Applicable Products: Mediant 3000.

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

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

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

14. 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.

    Applicable Products: Mediant 3000.

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

    Applicable Products: Mediant 3000.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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

    Applicable Products: Mediant 3000.

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

    Applicable Products: Mediant 1000.

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

    Applicable Products: Mediant 1000 and Mediant 1000 MSBG.

5.3 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).

   Applicable Products: Mediant 800 MSBG, Mediant 1000, Mediant 1000 MSBG, and Mediant 3000.

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).

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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).

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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.

   Applicable Products: Mediant 3000 with TP-6310.

5.3.1 DS3 Constraints

This release includes the following known DS3 constraints:

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

   Applicable Products: Mediant 3000 with TP-6310.

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

   Applicable Products: Mediant 3000 with TP-6310.

3. The DS3 External clock is not relevant for Asynchronous mapping of DS3 in OC3. **Applicable Products:** Mediant 3000 with TP-6310.

5.3.2 SDH Constraints

This release includes the following known SDH constraints:

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

   Applicable Products: Mediant 3000 with TP-6310.

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.

   Applicable Products: Mediant 3000 with TP-6310.

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".

   Applicable Products: Mediant 3000 with TP-6310.

5.4 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).

   Applicable Products: Mediant 1000 and Mediant 1000 MSBG.

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.

   Applicable Products: Mediant 1000 and Mediant 1000 MSBG.

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

   Applicable Products: Mediant 1000 and Mediant 1000 MSBG.

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.

   Applicable Products: Mediant 1000 and Mediant 1000 MSBG.

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.

   Applicable Products: Mediant 1000 and Mediant 1000 MSBG.

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

   Applicable Products: Mediant 1000 and Mediant 1000 MSBG.

5.5 Networking Constraints

This release includes the following known networking constraints:

1. The AMC CPU should expose two MAC addresses (as appears on the printed label on the chassis) to the external network. However, only the first MAC address is exposed.

   Applicable Products: Mediant 4000.

2. Only two physical Ethernet ports are supported; any additional Ethernets ports located on the server are not recognized.

   Applicable Products: Mediant Software E-SBC.

3. When upgrading to Version 6.4, RIP remains enabled (if previously configured), but advanced RIP configuration is lost. A possible workaround is to reconfigure necessary RIP features through the CLI.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

4. When configuring the device with multiple interfaces on multiple physical port groups, all interfaces that belong to a specific subnet must connect to (and reside on) a single port group. In other words, equipment with the same MAC addresses cannot be connected to two or more different physical port groups of the device.

   Applicable Products: Mediant 800 and Mediant 1000B.

5. 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.

   Applicable Products: Mediant 1000 and Mediant 3000.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

8. Debug Recording:

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

5.6 Security Constraints

This release includes the following known security constraints:

1. VPN server configuration (i.e., PPTP/L2TP in server mode) doesn’t function; the device reboots when trying to modify setup.

   Applicable Products: Mediant 800 MSBG, Mediant 1000, and Mediant 1000 MSBG.

2. When the device is set up with a T1 WAN interface, the Web interface does not provide the option to configure cellular 3G connection as backup for the T1 WAN interface. A workaround is to use CLI to configure the cellular 3G connection.

   Applicable Products: Mediant 800 MSBG.

5.7 High Availability Constraints

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

1. The subnet of the Maintenance HA address cannot be changed during HA system runtime and requires a separate configuration and reset for each device.

   Applicable Products: Mediant 4000 and Mediant Software E-SBC.

2. Redundancy of physical Ethernet ports is not operational and thus, disconnection of the physical ports may adversely affect HA functionality. For example, disconnection of the physical port that carries the Maintenance interface will cause Active-Active state between the two E-SBCs

   Applicable Products: Mediant Software E-SBC.

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

   Applicable Products: Mediant 3000 HA with TP-6310 or TP-8410.

4. 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.

   Applicable Products: Mediant 3000 HA with TP-6310 or TP-8410.

5. 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.

   Applicable Products: Mediant 3000 HA with TP-6310.

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

   Applicable Products: Mediant 3000 HA with TP-6310 or TP-8410.

5.8 Infrastructure Constraints

This release includes the following known infrastructure constraints:

1. Core Dump to the internal flash device may take up to 4 minutes. During this period, a red alarm LED is lit.

   Applicable Products: Mediant 4000.

2. Only E&M Type V is supported (Type I, II, III, and IV are currently not supported).

   Applicable Products: Mediant 800 MSBG.

3. 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.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

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

   Applicable Products: Mediant 3000 with TP-6310.

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

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

7. 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).

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

5.9 Management Constraints

5.9.1 Web Constraints

This release includes the following known Web constraints:

1. After manual switchover in HA Revertive Mode, the Web Home page isn’t refreshed automatically. Users should manually refresh the Home page to get the updated status.

   Applicable Products: Mediant 4000.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 2000, and Mediant 3000.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

5. In the 'Network IP Settings' page, the 'Underlying Interface' drop-down list displays duplicated values (e.g., "Port 1", "Port 1"), as the Physical Port Settings table has two row entries with identical names for each LAN port-pair redundancy.

   Applicable Products: Mediant 800 and Mediant 1000B.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC

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

   Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant

1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

9. The Web pages in the Data section do not display some images when accessing the Web interface through a proxy server.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

11. Only partial help is provided in the Online Help for the Physical Ports Settings page.

    Applicable Products: Mediant 800, Mediant 1000B, and Mediant 4000.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

17. 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.

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

18. Some Web pages cannot be added to a Scenario.

    Applicable Products: Mediant 600, Mediant 1000, and Mediant 3000.

19. Web Login Authentication using Smart Cards (CAC) is not supported.

    Applicable Products: This constraint is applicable to Mediant Software E-SBC.

20. RADIUS is not supported.

    Applicable Products: This constraint is applicable to Mediant Software E-SBC.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC.

22. The SILK voice coder cannot be configured in the Web interface. To configure it, use the *ini* file.

    Applicable Products: Mediant 800 and Mediant 800 MSBG.

23. 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.

    Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, and Mediant 3000.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC, Mediant Software E-SBC.

25. 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 remains active (should be unavailable). A workaround for this constraint is not to click this button.

    Applicable Products: Mediant 600.

26. 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.

    Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

27. The horizontal scroll bar is missing in the Connection Status page (**Status & Diagnostics** tab > **Data Status** menu > **Connection Statistics**). This results in loss of some of the information at the end of the line.

    Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000.

5.9.2 SNMP Constraints

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

1. SNMP is not supported.

   Applicable Products: Mediant 4000 and Mediant Software E-SBC.

2. Incorrect indications of the DS3 interfaces in the ifTable – ifOperStatus.

   Applicable Products: Mediant 3000 with TP-6310.

3. In the acSysModuleTable, the first LAN port number on the second module should be sequential.

   Applicable Products: Mediant 800 MSBG and Mediant 800.

4. When configuring acSysInterfaceTable using SNMP or the Web interface, validation is done only after device reset.

   Applicable Products: Mediant 3000.

5. The DS3 ifAdmin-State field cannot be changed in the IF-Table, using SNMP.

   Applicable Products: Mediant 3000 with TP-6310.

6. In the DS3/E3 Current Table, the objects dsx3CurrentSEFSs and dsx3CurrentUASs are not supported.

   Applicable Products: Mediant 3000 with TP-6310.

7. In the DS3/E3 Interval Table, the following objects are not supported: dsx3IntervalPSESs and dsx3IntervalSEFSs.

   Applicable Products: Mediant 3000 with TP-6310.

8. The dsx3Total Table is not supported.

   Applicable Products: Mediant 3000 with TP-6310.

9. The Admin State does not change to “Redundant”.

   Applicable Products: Mediant 3000 HA with TP-6310 or TP-8410.

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

    Applicable Products: This constraint is applicable to Mediant 600, Mediant 800 MSBG, Mediant 800 Gateway & E-SBC, Mediant 1000, Mediant 1000 MSBG, Mediant 1000B Gateway & E-SBC, Mediant 2000, Mediant 3000, Mediant 4000 E-SBC.

5.9.3 Element Management System Constraints

This release includes the following known Element Management System (EMS) management tool constraints:

1. EMS Version 6.4 GA is not supported:

   Applicable Products: This constraint is applicable to Mediant 1000B, Mediant 800, Mediant 4000, and Mediant Software E-SBC.

5.9.4 CLI Constraints

This release includes the following known command-line interface (CLI) constraints:

1. Only the CLI commands explicitly mentioned in the *Installation Manual* are supported.

   Applicable Products: Mediant Software E-SBC.

2. 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.

   Applicable Products: Mediant 600, Mediant 1000, and Mediant 3000.

3. The NFS table cannot be configured through the CLI. A workaround is to configure it through the Web interface.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

6 Resolved Constraints in Release 6.4

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

6.1 SIP Resolved Constraints

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

1. Termination of REFER \ 3xx \ Hold \ Re-INVITE is supported only by the IP2IP application.

   Applicable Products: Mediant 800 MSBG, Mediant 1000 MSBG, Mediant 3000, Mediant 4000, Mediant SW E-SBC.

2. 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.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

6.2 Media Resolved Constraints

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

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.

   Applicable Products: Mediant 3000.

2. RTCP XR is not supported.

   Applicable Products: Mediant 800 MSBG.

6.3 Security Resolved Constraints

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

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.

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

2. The following CLI commands do not function with SHDSL-ATM interfaces:

   - show data interfaces
   - show data ip interface
   - show data qos match-map
   - show data hosts

   Applicable Products: Mediant 800 MSBG and Mediant 1000 MSBG.

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.

   Applicable Products: This resolved constraint is applicable to all devices.

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.

   Applicable Products: Mediant 1000 MSBG and Mediant 3000.

6.4 Web Resolved Constraints

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

1. 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.

   Applicable Products: This constraint was applicable to all devices.

2. When only the digital module is assembled in the chassis, the Web interface's Home page also displays the analog legend describing the icon color-codes.

   Applicable Products: Mediant 600.

.

Reader’s Notes

.

SIP Release Notes
Release 6.4, Version 13.5

www.audiocodes.com