Enterprise Session Border Controllers (E-SBC)

Multi-Service Business Routers (MSBR)

VoIP Analog & Digital Media Gateways

Release Notes

SAS
Stand Alone Survivability
Continuous VoIP Service

HD VoIP
Sounds Better

SBC

Version 6.6

AudioCodes

Table of Contents

List of Tables

Notice

This document describes the new features of Release 6.6 for AudioCodes SIP-based Voice-over-IP (VoIP) Analog & Digital Media Gateways, Enterprise Session Border Controllers (E-SBC), and Multi-Service Business Routers (MSBR) products.

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.

Date Published: June-06-2016

Trademarks

WEEE EU Directive

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

Customer Support

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

Abbreviations and Terminology

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

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

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at http://www.audiocodes.com/downloads.

Related Documentation

Document Name
MP-11x and MP-124 SIP Installation Manual
MP-11x SIP Fast Track Guide
MP-124 AC SIP Fast Track Guide
MP-124 DC SIP Fast Track Guide
MP-11x and MP-124 SIP User's Manual
Mediant 500 MSBR Installation Manual
Mediant 500 MSBR User's Manual
Mediant 600 Installation Manual
Mediant 800 MSBR Installation Manual
Mediant 800 MSBR User's Manual
Mediant 800 Gateway and E-SBC Installation Manual
Mediant 800 Gateway and E-SBC User's Manual
Mediant 850 MSBR Installation Manual
Mediant 850 MSBR User's Manual
Mediant 1000 SIP Installation Manual
Mediant 600 & Mediant 1000 SIP User's Manual
Mediant 1000B MSBR SIP Installation Manual
Mediant 1000B MSBR SIP User's Manual
Mediant 1000B Gateway and E-SBC SIP Installation Manual
Mediant 1000B Gateway and E-SBC SIP User's Manual
Mediant 2000 SIP Installation Manual
Mediant 2000 SIP User's Manual
Mediant 3000 SIP Installation Manual
Mediant 3000 SIP User's Manual
Mediant 2600 E-SBC Installation Manual
Mediant 2600 E-SBC User's Manual
Mediant 4000 E-SBC Installation Manual
Mediant 4000 E-SBC User's Manual
Mediant Software E-SBC Server Edition Installation Manual
Mediant Software E-SBC Virtual Edition Installation Manual
Mediant Software E-SBC User's Manual
MSBR Series CLI Reference Guide for System and VoIP Functionalities
MSBR Series CLI Reference Guide for Data Functionality

1 Introduction

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

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 the MSBR product family, open source software may have been added and/or amended for this product. For further information, visit AudioCodes 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.
- Release 6.6 no longer supports Mediant 500 MSBR, Mediant 800 Family Series, Mediant 1000B; Mediant 3000, Mediant 2600, Mediant 4000, Mediant Software. Release 6.8 and later should be used for these products.

1.1 Released Software Revision Record

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

Table 1-1: Released Software Revision Record

Software Version	Date
General Availability (GA)	December 2012
6.60A.312.003	December 2015
6.60A.314.004	December 2015
6.60A.317.001	January 2016
6.60A.319.003	February 2016
6.60A.322	May 2016
6.60A.323.005	June 2016

1.2 Products Supported in Version 6.6

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

1.2.1 MediaPack 1xx

This release supports the following existing hardware platforms:

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

Note: See section 2.1 on page 27 for the new MP-124 hardware revision, MP-124 Rev. E.

1.2.2 Mediant 600

Mediant 600 continues to be supported.

1.2.2.1 New Hardware

This release introduces no new hardware configurations for Mediant 600.

1.2.2.2 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 BRI ports)
- Up to 2 FXS modules (where each module provides 4 FXS ports)
- Up to 2 FXO modules (where each module provides 4 FXO ports)

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

1.2.3 Mediant 800 MSBR

Mediant 800 MSBR continues to be supported.

1.2.3.1 New Hardware

This release introduces the following new hardware feature:

- (Optional, customer-ordered) Wireless LAN 802.11n (Wi-Fi) access point at 2.4 and 5 GHz, integrated 3 Tx / 3 Rx, enabling data rates of up to 300 Mbps. The Wi-Fi interface also supports 802.11b/802.11g backward compatibility, allowing interoperability of multiple devices with different types of Wi-Fi.

1.2.3.2 Existing Hardware

This release supports the following existing hardware:

- Optional, single E1/T1 telephony port (over single copper wire pair)
- Up to 8 BRI ports (supporting up to 16 voice channels)
- Up to 12 FXS ports
- Up to 12 FXO ports
- 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).
  - ADSL / VDSL interface (RJ-45 port):
    - ATM (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
    - EFM (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

- 1 x Symmetric High-Speed Digital Subscriber Line (SHDSL) WAN port, providing up to 4 SHDSL wire-pairs housed on a single RJ-45 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
- 3G Cellular WAN access (primary or backup) using a USB modem. The following 3G cellular USB modems are currently supported:
  - ZTE MF626
  - ZTE MF637
  - Alcatel X220
  - Huawei E182E
  - Huawei E173
  - Huawei E160
  - Sierra Wireless AirCard 308

- Power over Ethernet (PoE) supported on all LAN ports, complying with IEEE 802.3af-2003. Various power budgets (120 and 50 Watt) are supported for PoE on the LAN ports.
- OSN server platform for hosting third-party applications (such as an IP PBX). The following OSN server platforms are available (depending on configuration):
  - OSN1: Intel® Atom™ 1.6 GHz processor, with 1GB or 2GB RAM (depending on Mediant 800 model) and a single storage hard disk drive (SATA storage)
  - OSN2: Intel® Celeron® 847E (2x 1.1 GHz), 2 MB L2 Cache, Intel® HM65 Second Generation
- 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).

Note: For available hardware configuration models, contact your AudioCodes sales representative.

1.2.4 Mediant 800 Gateway & E-SBC

Mediant 800 Gateway & E-SBC continues to be supported.

1.2.4.1 New Hardware

This release introduces the following new hardware configuration:

- 2 x E1/T1 PRI port interfaces

1.2.4.2 Existing Hardware

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 ports
- Up to 2 E1/T1 PSTN ports (over single copper wire pair)
- Up to 8 BRI ports (supporting up to 16 voice channels)
- Up to 12 FXS ports
- Up to 8 FXO ports

The Mediant 800 also offers up to 12 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 an IP PBX.

Note: For available hardware configuration models, contact your AudioCodes sales representative.

1.2.5 Mediant 1000

Mediant 1000 continues to be supported.

1.2.5.1 New Hardware

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

1.2.5.2 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 ports)
- Up to 6 FXO modules (where each module provides 4 FXO ports)
- 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.

1.2.6 Mediant 1000B MSBR

Mediant 1000B MSBR continues to be supported.

1.2.6.1 New Hardware

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

1.2.6.2 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 ports)
- Up to 6 FXO modules (where each module provides 4 FXO ports)
- 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-SD: SHDSL port (providing 4 SHDSL wire-pairs 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 (OSN3) for hosting third-party applications (such as an IP PBX). This includes Intel® Core™ 2 Duo 1.5 GHz processors L7400 with Intel 3100 Chipset (64-bit).
- Chassis - 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 MSBR data-routing functionalities.

1.2.7 Mediant 1000B Gateway & E-SBC

Mediant 1000B Gateway & E-SBC continues to be supported.

1.2.7.1 New Hardware

This release introduces no new hardware configurations for Mediant 1000B Gateway & E-SBC.

1.2.7.2 Existing Hardware

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 digital 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 an IP PBX.

1.2.8 Mediant 2000

Mediant 2000 continues to be supported.

1.2.8.1 New Hardware

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

1.2.8.2 Existing Hardware

This release supports the following existing hardware:

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

1.2.9 Mediant 3000

Mediant 3000 continues to be supported.

1.2.9.1 New Hardware

No new hardware has been introduced in this release for Mediant 3000.

1.2.9.2 Existing Hardware

This release supports the following existing hardware:

- Configurations hosting TP-6310 blade:
  - 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.
  - 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)
- Configurations hosting TP-8410 blade:
  - 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).

1.2.10 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).

1.2.10.1 New Hardware

This release introduces the following new hardware:

- Optional, Media Processing module (MPM), providing additional DSP resources for transcoding sessions

1.2.10.2 Existing Hardware

This release supports the following existing hardware:

- Modular, 1U chassis.
- A single AudioCodes Full-Height AMC module running the 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

- 1+1 power load-sharing and redundancy using two Power Supply modules
- 1+1 High Availability using two Mediant 4000 devices

1.2.11 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' 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.

Mediant Software E-SBC is available in the following editions:

- **Server Edition** - x86 server based platform. The Server Edition must be installed on a server with the following hardware requirements:
  - Platform: HP ProLiant DL120 G7 or HP ProLiant DL320e G8
  - Processor: Intel Xeon E3-1220 or E3-1220v2 (4 cores, 3.1 GHz, 8M Cache)
  - Memory: 4 GB
  - Disk space: 72 GB or more
  - Installation from CD/DVD drive
  - Installation interface: VGA Monitor and Keyboard
- **Virtual Edition** - installed and hosted in a virtual machine environment. The Mediant Software E-SBC Virtual Edition can be installed on a VMware ESXi host, with sufficient available resources, running version 5.0 or later:
  - Host OS: VMware ESXi version 5.0 or later
  - Processor: 2 Cores or more.
  - Memory: 4 GB or more
  - Disk space: 60 GB or more
  - Network: At least two virtual networks preconfigured

Notes:

- When upgrading from Version 6.4 to 6.6 using the Web interface, the Software Upgrade Wizard is not supported. Customers should back up the current configuration (ini file), install the new 6.6 version from the installation CD, and then restore configuration.
- Customers who upgrade to Version 6.6 need a new Software License Key. Refer to the *Installation Manual* on how to obtain the new Software License Key.

1.3 Document Revision Record Table

Features that were added after the initial publication of this document series are listed in the table below:

Table 1-2: Document Revision Record

Feature	Section	LTRT
Patch Release 6.60A.323.005	Section 6.7	26966
Channel capacity update for MP-124 Rev. E	Section 4.2 on page 130	26962
Patch Release 6.60A.322	-	26961
Resolved Constraints for Version 6.60A.319.003	-	26951
New Product variant MP-124 Rev. E	Section 2.1 on page 27	26951
Constraints and New Features for Version 6.60A.317.001	-	26947
Constraints Version 6.60A.312.003 and 6.60A.314.004	-	26942
Update to Mediant 8xx DSP templates	Section 4.4 on page 132	26916
ISO 8859 Character Set Type	Section 3.1.2.47 on page 71	26915
Mediant 2600 E-SBC	Section 2.4 on page 28	26913
Mediant 2600 E-SBC	Section 4.8 on page 144	26913
Intrusion Detection System	Section 3.1.1.1 on page 29	26912
Configurable User Information Table via CLI	Section 3.1.1.2 on page 30	26912
Mediant 500 MSBR	Section 2.2 on page 27	26911
Remote Trigger of Automatic Update or Reset using SIP NOTIFY	Section 3.1.1.3 on page 32	26911
Increase in Maximum Record-Route Headers in INVITE / 200 OK	Section 3.1.1.4 on page 32	26911
SRTP State Reset for Session Refresh upon New Key	Section 3.1.1.5 on page 33	26911
TCP Keep-Alive per SIP Interface	Section 3.1.1.6 on page 33	26911
Call Disconnect upon User-Defined Session Expiry	Section 3.1.1.7 on page 34	26911
Accept CANCEL Requests Received after 200 OK	Section 3.1.1.8 on page 34	26911
Reject SIP Requests with Different User in Request-URI and Previous Contact	Section 3.1.1.9 on page 35	26911
Testing SIP Calls	Section 3.1.1.10 on page 35	26911
Filtering Syslog Messages and Debug Recordings	Section 3.1.1.11 on page 37	26911
ENUM Domain Name as FQDN and NRENum Support	Section 3.1.1.12 on page 39	26911
V.150.1 SDP Format	Section 3.1.2.1 on page 49	26911
Double Wink-Start Signaling and Polarity Reversal	Section 3.1.2.2 on page 49	26911
Increase in Maximum SIP Calling Name Manipulation Rules	Section 3.1.2.3 on page 50	26911

Feature	Section	LTRT
Simultaneous Negotiation of Fax (T.38) and Modem (V.150.1) Relay CED Tone	Section 3.1.2.4 on page 50	26911
Different RTP Ports for Held and New Call by FXS Endpoint	Section 3.1.2.5 on page 51	26911
Interworking User-to-User Header with Text Format to UUIE IA5 Characters in Q.931 Messages	Section 3.1.2.6 on page 52	26911
New Format for re-INVITE for Call Hold	Section 3.1.2.7 on page 52	26911
Disconnect IP-to-Tel Call upon Answer Machine Detection	Section 3.1.2.8 on page 53	26911
Calling Name Retrieval from AD using LDAP Query	Section 3.1.2.9 on page 53	26911
SAS Emergency upon OPTIONS Only Response Failure	Section 3.1.3.1 on page 72	26911
Increase in Number of Maximum Transcoding Sessions	Section 3.1.4.1 on page 73	26911
User Registration Time per IP Profile	Section 3.1.4.2 on page 73	26911
Interworking DTMF Payload Type for RFC 2833	Section 3.1.4.3 on page 74	26911
Removing 'gop' parameter in SBC Authentication Challenge	Section 3.1.4.4 on page 74	26911
Media (RTP) Normalization	Section 3.1.4.5 on page 75	26911
Increase in Maximum Number of SBC IP-to-IP Routing Rules	Section 3.1.4.6 on page 75	26911
Increase in Maximum Number of Classification Rules	Section 3.1.4.7 on page 75	26911
SIP Response Code for Unclassified Calls	Section 3.1.4.8 on page 75	26911
Call Forking to Available Contacts Only	Section 3.1.4.9 on page 76	26911
Call Forking of Specific Contact to all Contacts under AoR	Section 3.1.4.10 on page 76	26911
Termination of REGISTER for Shared Lines	Section 3.1.4.11 on page 76	26911
Interworking Call Hold and Retrieve Requests	Section 3.1.4.12 on page 77	26911
Cloud Resilience Package Application	Section 3.1.5.1 on page 89	26911
Multiple IP Interfaces per VLAN	Section 3.1.7.1 on page 95	26911
DHCP Server Options	Section 3.1.8.1 on page 99	26911
DHCP Client Option 121	Section 3.1.8.2 on page 99	26911
Monitoring IP Entity and HA Switchover upon Ping Failure	Section 3.1.10.1 on page 103	26911
Redundant Device Display on Web Home Page of Active Unit	Section 3.1.10.2 on page 104	26911
B-Channel Restart	Section 3.1.11.1 on page 104	26911
FXS Line Testing	Section 3.1.12.1 on page 106	26911
Zero Configuration using AudioCodes HTTPS Redirect Server	Section 3.1.13.1 on page 107	26911

Feature	Section	LTRT
Automatic Update using Zero Configuration Certificate	Section 3.1.13.2 on page 108	26911
Automatic Update using CLI Scripts	Section 3.1.13.3 on page 109	26911
Automatic Update through WAN Interface	Section 3.1.13.4 on page 109	26911
Configuration of Automatic Update using CLI	Section 3.1.13.5 on page 109	26911
Web Access from Any Interface	Section **3.1.14.1** on page 110	26911
Clear History Alarms Table	Section 3.1.14.2 on page 110	26911
Quality of Service using MIBs	Section 3.1.15.1 on page 114	26911
Information on Physical Configuration	Section 3.1.15.2 on page 114	26911
New show Commands	Section 3.1.16.1 on page 117	26911
Show VoIP DSP Status Commands	Section 3.1.16.2 on page 118	26911
Auto-Configuration Server Discovery via DHCP	Section 3.1.17.1 on page 121	26911
TR-104 Support	Section 3.1.17.2 on page 121	26911

1.4 Product Naming Conventions

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

- **MP-1xx:**
  - MP-112
  - MP-114
  - MP-118
  - MP-124
- **Mediant 8xx Series:**
  - Mediant 800 MSBR
  - Mediant 800 Gateway & E-SBC
  - Mediant 850 MSBR
- **Mediant 1000 Series:**
  - Mediant 1000
  - Mediant 1000B MSBR
  - Mediant 1000B Gateway & E-SBC
- **MSBR Series:**
  - Mediant 500 MSBR
  - Mediant 800 MSBR
  - Mediant 850 MSBR
  - Mediant 1000B MSBR
- **E-SBC Series:**
  - Mediant 500 MSBR
  - Mediant 800 MSBR
  - Mediant 800 Gateway & E-SBC
  - Mediant 850 MSBR
  - Mediant 1000B MSBR
  - Mediant 1000B Gateway & E-SBC
  - Mediant 2600 E-SBC
  - Mediant 3000
  - Mediant 4000 E-SBC
  - Mediant Software E-SBC

This page is intentionally left blank.

2 New Products

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

2.1 MP-124 Rev. E

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

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

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

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

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

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

2.2 Mediant 500 MSBR

The Mediant 500 MSBR is based on the incumbent Mediant 800 MSBR, and provides the following interfaces:

- Multiple WAN:
  - 1 x Gigabit Ethernet copper (10/100/1000Base-T) unshielded twisted pair (UTP) interface port (RJ-45)
  - Dual-mode Optical Fiber Small Form-Factor Pluggable (SFP), supporting 100 Mbps and 1000 Mbps Ethernet (available with optional software license)
  - ADSL2+ / VDSL2 (RJ-11 port interfaces)
  - 3G Cellular WAN access (primary or backup) using a USB modem
- Four Gigabit Ethernet (10/100/1000Base-T) LAN ports (RJ-45)
- (Optional, customer-ordered) Wireless LAN 802.11n (Wi-Fi) access point at 2.4 and 5 GHz, integrated 2 Tx / 2 Rx, enabling data rates of up to 300 Mbps. Two Wi-Fi antennas. The Wi-Fi interface also supports 802.11b/802.11g backward compatibility, allowing interoperability of multiple devices with different types of Wi-Fi.
- Two USB ports for an optional, 3G cellular WAN modem and/or USB storage services
- Serial console port (RJ-45) for device management
- (Optional, customer-ordered) Two BRI ports (RJ-45), supporting up to 4 voice channels as well as PSTN fallback

Note: For available hardware configurations, please consult with your AudioCodes sales representative.

2.3 Mediant 850 MSBR

The Mediant 850 MSBR is based on the incumbent Mediant 800 MSBR, but with the following additional support:

- 2 x USB interface ports
- RJ-45 serial connector
- Optional, Power Over Ethernet (PoE) per the IEEE 802.3at standard
- Optional, dual E1/T1 PRI spans
- (Optional, customer-ordered) Wireless LAN 802.11n (Wi-Fi) access point at 2.4 and 5 GHz, integrated 3 Tx / 3 Rx, enabling data rates of up to 300 Mbps. The Wi-Fi interface also supports 802.11b/802.11g backward compatibility, allowing interoperability of multiple devices with different types of Wi-Fi.
- Multiple WAN interfaces that include an integrated Gigabit Ethernet (GE) Unshielded Twisted Pair (UTP) interface port, and a combination of any one or two ports of the following interfaces (factory assembled option):
  - GE UTP
  - Optical Fiber SFP form factor, supporting 100 Mbps and 1000 Mbps Ethernet
  - ADSL2+ / VDSL2 (RJ-11 port interfaces)
  - SHDSL, supporting up to four wire-pairs (provided by two RJ-11 port interfaces)

Note: For available hardware configurations, please consult with your AudioCodes sales representative.

2.4 Mediant 2600 E-SBC

The Mediant 2600 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). Designed for medium-sized deployments with high performance demands, the Mediant 2600 E-SBC scales up to 600 concurrent SBC VoIP sessions.

- Modular, 1U chassis.
- A single AudioCodes Full-Height AMC module running the 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
- (Optional) Media Processing module (MPM), providing additional DSP resources for transcoding sessions
- 1+1 power load-sharing and redundancy using two Power Supply modules
- 1+1 High Availability using two Mediant 4000 devices

3 New Features

This section describes the new software features introduced in Release 6.6.

3.1 Version GA

This section lists new features introduced in the GA version.

3.1.1 SIP General Features

This subsection describes the new general SIP features.

3.1.1.1 Intrusion Detection System

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

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

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

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

To support this feature, the following parameters were added:

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

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

Applicable Products: Mediant 500; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.1.2 Configurable User Information Table via CLI

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

This database is used for the following applications:

- Gateway application: maps PBX extensions connected to the device to "global" IP numbers, and registers each PBX user to an external registrar server
- SBC application:
  - Registers to an external registrar server on behalf of a specific user
  - Authenticates (for any SIP request and as a client) on behalf of a specific user if challenged by an external server
  - Authenticates (as a server) incoming user requests

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

- Gateway application:

  `gw-user-info`

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

- SBC application:

  ```
  sbc-user-info
  ```

  Includes the following parameters:

  - **local-user:** Identifies the user and is used as the URI user part for the AOR in the database
  - **ip-group-id:** IP Group ID to which the user belongs and is used as the URI source host part for the AOR in the database
  - **username:** Authentication username (e.g., user405)
  - **password:** Authentication password (hidden for security)
  - **status:** Registration status ("registered" or "not-registered")

The path to these tables is as follows:

```
# configure voip
(config-voip)# sip-definition proxy-and-registration
(sip-def-proxy-and-reg)# user-info <gw-user-info | sbc-user-info>
```

The following commands can be used:

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

```
(sip-def-proxy-and-reg)# user-info gw-user-info display
---- gw-user-info-0 ----
  pbx-ext (405)
  global-phone-num (405)
  display-name (Ext405)
  username (user405)
  password (0aGzoKfh5uI=)
  status (not-resgistered)
---- gw-user-info-1 ----
  pbx-ext (406)
  global-phone-num (406)
  display-name (Ext406)
  username (user406)
  password (0KCwoaDg5eA=)
  status (not-resgistered)
```

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

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

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

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

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

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

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

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

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

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

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

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

Applicable Products: All.

3.1.1.3 Remote Trigger of Automatic Update or Reset using SIP NOTIFY

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

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

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=false
```

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

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

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

Applicable Products: All.

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

This feature provides support for an increase in the maximum number of supported SIP Record-Route headers to 20 that can be received in SIP INVITE requests or 200 OK responses. If the device receives an INVITE containing more than 20 Record-Route

headers, it responds with a 513 Message Too Large response, indicating that the message is too large for processing.

Applicable Products: All.

3.1.1.5 SRTP State Reset for Session Refresh upon New Key

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

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

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

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

CLI: srtp-state-behavior-mode [ResetSRTPStateUponRekey]	Enables the resetting of the SRTP state (such as ROC) when a new session key is generated due to a session expires. ▪ [0] Disable (default) = ROC is not reset. ▪ [1] Enable = ROC index used on the device side is reset and thereby, synchronized with the ROC on the server side (e.g., Lync) whenever a new session key is generated.
IP Profile Table	This feature can also be configured for an IP Profile, using the following parameter: IpProfile_SRTPStateBehaviorMode: ▪ [0] Default ▪ [1] Lync

Applicable Products: All.

3.1.1.6 TCP Keep-Alive per SIP Interface

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

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

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

SIP Interface Table - TCP Keepalive Enable [SIPInterface_TCPKeepAliveEnable]	Enables the TCP Keep-Alive feature per SIP Interface: ▪ [0] No (default) ▪ [1] Yes
TCP Keep Alive Idle Time [TCPKeepAliveTime]	Defines the interval (in sec) between the last data packet sent and the first keep-alive probe to send. The valid value is 10 to 65,000. The default is 60. Note: Simple ACKs such as keep-alives are not

	considered data packets.
TCP Keep Alive Interval Time [TCPKeepAliveInterval]	Defines the interval (in sec) between consecutive keep-alive probes, regardless of what the connection has exchanged in the meantime. The valid value is 10 to 65,000. The default is 10.
TCP Keep Alive Retry Number [TCPKeepAliveRetry]	Defines the number of unacknowledged keep-alive probes to send before considering the connection down. The valid value is 1 to 100. The default is 5.

Applicable Products: All.

3.1.1.7 Call Disconnect upon User-Defined Session Expiry

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

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

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

Applicable Products: All.

3.1.1.8 Accept CANCEL Requests Received after 200 OK

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

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

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

Applicable Products: All.

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

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

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

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

Applicable Products: All.

3.1.1.10 Testing SIP Calls

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

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

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

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

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

Test Call ID CLI: testcall-id [TestCallID]	Defines the prefix number of the simulated test endpoint. All incoming calls with this called (destination) prefix number is identified as a test call and sent to the simulated endpoint. This can be any string. The default is not configured.
SBC Test ID CLI: sbc-test-id [SBCtestID]	Defines the prefix number of the called number for identifying the incoming call as an SBC test call. The device removes this prefix, enabling it to route the call according to the IP-to-IP Routing rules to an external proxy/registrar, instead of directly to the simulated test endpoint. Only when the device receives the call from the proxy/registrar, does it route the call to the simulated test endpoint. This can be any string. The default is not configured. Note: This is applicable only to the SBC application.
Test Call Table CLI: test-endpoint	Defines the local and remote test endpoints that you want to test.

[Test_Call]	[Test_Call] FORMAT Test_Call_Index = Test_Call_EndpointURI, Test_Call_CalledURI, Test_Call_RouteBy, Test_Call_IPGroupID, Test_Call_DestAddress, Test_Call_DestTransportType, Test_Call_SRD, Test_Call_ApplicationType, Test_Call_AutoRegister, Test_Call_UserName, Test_Call_Password, Test_Call_CallParty, Test_Call_MaxChannels, Test_Call_CallDuration, Test_Call_CallsPerSecond, Test_Call_TestMode, Test_Call_TestDuration, Test_Call_Play, Test_Call_ScheduleInterval; [\Test_Call] Where: ▪ EndpointURI = Endpoint's URI (string; default is empty) ▪ CalledURI = Called URI (string; default is empty). ▪ RouteBy = Type of routing method: ✓ [0] GW Tel2IP = (Default) Calls are matched by (or routed to) an SRD and Application type (defined in the SRD and Application Type parameters below). ✓ [1] IP Group = Calls are matched by (or routed to) an IP Group ID. ✓ [2] Dest Address = Calls are matched by (or routed to) an SRD and application type. ▪ IPGroupID = IP Group ID (default is empty) ▪ DestType = Destination type: ✓ [0] Tel2IP (default) ✓ [1] IP Group ✓ [2] IP address ▪ DestAddress = Destination address (string; default is empty). ▪ DestTransportType = Destination transport type: ✓ [-1] Not configured (default) ✓ [0] UDP ✓ [1] TCP ✓ [2] TLS ▪ SRD = SRD ID (default is 0). ▪ ApplicationType = Application type: ✓ [0] GW & IP2IP (default) ✓ [2] SBC ▪ AutoRegister = Enables automatic registration: ✓ [0] Disable (default) ✓ [1] Enable ▪ UserName = Authentication username (string; default is empty) ▪ Password = Authentication password (string; default is empty ▪ CallParty = Defines the call party: ✓ [0] Caller (default) ✓ [1] Called ▪ MaxChannels = Maximum number of concurrent channels for the session. ▪ CallDuration = Call duration (in seconds). ▪ CallsPerSecond = Number of calls per second. ▪ TestMode = Defines the test session mode: ✓ [0] Once = (Default) The test runs until the lowest value between the following is reached: - Maximum channels is reached for the test session,

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

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

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

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

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

Where:

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

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

The table is accessed from:

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

Parameters are accessed from:

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

and

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

Applicable Products: All.

3.1.1.11 Filtering Syslog Messages and Debug Recordings

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

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

- Any – no filtering (all are sent)
- Specific Trunk Group (applicable only to the Gateway/IP-to-IP application)
- Specific Trunk (applicable only to the Gateway application)
- Specific Trunk/B-channel (applicable only to the Gateway application)
- Specific FXS and FXO port (applicable only to the Gateway application)
- Specific Tel-to-IP routing rule listed in the Outbound IP Routing table (applicable only to the Gateway/IP-to-IP application)
- Specific IP-to-Tel routing rule listed in the Inbound IP Routing table (applicable only to the Gateway/IP-to-IP application)
- Specific IP Group
- Specific SRD
- Specific Classification rule (applicable only to SBC application)
- Specific IP-to-IP routing rule listed in the IP-to-IP Routing table (applicable only to the SBC and SAS applications)
- Specific user, defined by username or user@host
- IP trace - records any IP stream, for example, HTTP (that isn't associated with media RTP/RTCP for MP-1xx, Mediant 600/1000, Mediant 2000 and Mediant 3000), according to destination and/or source IP address or port and Layer-4 protocol (UDP, TCP or any other IP type as defined by http://www.iana.com). When this option is selected, only the 'Value' field is applicable, supporting the following Wireshark-like expression fields:
  - ip.src / ip.dst: source and destination IP address
  - ip.addr: up to two IP addresses can be entered
  - ip.proto: IP protocol type (PDU) - enum (e.g., 1 is ICMP, 6 is TCP, 17 is UDP)
  - udp / tcp / icmp / sip / ldap / http / https: single expressions of protocol type
  - udp.port / tcp.port: transport layer
  - udp.srcport / tcp.srcport: transport layer for source port
  - udp.dstport / tcp.dstport: transport layer for destination port
  - and / && / == / < / >: between expressions

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

DR can be filtered using the following criteria:

- None (default)
- Signaling – contains all information related to signaling such as SIP signaling messages, Syslog, and CDR
- Signaling and media (RTP/RTCP/T.38)
- Signaling, media, and PCM - voice signals from and to TDM
- PSTN (ISDN and CAS) traces - applicable only for Trunk-related filters

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

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

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

Applicable Products: All.

3.1.1.12 ENUM Domain Name as FQDN and NRENum Support

This feature provides the following support:

- Configuring the ENUM domain name as any FQDN (e.g., e164.customer.net). Up until this release, the ENUM domain name could be configured only as an e164.arpa domain name (e.g., 3.0.1.9.5.8.9.1.6.3.e164.arpa).
- Support for the NRENum.net (www.nrenum.net) ENUM service (in addition to the already supported e164.arpa ENUM service). NRENum.net is an ENUM service for academia that uses a private dialing plan. NRENum.net provides countries, where the Golden ENUM Tree is unavailable, with the possibility to publish ENUM data. The NRENum.net tree is queried by the participating partners if no ENUM data is found in the Golden Tree. Countries that already have access to the Golden Tree cannot get a delegation in NRENum.net. As soon as the Golden Tree is available in a country, e164.arpa is used and the delegation in NRENum.net is then revoked

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

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

Applicable Products: MP-1xx; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series.

3.1.1.13 Debug Recording Destination Configuration and Activation

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

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

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

Applicable Products: All.

3.1.1.14 New CDR Fields for Call Termination Reasons

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

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

- SipTermReason – SIP termination reason. Possible values can include the SIP methods BYE or CANCEL, or SIP response codes such as 404.
- SipTermDesc – Description of SIP termination reason:
  - SIP reason header if exists, for example: SIP ;cause=200 ;text="Call completed elsewhere".
  - If no SIP Reason header exists, the description is taken from the reason text if exists, of the SIP response code, for example, "417 Unknown Resource-Priority".
  - If no reason text exists in the SIP response code, the description is taken from an internal SIP response mapping mechanism. For example, if the device receives a SIP response "422", it sends in the CDR "422 Session Interval Too Small method" as the description.
- PstnTermReason – Q.850 protocol termination reason. Possible values are 0-127.

This feature is application to the SBC and Gateway application.

Applicable Products: All.

3.1.1.15 Unique Session ID per Call Session for Syslog and DR

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

- Gateway application: A call session is considered either as a Tel-to-IP leg or an IP-to-Tel leg, where each leg is assigned a unique SID.
- SBC application: A session is considered as both the outgoing and incoming legs, where both legs share the same SID.

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

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

Applicable Products: All.

3.1.1.16 CDR Filtering of Debug Recordings with Wireshark Plugin

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

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

Applicable Products: All.

3.1.1.17 Reporting IP Address in CDRs of SIP UAs behind NAT

This feature provides support for reporting the IP address of SIP User Agents (UA) located behind NAT, in SIP PUBLISH messages for CDRs. During SIP signaling negotiation between the device and the SIP UA, the SIP UA provides its media IP address. However, in scenarios where the SIP UA is located behind NAT, this IP address is not the SIP UA's source media IP address. Up until this release, the device reported this "incorrect" IP address in the PUBLISH message for CDRs (and RTCP XR). The SIP UAs media IP address is acquired only upon receipt of the first incoming RTP packet, where the device "latches" on to the RTP media and "discovers" the IP address of the SIP UA. From this point on, the device publishes CDRs with this "updated" IP address instead of the NAT device's IP address.

Applicable Products: Mediant 3000.

3.1.1.18 Local LDAP Cache for LDAP Query Results

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

The benefits of this feature include the following:

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

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

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.1.19 LDAP Query of Multiple Subtrees (DNs)

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.1.20 Multiple IP Addresses for LDAP Server using FQDN

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.1.21 Deriving Call IP Destination from Dial Plan File

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

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

- For the SBC application, a new option, [5] Dial Plan has been added to the 'Destination Type' field of the SBC IP-to-IP Routing table to support this feature. The 'Destination Address' field is then used to specify the Dial Plan index, where "0" denotes [PLAN1], "1" denotes [PLAN2], and so on.
- For the Gateway/IP-to-IP application (Tel-to-IP calls), the 'Destination Address' field in the Outbound IP Routing table is used to specify the Dial Plan index instead of the IP address. The entered value is a string (case-sensitive) in the format "DialPlan<index>", where "DialPlan0" denotes [PLAN1] in the Dial Plan file, "DialPlan1" denotes [PLAN2], and so on.

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

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

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

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

Applicable Products: All.

3.1.1.22 Speex Voice Codec Support

This feature provides support for the Speex voice coder. Speex is a patent-free audio compression format designed for speech and also a free software speech codec that is targeted for VoIP applications and podcasts. It is based on the CELP speech coding algorithm. Speex claims to be free of any patent restrictions and is licensed under the revised (3-clause) BSD license. It may be used with the Ogg container format or directly transmitted over UDP/RTP.

The Speex codec is designed to optimize high quality speech and low bit rate. To achieve this, the codec uses multiple bit rates and supports wideband (16-kHz sampling rate) and narrowband (telephone quality, 8-kHz sampling rate). Since Speex was designed for VoIP, the codec must be robust to lost packets, but not to corrupted ones. All this led to the choice of Code Excited Linear Prediction (CELP) as the encoding technique for Speex.

Two new options, 'Speex NB' and 'Speex WB' have been added to the Coders table and Coder Group Settings table to support this feature:

<table>
<tr><td rowspan="4">Coders Table / Coder Group Settings
CLI: config voip > coders-and-profiles coders-group [CodersGroupX]</td><td colspan="5">Defines groups of coders, where x denotes the group index from 0 to 9. Up to 10 groups of coders can be defined, where each group can include up to 10 coders.</td></tr>
<tr><td>Coder</td><td>Ptime (msec)</td><td>Rate (kbps)</td><td>Payload Type</td><td>Silence Suppression</td></tr>
<tr><td>speex_nb</td><td>20</td><td>2.15 (default); 5.95; 8; 11; 15; 18.2; 24.6; 3.95</td><td>78</td><td>-</td></tr>
<tr><td>speex_wb</td><td>20</td><td>3.95 (default); 5.75; 7.75; 9.8; 12.8; 16.8; 20.6; 23.8; 27.8; 34.2; 42.2</td><td>78</td><td>-</td></tr>
<tr><td>Web: Speex NB Bit Rate
[SpeexNBBitRate]</td><td colspan="5">Defines the transmit (Tx) bit rate for the Speex narrowband codec at clock rate of 8 kHz sampling rate.
▪ [1] 2.15 Kbps
▪ [2] 5.95 Kbps
▪ [3] 8.00 Kbps (default)
▪ [4] 10.0 Kbps
▪ [5] 15.0 Kbps
▪ [6] 18.2 Kbps
▪ [7] 24.6 Kbps
▪ [8] 3.95 Kbps</td></tr>
<tr><td>Web: Speex NB Bit Rate
[SpeexNBBitRate]</td><td colspan="5">Defines the transmit (Tx) bit rate for the Speex narrowband codec at clock rate of 8 kHz sampling rate.
▪ [1] 2.15 Kbps
▪ [2] 5.95 Kbps
▪ [3] 8.00 Kbps (default)
▪ [4] 10.0 Kbps
▪ [5] 15.0 Kbps
▪ [6] 18.2 Kbps
▪ [7] 24.6 Kbps
▪ [8] 3.95 Kbps</td></tr>
</table>

Applicable Products: Mediant 3000.

3.1.1.23 Increase in Maximum Number of Coder Groups

This feature provides support for an increase in the maximum number of Coder Groups from 4 to 10 that can be configured. The Coder Groups are configured in the Coder Group Settings table. This also affects other features that use the Coder Group Settings table such as the IP Profile table (SBCExtensionCodersGroupID, CodersGroupID, SBCAllowedCodersGroupID, and SBCFaxCodersGroupID parameters).

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000.

3.1.1.24 Proxy IP Address as Host Name in REGISTER Requests

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

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

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

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

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

Applicable Products: All.

3.1.1.25 SIP Header Manipulations using Regular Expressions

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

This feature provides the following main benefits:

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.1.26 Manipulation based on Source/Destination Address of SIP Message

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

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

Applicable Products: All.

3.1.1.27 Manipulation of Port and IP Address in SDP

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

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

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

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

Applicable Products: All.

3.1.1.28 Empty Prefix as Matching Criteria for Routing and Manipulation

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

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

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

Applicable Products: All.

3.1.1.29 TLS Mutual Authentication per SIP Interface

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

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

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

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

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

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

Applicable Products: All.

3.1.1.31 Same Defaults for IP / Tel Profiles and Global Parameters

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

Applicable Products: All.

3.1.1.32 Increase in Maximum Number of SIP Message Manipulation Rules

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.1.33 Failed Registration Request Handling

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

Applicable Products: All.

3.1.1.34 Registration Expiry Time from Original Contact

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

Applicable Products: All.

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

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

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

[VerifyRecievedVia]	Enables the device to reject initial requests in which the top-most Via header contains an IP address that is different than the source IP address received in the From header. These requests are rejected without sending a response. ▪ [0] Disable (default) = SIP request is not rejected, as this IP address mismatch indicates that the UA is behind NAT. ▪ [1] Enable = SIP request is rejected.

Applicable Products: All.

3.1.2 SIP Gateway / IP-to-IP Features

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

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

3.1.2.1 V.150.1 SDP Format

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

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

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

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

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

Applicable Products: All.

3.1.2.2 Double Wink-Start Signaling and Polarity Reversal

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

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

Web/EMS: Enable DID Wink CLI: did-wink-enbl [EnableDIDWink]	Enables Direct Inward Dialing (DID) using Wink-Start signaling, typically used for signaling between an E-911 switch and the PSAP. ▪ [0] Disable (default) ▪ [1] Single = The device can be used for connection to EIA/TIA-464B DID Loop Start lines. Both FXO (detection) and FXS (generation) are supported: ✓ The FXO interface dials DTMF (or MF) digits upon detection of a Wink signal, instead of a dial tone. ✓ The FXS interface generates a Wink signal upon detection of an off-hook state, instead of playing a dial tone. Example: (Wink) KP I(I) xxx-xxxx ST (Off Hook) Where: ✓ I = one or two information digits ✓ x = ANI Note: The FXO interface generates such MF digits when

	the Enable911PSAP parameter is set to 1. ▪ [2] Double Wink = Double-wink signaling. The FXS interface generates the first wink upon detection of an off-hook state in the line. The second wink is generated after a user-defined interval (configured by the TimeBetweenDIDWinks parameter), after which the DTMF/MF digits are collected by the device. Digits that arrive between the first and second wink are ignored as they contain the same number. Example: (Wink) KP 911 ST (Wink) KP I(I) xxx-xxxx ST (Off Hook). ▪ [3] Wink and Polarity = The FXS interface generates the first wink after it detects an off-hook state. A polarity change from normal to reversed is generated after a user-defined time (configured by the TimeBetweenDIDWinks parameter). DTMF/MF digits are collected only after this polarity change. Digits that arrive between the first wink and the polarity change are ignored as they always contain the same number. In this mode, the FXS interface does not generate a polarity change to normal if the Tel-to-IP call is answered by an IP party. Polarity reverts to normal when the call is released. Example: (Wink) KP 911 ST (Polarity) KP I(I) xxx-xxxx ST (Off Hook) Notes: ▪ Options [2] and [3] are applicable only to FXS interfaces. ▪ The EnableReversalPolarity and PolarityReversalType parameters must be set to [1] for FXS interfaces. ▪ See also the Enable911PSAP parameter. ▪ This parameter can also be configured in a Tel Profile.
[TimeBetweenDIDWinks]	Defines the interval (in msec) for wink signaling: ▪ Double-wink signaling [2]: interval between the first and second wink ▪ Wink and Polarity signaling [3]: interval between wink and polarity change The default value is 100 to 2000. The default is 1000. Note: See the EnableDIDWink parameter for configuring the wink signaling type.

Applicable Products: MP-1xx; Mediant 600; Mediant 1000 Series; Mediant 8xx Series.

3.1.2.3 Increase in Maximum SIP Calling Name Manipulation Rules

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.4 Simultaneous Negotiation of Fax (T.38) and Modem (V.150.1) Relay CED Tone

This feature provides support for negotiating fax relay (T.38) and modem relay (V.150.1) sessions in the same, already established call channel. Fax relay sessions require bypass answering tone (CED), while modem relay requires RFC 2833 answering tone. As the

device is not always aware at the start of the session whether the answering tone is fax or modem, it uses both methods for CED tone transfer. It sends both answering tone types and then sends only the fax or modem, depending on which is detected. Up until this release, the device could only be configured for fax relay or modem relay, not both.

To support this feature, a Coders Group must be configured (in the Coders Group table) that includes the T.38, V.150, and G.711/VBD coders.

Note: For V.150 support, the installed Software License Key must include the V.150.1 feature.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 3000.

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

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

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

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

Applicable Products: MP-1xx; Mediant 600; Mediant 1000 Series; Mediant 8xx Series.

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

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

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

[UserToUserHeaderFormat]	Defines the format of the SIP User-to-User header in INVITE messages for interworking with the ISDN User to User (UU) IE data to SIP. This applies to Tel-to-IP and IP-to-Tel calls.
	▪ [0] = (Default) Format: X-UserToUser.
	▪ [1] = Format: User-to-User with Protocol Discriminator (pd) attribute. For example:
	`User-to-User=30303734353137343136353 53b313233343b3834;pd=4`
	This format is according to IETF Internet-Draft draft-johnston-sipping-cc-uui-04.
	▪ [2] = Format: User-to-User with encoding=hex at the end and pd embedded as the first byte. For example:
	`User-to-User=043030373435313734313635353b313233343b3834; encoding=hex`
	Where "04" at the beginning of this message is the pd. This format is according to IETF Internet-Draft draft-johnston-sipping-cc-uui-03.
	▪ [3] = Interworks the SIP User-to-User header containing text format to ISDN UUIE in hexadecimal format, and vice versa. For example:
	SIP Header in text format:
	`User-to-User=01800213027b712a;NULL;4582166;`
	Translated to hexadecimal in the ISDN UUIE:
	`3031383030323133303237623731326 13b4e554c4c3b343538323136363b`
	The Protocol Discriminator (pd) used in UUIE is "04" (IUA characters).

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.7 New Format for re-INVITE for Call Hold

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

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

Web/EMS: Hold Format CLI: hold-format [HoldFormat]	Determines the format of the SDP in the sent re-INVITE hold request. ▪ [0] 0.0.0.0 = (Default) The SDP "c=" field contains the IP address "0.0.0.0" and the "a=inactive" attribute. ▪ [1] Send Only = The SDP "c=" field contains the device's IP address and the "a=sendonly" attribute.

	▪ [2] x.y.z.t = The SDP "c=" field contains the device's IP address and the "a=inactive" attribute. Notes: ▪ The device does not send any RTP packets when it is in hold state (for both hold formats). ▪ For digital interfaces: This parameter is applicable only to QSIG and Euro ISDN protocols.

Applicable Products: MP-1xxMediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 2000; Mediant 3000.

3.1.2.9 Calling Name Retrieval from AD using LDAP Query

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

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

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

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

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

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

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

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

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

CLI: ldap-display-nm-attr [MSLDAPDisplayNameAttributeName]	Defines the attribute name that represents the Calling Name in the AD for LDAP queries based on calling number. The valid value is a string of up to 49 characters. The default is "displayName".

Notes:

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

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

3.1.2.10 Call Preemption per Trunk

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

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

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

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

Notes:

- For trunks configured with call preemption, all must be configured to [1] or all configured to [2]. In other words, the device cannot have some trunks set to [1] and some to [2].
- The global parameter must be set to the same value as that of the Tel Profile parameter; otherwise, the Tel Profile parameter will not be applied.

- If you configure call preemption using the global parameter and a new Tel Profile is subsequently added, the TelProfile_CallPriorityMode parameter automatically acquires the same setting as well.

Applicable Products: MP-11x; Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.11 Interworking MLPP Network Identity between ISDN and SIP

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

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

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

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

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

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

Notes:

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

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

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

MLPP Default Namespace CLI: mlpp-dflt-namespace [MLPPDefaultNamespace]	Determines the namespace used for MLPP calls that are received from the ISDN side without a Precedence IE and destined for the Application server. This value is used in the Resource-Priority header of the outgoing SIP INVITE request. ▪ [1] DSN (default)

	▪ [2] DOD ▪ [3] DRSN ▪ [5] UC ▪ [7] CUC **Note:** If the ISDN message contains a Precedence IE, the device automatically interworks the "network identity" (NI) digits in the IE to the network domain subfield in the Resource-Priority header, as follows: Precedence IE — Resource-Priority Header 0000 — uc 0001 — cuc 0002 — dod 0003 — nato

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.13 User-Defined MLPP Network Domains

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

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

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

- If the network-domain field in the Resource-Priority header is "uc", then the device sets the Precedence Level field in the ISDN PRI Precedence Level IE according to Table

5.3.2.12-4 (Mapping of RPH r-priority Field to PRI Precedence Level Value):

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

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

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

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

[ResourcePriorityNetworkDomains]	Defines MLPP network domain names. The domain name is a string that can contain up to 10 characters. FORMAT ResourcePriorityNetworkDomains_Index = ResourcePriorityNetworkDomains_Name, ResourcePriorityNetworkDomains_EnableIp2TelInterworking; ResourcePriorityNetworkDomains 1 = dsn, 0; ResourcePriorityNetworkDomains 2 = dod, 0; ResourcePriorityNetworkDomains 3 = drsn, 0; ResourcePriorityNetworkDomains 5 = uc, 1; ResourcePriorityNetworkDomains 7 = cuc, 0; [\ResourcePriorityNetworkDomains] **Notes:** ▪ Indices 1, 2, 3, 5, and 7 cannot be modified and are defined for DSN, DOD, DRSN, UC, and CUC, respectively. ▪ If the MLPPDefaultNamespace parameter is set to -1, interworking from PSTN NI digits is done automatically.

Applicable Products: Mediant 1000 Series; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

To enable this feature, the device supports manipulation of the original destination number (i.e., 911) received from E-911 remote branch callers to the destination number of an emergency provider relevant to the geographical area in which the remote branch office is

located. The device identifies these callers by their ELIN numbers, contained in the PIDF-LO XML body of the received SIP INVITE message. The ELIN number is associated with the precise location (e.g., civic address and building floor level) of the E-911 caller.

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.16 Rejecting Emergency INVITE Messages with SIP 503 Response

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

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

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

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

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

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

[FaxReroutingMode]	Determines the re-routing of Tel-to-IP calls that are identified as fax calls. If a CNG tone is detected on the Tel side of a Tel-to-IP call, the prefix string "FAX" is appended to the destination number before routing and manipulation. A value of "FAX" entered as

	the destination number in the Outbound IP Routing table is then used to route the call, and the destination number manipulation mechanism is used to remove the "FAX" prefix, if required. Note that the "FAX" prefix string in routing and manipulation tables is case-sensitive. If the initial INVITE used to establish the voice call (not fax) was already sent, a CANCEL (if not connected yet) or a BYE (if already connected) is sent to release the voice call. ▪ [0] Disable (default) ▪ [1] Rerouting without Delay ▪ [2] Progress and Delay = Incoming ISDN calls are delayed until a CNG tone detection or timeout, set by the FaxReroutingDelay parameter. If the EnableComfortTone parameter is set to 1, a Q.931 Progress message with Protocol Discriminator set to 1 is sent to the PSTN and a comfort tone is played accordingly to the PSTN. When the timeout expires, the device sends an INVITE to a specific IP Group or to a fax server, according to the Outbound IP Routing table rules. This option is applicable only to ISDN. ▪ [3] Connect and Delay = Incoming ISDN calls are delayed until a CNG tone detection or timeout, set by the FaxReroutingDelay parameter. A Q.931 Connect message is sent to the PSTN. If the EnableComfortTone parameter is set to 1, a comfort tone is played to the PSTN. When the timeout expires, the device sends an INVITE to a specific IP Group or to a fax server according to the Outbound IP Routing table rules. This option is applicable only to ISDN. **Note:** This parameter replaces the EnableFaxRerouting parameter. For backward compatibility, the EnableFaxRerouting parameter set to 1 is equivalent to the FaxReroutingMode parameter set to 1.
[FaxReroutingDelay]	Defines the maximum time interval (in seconds) that the device waits for CNG detection before re-routing calls identified as fax calls to fax destinations (terminating fax machine). The valid value range is 1-10. The default is 5.

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

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

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

Applicable Products: MP-11x; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.19 T.38 re-INVITE upon Detection of V.34 / Super G3 V8-CM Signals

This feature provides support for enhanced fax-relay handling upon detection of V.34/Super G3 V8-CM (Call Menu) signals. If the device detects V8-CM signals (or a fax CNG tone) from the originating fax, it sends a SIP re-INVITE with T.38 parameters in the SDP to the terminating fax. Up until this release, sending T.38 re-INVITE was only possible upon detection of fax CNG tones. Detection of the CNG tone is done only if enabled (using the CNGDetectorMode parameter).

To support this feature, a new option, [2] has been added to the existing 'Fax CNG Mode' parameter:

Fax CNG Mode [FaxCNGMode]	Determines the device's handling of fax relay upon detection of a fax CNG tone or a V.34/Super G3 V8-CM (Call Menu) signal from originating faxes. ▪ [0] = (Default) SIP re-INVITE is not sent. ▪ [1] = Sends a SIP re-INVITE with T.38 parameters in SDP upon detection of a fax CNG tone if the CNGDetectorMode parameter is set to 1. ▪ [2] = Sends a SIP re-INVITE with T.38 parameters in SDP upon detection of a fax CNG tone (if the CNGDetectorMode parameter is set to 1) or upon detection of a V8-CM signal. **Notes:** ▪ For Mediant 3000: Option [2] is applicable only if the device is loaded with DSP template 10 (i.e., DSPVersionTemplateNumber parameter is set to 10). ▪ If this parameter is set to [2] and the CNGDetectorMode parameter is set to [0], the device sends a re-INVITE only if it detects a V8-CM signal from the originating fax. ▪ This feature is applicable only if the IsFaxUsed parameter is set to [1] or [3]. ▪ The device also sends T.38 re-INVITE if the CNGDetectorMode parameter is set to [2], regardless of the FaxCNGMode parameter settings.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 3000.

3.1.2.20 Call Detail Records for IP-to-IP Application

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

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

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

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

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

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.22 Manipulation of SIP REGISTER Messages

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

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.23 Host Name as Match Criteria for Number Manipulation Rules

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

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

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

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

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

Applicable Products: MP-11x; Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.24 Destination Number Manipulation Rules per Destination IP Group

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

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

Applicable Products: MP-11x; Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.25 Increase in Number of Destination Number Manipulation Rules

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

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

Applicable Products: MP-11x; Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.26 Forcing Device to Send Local Date / Time to PBX

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

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

Send Local Time To ISDN Connect [SendLocalTimeToISDNC	Determines the device's handling of the date and time sent in the ISDN Connect message (Date / Time Information Element) upon receipt of SIP 200 OK messages. This

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.27 Routing SIP Calls to Specific E1/T1 Trunks

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.28 Euro ISDN and QSIG to SIP Redirected Number Manipulation

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

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

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

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

For example, assume the following required manipulation:

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

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

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.29 IP-to-Tel Routing based on Source SRD

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.30 Interworking User Information from REFER to Q.931 Setup

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

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

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

Enable User-to-User IE for IP to Tel CLI: uui-ie-for-ip2tel [EnableUUIIP2Tel]	Enables interworking of SIP user-to-user information (UUI) to User-to-User IE in ISDN Q.931 messages. ▪ [0] Disable (default) = Received UUI is not sent in ISDN message. ▪ [1] Enable = Device interworks UUI from SIP to ISDN. The device supports the following SIP-to-ISDN interworking of UUI: ✓ SIP INVITE to Q.931 Setup ✓ SIP REFER to Q.931 Setup ✓ SIP 200 OK to Q.931 Connect ✓ SIP INFO to Q.931 User Information ✓ SIP 18x to Q.931 Alerting ✓ SIP BYE to Q.931 Disconnect Notes: ▪ The interworking of ISDN User-to-User IE to SIP INFO is

	applicable only to the Euro ISDN, QSIG, and 4ESS PRI variants. ▪ To interwork the UUIE header from SIP-to-ISDN messages with the 4ESS ISDN variant, the ISDNGeneralCCBehavior parameter must be set to 16384.

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.31 Special Dial Tone to FXS Phones when Call Forward Activated

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

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

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

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

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

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

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

Applicable Products: MP-1xx; Mediant 1000 Series; Mediant 8xx Series.

3.1.2.32 FXS Call Transfer using SIP INVITE and re-INVITE Messages

This feature provides support for handling call transfers using SIP INVITE and re-INVITE messages instead of REFER messages. This feature is useful when communicating with SIP UAs that do not support the receipt of REFER messages. This feature is applicable to FXS interfaces.

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

Enable Call Transfer Service using REINVITES CLI: enable-call-transfer-using-reinvites [EnableCallTransferUsingReinvites]	Enables call transfer using re-INVITEs. ▪ [0] Disable = (Default) Call Transfer is done using REFER messages. ▪ [1] Enable = Call transfer is done by sending re-INVITE messages (instead of REFER). **Note:** This parameter is applicable only to FXS interfaces.

Applicable Products: Mediant 1000 Series; Mediant 8xx Series.

3.1.2.33 Denial of Collect Calls per Tel Profile

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

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

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

Applicable Products: MP-11x; Mediant 600; Mediant 1000 Series; Mediant 8xx Series.

3.1.2.34 Increase in Maximum Number of Trunk Groups

This feature provides support for an increase in the maximum number of Trunk Groups from 120 to 240 that can be configured. Accordingly, the maximum number of row entries (indexes) of the Trunk Group Settings table has been increased from 100 to 240.

Applicable Products: Mediant 3000.

3.1.2.35 Configurable Name for Trunk Group

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

For example:

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

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

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

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

- UseSIPtgrp
- UseBroadsoftDTG

Applicable Products: MP-11x; Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.36 Connected Number Subaddress Added to Connect Message

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

Applicable Products: Mediant 1000 Series; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.37 Minimum Call Duration for Disconnecting PSTN Calls

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

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.38 Increased Timeout for Call Disconnect upon LOS / LOF

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

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

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

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

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

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

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

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

Applicable Products: MP-1xx; Mediant 600; Mediant 1000 Series; Mediant 8xx Series.

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

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

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

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

Applicable Products: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 1000 Series; Mediant 8xx Series.

3.1.2.42 Early Answer Timeout per Call

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

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.43 Coder Negotiation Priority between Local or Remote Coder List

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

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

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

Applicable Products: MP-1xx; Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

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

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

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

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

	of the re-INVITE for re-negotiating the coder.

Applicable Products: MP-1xx; Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.45 Increase in Number of On-Board Three-Way Conferencing

This feature provides support for an increase, from two to five in the maximum number of simultaneous, on-board three-way conferences. This is relevant for FXS and BRI interfaces. The number of simultaneous, three-way conferences can be limited using the existing parameter, MaxInBoardConferenceCalls.

Applicable Products: Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series.

3.1.2.46 Performance Monitoring for All Trunks Busy (ATB)

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

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

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

To support this feature:

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.2.47 ISO 8859 Character Set Type

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

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

CLI: iso8859-charset [ISO8859CharacterSet]	Defines the ISO 8859 character set type (languages) for representing the alphanumeric string of the calling name (caller ID) in the forwarded message, for IP-to-Tel and Tel-to-IP calls. ▪ [0] No Accented = Proprietary method where incoming INVITE messages with any accented characters (e.g., á, é, í, ó, and ü), which are represented in a 2-byte unicode character, are translated to Latin-only, which are normal one-byte ASCII characters (a, e, i, o, and u, respectively). ▪ [1] Western European (Default) ▪ [2] Central European ▪ [3] South European ▪ [4] North European ▪ [5] Cyrillic ▪ [6] Arabic ▪ [7] Hebrew ▪ [8] Turkish

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.3 SIP Stand-Alone Survivability (SAS) Features

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

3.1.3.1 SAS Emergency upon OPTIONS Only Response Failure

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

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

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

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

Applicable Products: All.

3.1.3.2 Re-using TCP Connections for SAS

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

For example, assume the following:

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

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

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

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

Applicable Products: All.

3.1.4 Session Border Controller Features

This subsection describes the new Session Border Controller (SBC) application features.

Note: This section is applicable only to devices that support the SBC application.

3.1.4.1 Increase in Number of Maximum Transcoding Sessions

This feature provides support for an increase in the maximum number of IP-to-IP coder transcoding sessions from 325 to 1,092 for Mediant 4000, and from 175 to 350 for Mediant 2600. This is achieved by the use of the new Media Processing Module (MPM), which provides additional digital signal processors (DSP). The MPM module is installed in Slots 1 and 2.

Notes:

- The MPM is a customer-ordered item.
- For existing customers that want to add the MPM, the E-SBC (CPU) module must be relocated to Slot 5-6.

Applicable Products: Mediant 2600; Mediant 4000.

3.1.4.2 User Registration Time per IP Profile

This feature provides support for configuring user registration time for IP Profiles, which is done in the IP Profile table. This enables assigning different use registration times to specific calls. Up until this release, registration time could only be configured for all calls.

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

SBC User Registration Time [IpProfile_SBCUserRegistrationTime]	Defines the duration (in seconds) of the periodic registrations that occur between the user and the device (the device responds with this value to the user). When set to 0, the device does not change the Expires header's value received in the user's REGISTER request. If no Expires header is received in the REGISTER message and this parameter is set to 0, the Expires header's value is set to 180 seconds, by default. The valid range is 0 to 2,000,000 seconds. The default is 0.

Applicable Products: E-SBC Series.

3.1.4.3 Interworking DTMF Payload Type for RFC 2833

This feature provides support for interworking the DTMF payload type for RFC 2833 between different SBC call entities. For example, if two communicating UAs require different RFC 2833 DTMF payload types, the SDP offer received by the device from one UA is forwarded to the destination UA with its DTMF payload type replaced with the configured payload type, and vice versa.

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

SBC RFC2833 DTMF Payload Type Value CLI: sbc-2833dtmf-payload [IpProfile_SBC2833DTMFPayloadType]	Defines the RFC 2833 DTMF Payload Type. The value range is 96 to 127. The default is 0 (i.e., the device forwards the received payload type as is).

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.4.4 Removing 'gop' parameter in SBC Authentication Challenge

This feature provides support for removing the 'qop' parameter from the sent SIP 401 response. The 'qop' parameter defines the authentication and 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 SIP 401 response with the Proxy-Authenticate header or WWW-Authenticate header containing the 'qop' parameter. The QoP offered in the 401 response can be 'auth', 'auth-int', both 'auth' and 'auth-int', or the 'qop' parameter can be omitted from the 401 response. In response to the 401, the client needs to send the device another INVITE with the MD5 hash of the INVITE message and indicate the selected QoP.

To support this feature, a new option, [3] has been added to the existing parameter, 'Authentication Quality of Protection':

Authentication Quality of Protection [AuthQOP]	Defines the authentication and 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 SIP 401 response with the Proxy-Authenticate header or WWW-Authenticate header containing the 'qop' parameter. The QoP offered in the 401 response can be 'auth', 'auth-int', both 'auth' and 'auth-int', or the 'qop' parameter can be omitted from the 401 response. In response to the 401, the client needs to send the device another INVITE with the MD5 hash of the INVITE message and indicate the selected auth type. ▪ [0] 0 = The device sends 'qop=auth' in the SIP response, requesting authentication (i.e., validates user by checking user name and password). This option does not authenticate the message body (i.e., SDP). ▪ [1] 1 = The device sends 'qop=auth-int' in the SIP response, indicating required authentication and authentication with integrity (e.g., checksum). This option restricts the client to authenticating the entire SIP message, including the body, if present. ▪ [2] 2 = (Default) The device sends 'qop=auth, auth-int' in the SIP response, indicating either authentication or integrity. This enables the client to choose 'auth' or 'auth-int'. If the client chooses 'auth-int', then the body is included in the authentication. If the client chooses 'auth', then the body is not authenticated. ▪ [3] 3 = No 'qop' parameter is offered by the device in the SIP 401 challenge message.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.4.5 Media (RTP) Normalization

This feature provides support for interworking (normalization) the media (RTP-to-RTP, SRTP-to-RTP, and SRTP-to-SRTP) between SBC legs. The SBC re-builds specific fields in the RTP header when forwarding the media packets. The main fields include the following:

- Sequence number
- SSRC
- Timestamp

This feature applies to all forwarded media.

Applicable Products: E-SBC Series.

3.1.4.6 Increase in Maximum Number of SBC IP-to-IP Routing Rules

This feature provides support for an increase in the maximum number of SBC IP-to-IP routing rules that can be configured in the SBC IP-to-IP Routing table from 200 to 1,000.

Applicable Products: Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.4.7 Increase in Maximum Number of Classification Rules

This feature provides support for an increase in the maximum number of Classification rules that can be configured in the Classification table from 20 to 100.

Applicable Products: E-SBC Series.

3.1.4.8 SIP Response Code for Unclassified Calls

This feature provides support for configuring the SIP response that the device sends to the requestor upon call classification failure. The device can either be configured to send a specific SIP reject response code (400 to 699) or not to send any response at all. Note that this is applicable only when the Unclassified Calls feature is disabled.

This feature is important for preventing Denial of Service (DoS) attacks, typically initiated from the WAN. Malicious attackers can use SIP scanners to detect ports used by SIP devices. These scanners scan devices by sending UDP packets containing a SIP request (OPTIONS, REGISTER, or INVITE) to a range of specified IP addresses, listing those that return a valid SIP response. Once the scanner finds a device that supports SIP, it extracts information from the response and identifies the type of device (IP address and name). Once the attacker has this list, he/she can execute DoS attacks. A way to defend the device against such attacks is to not send a SIP reject response to these unclassified "calls" so that the attacker assumes that no device exists at such an IP address and port.

To support this feature, the following new parameter has been added to the SIP Interface table:

Classification Failure Response Type CLI: classification_fail_response_type [SIPInterface_ClassificationFailureResponseType]	Defines the SIP response code that the device sends in response to a SIP request (OPTIONS, REGISTER, or INVITE) that has failed the classification process. The valid value can be a SIP response code from 400 through 699, or it can be set to 0 to not send any response at all. The default response code is 500 (Server Internal Error).

Applicable Products: E-SBC Series.

3.1.4.9 Call Forking to Available Contacts Only

This feature provides support for configuring SBC call forking of INVITE messages only to contacts that are available (i.e., not busy). The device forks calls to multiple available contacts if they are registered under the same AoR in its registration database. The device sends the INVITE sequentially to each available contact. If there is no answer from the first contact, it sends the INVITE to the second contact and so on until a contact answers. If no contact answers, the call fails or is routed to an alternative destination, if configured.

To support this feature, a new option - Sequential Available Only - has been added to the existing 'Enable SBC Client Forking' parameter in the IP Group table:

SBC Client Forking Mode [IPGroup_EnableSBCClientForking]	Defines the call forking mode of INVITE messages, to up to five separate SIP outgoing legs for User-type IP Groups. This occurs if multiple contacts are registered under the same AoR in the device's database. ▪ [0] Sequential (default) = Sequentially sends the INVITE to each contact. If there is no answer from the first contact, it sends the INVITE to the second contact, and so on until a contact answers. If no contact answers, the call fails or is routed to an alternative destination, if configured. ▪ [1] Parallel = Sends the INVITE simultaneously to all contacts. The call is established with the first contact that answers. ▪ [2] Sequential Available Only = Sequentially sends the INVITE to each available contact.

Applicable Products: E-SBC Series.

3.1.4.10 Call Forking of Specific Contact to all Contacts under AoR

This feature provides support for enabling SBC call forking of INVITE messages received with a Request-URI of a specific contact (user) to all other users located under the same AoR as the specific contact.

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

SBC Send Invite To All Contacts CLI: sbc-send-invite-to-all-contacts [SBCSendInviteToAllContacts]	Enables call forking of INVITE message received with a Request-URI of a specific contact registered in the device's database, to all users under the same AoR as the contact. ▪ [0] Disable (default) = Sends the INVITE only to the contact in the received Request-URI. ▪ [1] Enable

Applicable Products: E-SBC Series.

3.1.4.11 Termination of REGISTER for Shared Lines

This feature provides support for terminating on the SBC, SIP REGISTER messages of secondary lines related to the Shared Line feature.

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

SBC Shared Line Registration Mode CLI: sbc-shared-line-reg-mode [SBCSharedLineRegMode]	Enables termination on the SBC of SIP REGISTER messages from secondary lines pertaining to the Shared Line feature. ▪ [0] Disable = (Default) The SBC forwards the REGISTER messages as is (i.e., not terminated on the SBC). ▪ [1] Enable = REGISTER messages of secondary

	lines are terminated on the SBC. Note: The SBC always forwards the REGISTER of the primary line.

Applicable Products: E-SBC Series.

3.1.4.12 Interworking Call Hold and Retrieve Requests

This feature provides support for interworking call hold / retrieve requests between UAs supporting different call hold SDP formats and those that support and do not support play of the held tone.

This feature includes the following support:

- The device can interwork call hold between UAs supporting different SDP call hold formats. The interworking is done on the SDP of the re-INVITE sent by the device to the held party. The device can either terminate the call hold request and play a held tone to the held party, forward the received SDP as is to the held party, or modify the SDP ('a=' and / or 'c=' lines) sent to the held party. This is supported using the new IP Profile parameter, 'SBC Remote Hold Format'.
- The device can be configured to generate and play a held tone to the held party. This is useful for call-held parties that do not support the play of local held tones, or for UAs initiating call hold that do not support the generation of the held tone. This feature is configured using the new IP Profile parameter, 'SBC Play Held Tone'.
- The device can be configured to ignore received call hold requests (i.e., SDP with 'a=sendonly') and instead play a held tone to the held party. This is useful for UAs who initiate call hold but who do not support the generation of the held tone. This support is configured using the new IP Profile parameter, 'SBC Reliable Held Tone Source'.

To support this feature, the following new parameters have been added to the IP Profile table:

SBC Remote Hold Format [IPProfile_SBCRemoteHoldFormat]	Defines the SDP format for call hold that is sent to the held party. • [0] transparent = SDP forwarded as is. • [1] send-only = SDP sent with 'a=sendonly'. • [2] send only 0.0.0.0 = SDP sent with 'a=sendonly' and 'c=0.0.0.0'. • [3] inactive = SDP sent with 'a=inactive'. • [4] inactive 0.0.0.0 = SDP sent with 'a=inactive' and 'c=0.0.0.0'. • [5] not supported = Indicates that the remote side cannot identify a call hold message. The device terminates the received call hold message (re-INVITE / UPDATE) and sends a 200 OK to the call hold initiator. It plays a held tone to the held party if the 'SBC Play Held Tone' parameter is set to **Yes**.
SBC Play Held Tone [IpProfile_SBCPlayHeldTone]	Enables the device to play a held tone to the held party. This is useful if the held party does not support playing a local held tone. • [0] No (default) • [1] Yes Note: If this parameter is set to **Yes**, the device plays the tone only if the 'SBC Remote Hold Format' parameter is set to **transparent**, **send-only**, **send only 0.0.0.0**, or **not supported**.
SBC Reliable Held Tone Source	Enables the device to consider the received call hold request (re-INVITE/UPDATE) with SDP containing

[IPProfile_ReliableHoldToneSource]	'a=sendonly', as genuine. • [0] No (default) = Even if the received SDP contains 'a=sendonly', the device plays a held tone to the held party. This is useful in cases where the initiator of the call hold does not support generation of held tones. • [1] Yes = If the received SDP contains 'a=sendonly', the device does not play a held tone to the held party (and assumes that the initiator of the call hold plays the held tone). Note: The device plays a held tone only if the 'SBC Play Held Tone' parameter is set to **Yes**.

Applicable Products: E-SBC Series.

3.1.4.13 Increase in Maximum Number of SBC Sessions

The Mediant 4000 now supports up to 4,000 SBC sessions (from 1,800).

Applicable Products: Mediant 4000.

3.1.4.14 Increase in Maximum Number of Registered Users

This feature provides support for an increase in the maximum number of registered users for the following products:

- **Mediant 3000 with TP-6310 or TP-8410 Depopulated (Fixed Configuration):** 5,000 (from 3,000)
- **Mediant 4000:** 20,000
- **Mediant SW E-SBC:** 20,000

Applicable Products: Mediant 3000; Mediant 4000; Mediant SW E-SBC.

3.1.4.15 Interworking SIP REFER (Call Transfer)

This feature provides support for enhanced interworking and handling of SIP REFER messages. SIP UAs may support different versions of the REFER standard while some may even not support REFER. This results in interoperability issues, which this feature resolves.

This feature enables the configuration of 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. The device generates a new INVITE to the alternative destination according to the rules in the IP-to-IP Routing table. The IP-to-IP 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 new 'Call Trigger' field in this table 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 IP-to-IP Routing table in the new 'Re-Route IP Group ID' field. For more information on this feature, see Section 3.1.4.24.

To support this feature, 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' has been added to this IP Profile parameter:

[IPProfile_SBCRemoteReferBehavior]	• [0] Regular = (Default) 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.

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 attempting 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

Applicable Products: E-SBC Series.

3.1.4.16 Interworking SIP PRACK Requests

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

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

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

Applicable Products: E-SBC Series.

3.1.4.17 Interworking SIP 3xx Redirect Responses

This feature provides support for interworking 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 such as Diversion, History-Info, P-Asserted-Id, and Priority. The source and destination URIs can be manipulated using the regular manipulation mechanism.

The E-SBC sends the new request to the alternative destination according to the IP-to-IP Routing table rules. The IP-to-IP Routing table has been enhanced to route such "re-route" requests differently than regular request routing. For the E-SBC to route requests triggered by 3xx, the new '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 IP-to-IP Routing table in the new 'Re-Route IP Group ID' field. For more information on this feature, see Section 3.1.4.24.

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" has been added to this IP Profile parameter to support 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 and forwards the 3xx response.

Applicable Products: E-SBC Series.

3.1.4.18 Interworking 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 mismatch by performing the keep-alive process on behalf of devices that do not support it.

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

[IPProfile_SBCSessionExpiresMode]	Determines the required session expires mode at the remote SIP endpoint. • [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

Applicable Products: E-SBC Series.

3.1.4.19 Interworking SIP Early Media

This feature provides support for handling SIP early media.

- **Early Media Enabling:**

  This feature provides support for interworking early media between SIP UAs (IP Groups) that support and do not support receipt of early media. Early media can arrive in provisional responses to an INVITE request. 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 ringback tone.

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

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

[IPProfile_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 provides support for determining the SIP provisional response type – 180 or 183 – to forward the early media to the caller.

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

[IPProfile_SBCRemoteEarlyMediaResponseType]	▪ [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:**

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

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

[IPProfile_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.

- **Early media RTP:**

  This feature provides support for interworking with remote clients that send 18x responses with early media, but consequent RTP is delayed (e.g. Lync), while others do not support this and require RTP to follow the 18x response immediately. Some clients do not support 18x with early media. Others require 18x with early media (i.e., they cannot play ringback tone locally).

  To support this feature, the following new parameters have been added to the IP Profile table:

SBC Remote Early Media RTP [IPProfile_SBCRemoteEarlyMediaRTP]	▪ [0] Immediate = (Default) Remote client sends RTP immediately after it sends 18x response with early media. ▪ [1] Delayed = After sending 18x response, the remote client waits before sending RTP (e.g., Microsoft Lync environment).
SBC Remote Supports RFC 3960 [IPProfile_SBCRemoteSupportsRFC3960]	Remote client is capable of receiving 18x messages with delayed RTP. ▪ [0] Not Supported = (Default) Remote client does not support receipt of 18x messages with delayed RTP. ▪ [1] Supported = Remote client is capable of receiving 18x messages with delayed RTP.
SBC Remote Can Play Ringback [IPProfile_SBCRemoteCanPlayRingback]	Remote client can play local ringback tone. If not, we must send 18x with early media. ▪ [0] No ▪ [1] Yes (Default)

Applicable Products: E-SBC Series.

3.1.4.20 Interworking SIP re-INVITE Messages

This feature provides support for handling SIP re-INVITE messages.

- **Interworking re-INVITE:**

  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 either be 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 adds it to the incoming re-INVITE request if it does not contain an SDP and only then forwards it to the destination endpoint.

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

[IPProfile_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.

Applicable Products: E-SBC Series.

3.1.4.21 Interworking SIP UPDATE Requests

This feature provides support for enabling 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 either be a success or a failure, depending on whether the E-SBC can bridge the media between the endpoints.

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

[IPProfile_SBCRemoteUpdateSupport]	Determines whether endpoints associated with 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.

Applicable Products: E-SBC Series.

3.1.4.22 Interworking SIP re-INVITE to UPDATE Requests

This feature provides support for enabling communication between endpoints (IP Groups) that do not support re-INVITE requests but support the UPDATE method, and vice versa. The E-SBC translates the re-INVITE request to the UPDATE request, and vice versa. Note that if a re-INVITE request arrives without SDP, the E-SBC generates SDP and adds it to the outgoing UPDATE request. To enable this feature, each IP Group needs to be configured with its capabilities by associating it with a relevant IP Profile. 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 is translated to an UPDATE request.

Applicable Products: E-SBC Series.

3.1.4.23 Interworking Delayed Offer

This feature provides support for enabling sessions between endpoints (IP Groups) that send INVITEs without SDP (delayed media) and those that do not support the 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.

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

[IPProfile_SBCRemoteDelayedOfferSupport]	Determines whether the remote endpoint supports 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.

Applicable Products: E-SBC Series.

3.1.4.24 Re-Routing SIP Requests using IP-to-IP Routing Table Rules

This feature provides support for complementing the features that enable the re-routing of requests (e.g., INVITE) upon receipt of SIP 3xx responses or REFER messages, using different routing rules than for regular requests.

To support this feature, the following new fields have been added to the IP-to-IP Routing table:

Call Trigger [IP2IPRouting_Trigger]	Defines the reason (or trigger) for re-routing the request: ▪ [0] Any = (Default) This routing rule is used for all scenarios (re-routes and non-re-routes). ▪ [1] 3xx = Re-routes the request if it was triggered as a result of a SIP 3xx response. ▪ [2] REFER = Re-routes the INVITE if it was triggered as a result of a REFER request. ▪ [3] 3xx or REFER = Same as [1] and [2]. ▪ [4] 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 IPGroup ID [IP2IPRouting_ReRouteIPGroupID]	Defines the IP Group that initiated (sent) the Redirect (e.g., 3xx) / REFER message. The default is -1 (i.e., not configured).

Applicable Products: E-SBC Series.

3.1.4.25 IP-to-IP Outbound Manipulation on Re-Routed SIP Requests

This feature provides support for manipulating SIP URI user part (source and destination) of re-routed, outbound SIP dialog requests. Re-routed requests can be done for received SIP 3xx responses or REFER messages.

To support this feature, the following new fields have been added to the IP-to-IP Outbound Manipulation table:

Call Trigger	Defines the reason (or trigger) for re-routing the request:

[IPOutboundManipulation_Trigger]	▪ [0] Any = (Default) All scenarios (re-routes and non-re-routes). ▪ [1] 3xx = Re-routes the request if it was triggered as a result of a SIP 3xx response. ▪ [2] REFER = Re-routes the INVITE if it was triggered as a result of a REFER request. ▪ [3] 3xx or REFER = Same as [1] and [2]. ▪ [4] Initial Only = 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 [IPOutboundManipulation_ReRouteIPGroupID]	Defines the IP Group that initiated (sent) the Redirect (e.g., 3xx) / REFER message. The default is -1 (i.e., not configured).

Applicable Products: E-SBC Series.

3.1.4.26 Session Description Protocol (SDP) Insertion

This feature provides support for adding an SDP body to the outgoing SIP message. For certain mid-call media negotiations such as interworking of re-INVITEs and 18x responses with or without SDP, the E-SBC needs to add an SDP offer or answer to 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.

Applicable Products: E-SBC Series.

3.1.4.27 Routing based on LDAP Queries

This feature provides support for the Lightweight Directory Access Protocol (LDAP), enabling the E-SBC device to make SBC call routing decisions based on information stored on a third-party, LDAP server (such as Microsoft's Active Directory). This feature was supported in previous releases only by the Gateway/IP-to-IP application.

To support this feature, a new option, [7] LDAP has been added to the 'Destination Type' field of the IP-to-IP Routing table. In addition, the LDAP server parameters, supported by the Gateway/IP-to-IP applications in the previous release are also now applicable to SBC.

Applicable Products: E-SBC Series.

3.1.4.28 Least Cost Routing

This feature provides support for least cost routing (LCR) for SBC calls. In LCR, the device selects the IP-to-IP routing rule based on lowest call cost. In the previous release, LCR was applicable only to the Gateway/IP-to-IP application.

To support this feature, the LCR tables are now also applicable to the SBC application and include the following:

- Routing Rule Groups Table – enables LCR
- Cost Group Table – configures Cost Groups, each defining fixed call connection cost and a call rate (charge per minute)
- Time Band table - configures time bands for Cost Groups. The time band defines the day and time range for which the time band is applicable as well as the fixed call connection charge and call rate per minute for this interval.

In addition, a new field, 'Cost Group' has been added to the IP-to-IP Routing table to assign Cost Groups to the routing rules:

Cost Group	Assigns a Cost Group, defined in the Cost Group table, to

[IP2IPRouting_CostGroup]	the routing rule for determining the cost of the call. By default, no (None) Cost Group is assigned to the rule.

Applicable Products: E-SBC Series.

3.1.4.29 SBC Call Forking Modes

This feature provides support for sequential forwarding of all SIP 18x responses received in response to the INVITE-initiating SIP UA for call forking. If 18x arrives with an offer only, the first offer is forwarded to the INVITE-initiating UA. Up until this release, only the first received 18x response was forwarded to the SIP UA that initiated the INVITE.

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

SBC Forking Handling Mode CLI: sbc-forking-handling-mode [SBCForkingHandlingMode]	Defines the handling of 18x responses received due to call forking of an INVITE. • [0] Latch On First = (Default) Only the first 18x is forwarded to the INVITE-initiating UA. If SIP 18x with SDP is received, the device opens a voice stream according to the received SDP and disregards any subsequent 18x forking responses (with or without SDP). If the first response is 180 without SDP, the device responds according to the PlayRBTone2TEL parameter and disregards the subsequent forking 18x responses. • [1] Sequential = All 18x responses are forwarded, one at a time (sequentially) to the INVITE-initiating UA. If 18x arrives with an offer only, then only the first offer is forwarded to the INVITE-initiating UA (and subsequent 18x responses are discarded).

Applicable Products: E-SBC Series.

3.1.4.30 Enhanced Anti-Tromboning for LAN UAs and WAN IP PBX

This feature provides support for anti-tromboning (or non-media anchoring) between UAs in the same network when a hosted IP PBX in the WAN is implemented. Thus, RTP media flows directly between the UAs without traversing the SBC.

By default, media packets traverse the SBC device. This is done in order to:

- Solve NAT problems
- Enforce media security policy
- Perform media transcoding between the two legs
- Media monitoring

However, since media packets traverse the SBC, media quality may degrade (due to, for example, delay).

In some setups, specific calls do not require media anchoring, for example, when there is no need for NAT, security, or transcoding. This is typical for calls between users in the LAN:

- Internal LAN calls: When the SBC routes a call between two UAs within the same LAN, the SBC can forward the SDP directly between caller and callee, and direct the RTP to flow between the UAs without traversing the SBC.
- Internal LAN calls via WAN: In this setup, the SBC dynamically identifies that the call is between UAs located in the same network (i.e., LAN) and thereby, directs the RTP to flow between these UAs without traversing the SBC.

Applicable Products: E-SBC Series.

3.1.4.31 SRTP Sessions without DSP Channel Resources

This feature provides support for SRTP sessions without using DSP channel resources. Up until this release, the E-SBC utilized one DSP channel for SRTP sessions. As a result of this feature, the following benefits are provided:

- Maximum number of SRTP-RTP sessions has been increased
- More DSP resources are now readily available for other functionalities such as transcoding

Applicable Products: Mediant 1000B MSBR; Mediant 1000B Gateway & SBC.

3.1.4.32 MKI Length Negotiation for SRTP-to-SRTP Calls

This feature provides support for enabling Master Key Identifier (MKI) length negotiation in SRTP flows between SIP networks (i.e., IP Groups). This includes the capability of modifying the MKI length on the inbound or outbound SBC call leg.

To support this feature, the following new parameters have been added to the IP Profile table:

[IpProfile_SBCEnforceMKISize]	Enables MKI length negotiation for SRTP-to-SRTP flows. • [0] Disable = (Default) Device forwards the MKI size as is. • [1] Enable = Device changes (overrides) the MKI length according to the settings of the IP Profile table field, MKISize.
MKI Size [IpProfile_MKISize]	Defines the size (in bytes) of the MKI in SRTP Tx packets. The valid values are -1, and 0 to 4. The default value is -1 (i.e., does not modify MKI size).

Applicable Products: E-SBC Series.

3.1.4.33 Notification of Expired User Registration to SIP Proxy / Registrar

This feature provides support for automatically notifying SIP Proxy / Registrar servers of users registered in the E-SBC database whose registration timeout has expired. When a user's registration timer expires, the E-SBC removes the user record from its Registration database and sends an unregister notification (REGISTER message with the Expires header set to 0) to the Proxy/Registrar.

This feature is enabled only if a REGISTER message was sent to an IP Group destination type, configured in the IP-to-IP Routing table.

Applicable Products: E-SBC Series.

3.1.4.34 SBC Classification based on Source URL

This feature provides enhanced support for the classification process based on source URL of incoming calls. When source URL is used as the classification criteria, the device classifies the incoming call to an IP Group as follows:

- For all SIP requests besides REGISTER, the source URL is taken from the SIP From header. If the From header value is ‘Anonymous’, the source URL is taken from P-Preferred-ID header, and if not exist, it is taken from the P-Asserted-ID header.
- For REGISTER requests, the source URL is obtained from the To header.

This feature also provides the option to determine from which SIP header in the incoming SIP request the device must take the source URL. This is done using a new field, 'Source URI Input' in the IP Group table.

Applicable Products: E-SBC Series.

3.1.4.35 Selectable Header for Matching Rules by Source/Destination URI

This feature provides support for selecting the SIP header of INVITE messages to use for incoming call matching characteristics based on source or destination URIs. This feature can be used for SBC call classification, message manipulation, and call routing. Note that these headers are only used for matching characteristics; the result of the call match, for example, manipulated number is done on the header according to the configured rule.

To support this feature, the following new parameters have been added to the IP Group table:

Source URI Input [IPGroup_SourceUriInput]	Defines the SIP INVITE's header to use for call matching characteristics based on source URIs. ▪ [-1] Not configured (default) ▪ [0] From ▪ [1] To ▪ [2] Request-URI ▪ [3] P-Asserted (first header) ▪ [4] P-Asserted (second header) ▪ [5] P-Preferred ▪ [6] Route ▪ [7] Diversion ▪ [8] History-Info ▪ [9] P-Associated-URI ▪ [10] P-Called-Party-ID ▪ [11] Contact
Destination URI Input [IPGroup_DestUriInput]	Defines the SIP INVITE's header to use for call matching characteristics based on destination URIs. ▪ [-1] Not configured (default) ▪ [0] From ▪ [1] To ▪ [2] Request-URI ▪ [3] P-Asserted (first header) ▪ [4] P-Asserted (second header) ▪ [5] P-Preferred ▪ [6] Route ▪ [7] Diversion ▪ [8] History-Info ▪ [9] P-Associated-URI ▪ [10] P-Called-Party-ID ▪ [11] Contact

For example, assume the following incoming INVITE:

```
INVITE sip:8000@10.33.4.226 SIP/2.0
Via: SIP/2.0/UDP 10.33.4.226;branch=z9hG4bKVEBTDAHSUYRTEXEDEGJY
From: <sip:100@10.33.4.226>;tag=YSQQKXXREVDPYPTNFMWG
To: <sip:8000@10.33.4.226>
Call-ID: FKPNOYRNKROIMEGBSSKS@10.33.4.226
CSeq: 1 INVITE
Contact: <sip:100@10.33.4.226>
Route: <sip:2000@10.10.10.10.10>,<sip:300@10.10.10.30>
Supported: em,100rel,timer,replaces
```

```
P-Called-Party-ID: <sip:1111@10.33.38.1>
User-Agent: Sip Message Generator V1.0.0.5
Content-Length: 0
```

And assume the following configuration:

Classification Table					
Index	Source Username Prefix	Source Host Prefix	Destination Username Prefix	Destination Host Prefix	Source IP Group ID
0	333	-	-	-	1
1	1111	-	2000	10.10.10.10	2

IP Group Table		
IP Group ID	Source URI Input	Destination URI Input
1	-	-
2	P-Called-Party-ID	Route

In this example, a match exists only for Classification rule #1, as the source (1111) and destination (2000) username prefixes match those in the INVITE's P-Called-Party-ID (<sip:1111@10.33.38.1>) and Route (<sip:2000@10.10.10.10.10>) headers, respectively. These headers were selected by the associated IP Group ID 2.

Notes:

- If this feature is configured and the selected SIP header does not exist in the incoming INVITE message, the classification of the message to a source IP Group fails.
- When the E-SBC receives an INVITE as a result of a REFER request or 3xx response, the incoming INVITE must be routed according to the Request-URI. The E-SBC identifies such INVITEs according to a specific prefix in the Request-URI header (configured by the SBCXferPrefix parameter). Thus, in this scenario, the E-SBC ignores the settings of this feature discussed above.

Applicable Products: E-SBC Series.

3.1.4.36 Voice Quality RTCP XR Measurements

This feature provides support for the calculation of voice quality metrics (RTCP XR) of RTP streams in SBC call sessions. These measurements are done by the E-SBC without the utilization of DSP resources. Since DSPs are not required for this functionality, reduction in voice quality is avoided and DSP resources are available for other functionalities requiring DSPs.

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.

Note that this feature was already supported in previous releases by MP-11x, Mediant 600, Mediant 1000 Series, Mediant 2000, and Mediant 3000.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.4.37 RADIUS Accounting CDRs for SBC Calls

This feature provides support for generating Remote Authentication Dial-In User Service (RADIUS) accounting reports (CDRs) for SBC calls. For each SBC call session, the device generates two CDRs, one for each call leg. Up until this release, RADIUS accounting was supported only for the Gateway/IP-to-IP application. The E-SBC now supports the same RADIUS attributes as the Gateway/IP-to-IP calls, except for 'Input/Output octets' and 'Input/Output packets'. In addition, the E-SBC calling-station-id and called-station-id attributes are 'Source URI' and 'Destination URI' (instead of 'Source Phone Number' and 'Destination Phone Number').

Applicable Products: E-SBC Series.

3.1.4.38 Media-Related CDR Reporting Level

This feature provides support for configuring the call stage at which media-related call detail records (CDR) are sent by the device for SBC calls. The E-SBC can send media CDR at the start of the media, upon a change (update) in the media, and at the end of the media.

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

Media CDR Report Level [MediaCDRReportLevel]	▪ [0] None = (Default) No media-related CDR is sent. ▪ [1] End Media = Sends a CDR only at the end of the call. ▪ [2] Start & End Media = Sends a CDR once the media starts. In some calls, it may only be after the call is established, but in other calls the media may start at ringback tone. A CDR is also sent upon termination (end) of the media in the call. ▪ [3] Update & End Media = Sends a CDR when an update occurs in the media of the call. For example, a call starts and a ringback tone occurs, a re-INVITE is sent for a fax call and as a result, a CDR with the MediaReportType field set to "Update" is sent, as the media was changed from voice to T.38. A CDR is also sent upon termination (end) of the media in the call. ▪ [4] Start & End & Update Media = Sends a CDR at the start of the media, upon an update in the media (if occurs), and at the end of the media.

Applicable Products: E-SBC Series.

3.1.4.39 Increase in Maximum Number of IP-to-IP Routing Rules

This feature provides support for an increase in the maximum number of SBC IP-to-IP routing rules from 120 to 200 that can be configured in the IP-to-IP Routing table.

Applicable Products: E-SBC Series.

3.1.5 New SIP Application

This section describes the new applications.

3.1.5.1 Cloud Resilience Package Application

This feature introduces a new application on the device referred to as Cloud Resilience Package (CRP). The CRP application, based on the SBC functionality, provides branch offices with call routing and survivability support similar to the existing SAS application. This application is implemented in a network topology whereby the device is located at the branch office, routing calls between the branch users themselves and/or between the branch users and other users located elsewhere (at headquarters or other branch offices), through a hosted server (IP PBX) located at the Enterprise headquarters. The device maintains call continuity even if a failure in communication with the hosted IP PBX occurs. It does this by using its Call Survivability feature, enabling the branch users to call one another or make external calls through the device's PSTN gateway interface.

One of the main advantages of the CRP application is that it enables quick-and-easy configuration setup. This is accomplished by providing pre-configured routing entities, whereby the customer only needs to minimal configuration such as IP addresses to get the device up and running and deployed in the network.

The pre-configured routing entities include IP Groups and IP-to-IP Routing rules. The CRP provides the following pre-configured IP Groups (in the IP Group table):

Index	Description	Type
1	"Users"	User
2	"Proxy"	Server
3	"Gateway"	Server

These IP Groups cannot be deleted and new IP Groups cannot be added. These IP Groups can be edited, except for the fields listed in the above table. The Users-Group denotes the LAN users (e.g., IP phones) at the branch office; the Server-Group denotes the server (e.g., hosted IP PBX at headquarters); the Gateway-Group denotes the interface with the PSTN.

The IP-to-IP Routing rules use these IP Groups to indicate the source and destination of the call. The pre-configured rules depend on the selected CRP survivability mode, which can be one of the following:

- Normal mode: Device interworks between the branch users and the IP PBX at headquarters. It forwards all requests (such as for registration) from the branch users to the IP PBX, and routes the calls based on the IP-to-IP routing rules. Note that SIP OPTIONS requests are terminated at the CRP. If communication with the IP PBX fails (i.e., Emergency mode), it routes calls between the branch users themselves and if this fails, it routes the call to the PSTN (if employed). REGISTER and OPTIONS requests are terminated at the CRP.
- Always Emergency: The CRP performs the call routing between the branch users themselves, as if connectivity with the IP PBX has failed. The CRP also registers the branch users in its internal database.
- Auto answer to registrations: This mode is the same as Normal mode, except that the CRP registers the branch users in its internal database instead of forwarding them to the IP PBX.

Figure 1: Always Emergency Mode

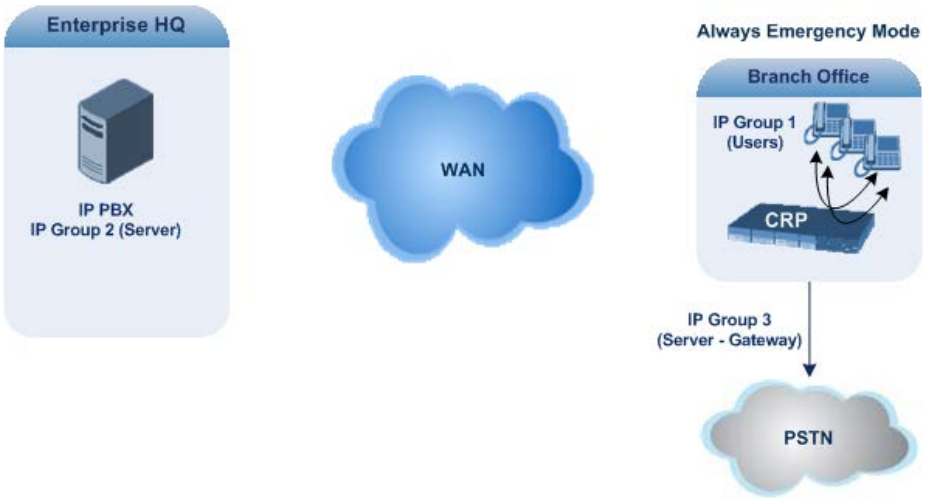
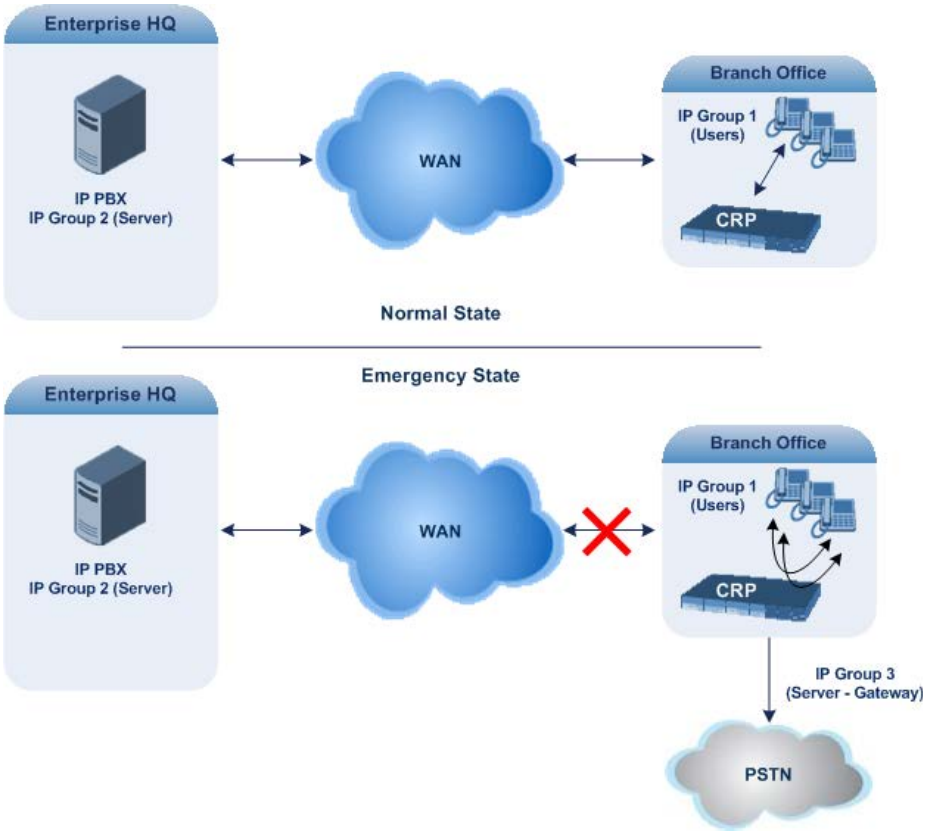


Figure 2: Normal & Auto Answer to Registrations Modes



The pre-configured IP-to-IP routing rules in the IP-to-IP Routing table are as follows, based on selected CRP mode:

Mode	Index	Source IP Group ID	Request Type	Destination Type	Destination IP Group ID	Destination Address	Alternative Route Options
Normal	1	*	OPTIONS	Dest Address	-	Internal	Route Row
	3	1	All	IP Group	2	-	Route Row
	4	1	All	IP Group	1	-	Alternative
	5	1	All	IP Group	3	-	Alternative
	6	2	All	IP Group	1	-	Route Row
	7	3	All	IP Group	2	-	Route Row
	8	3	All	IP Group	1	-	Alternative
Always Emergency	1	*	OPTIONS	Dest Address	-	Internal	Route Row
	2	*	REGISTER	Dest Address	-	Internal	Route Row
	4	1	All	IP Group	1	-	Route Row
	5	1	All	IP Group	3	-	Alternative
	8	3	All	IP Group	1	-	Route Row
Auto Answer to Registrations	1	*	OPTIONS	Dest Address	-	Internal	Route Row
	2	*	REGISTER	Dest Address	-	Internal	Route Row
	3	1	All	IP Group	2	-	Route Row
	4	1	All	IP Group	1	-	Alternative
	5	1	All	IP Group	3	-	Alternative
	6	2	All	IP Group	1	-	Route Row
	7	3	All	IP Group	2	-	Route Row
	8	3	All	IP Group	1	-	Alternative

To enable this feature, the following is required:

- Feature Key: The installed Software License Key must include the CRP feature and the defined number of sessions.
- The CRP application must be enabled in the Applications Enabling page.

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

Web: CRP Application CLI: enable-crp [EnableCRPApplication]	Enables the CRP application. This parameter has been added to the Applications Enabling page and appears instead of the Enable SBC Application parameter. ▪ [0] Disable (default) ▪ [1] Enable Note: A device reset is required for this parameter to take effect.
Web: CRP Survivability Mode CLI: crp-survivability-mode [CRPSurvivabilityMode]	Defines the CRP mode. This parameter appears in the General Settings page. ▪ [0] Standard Mode (default) ▪ [1] Always Emergency Mode ▪ [2] Auto-answer REGISTER

Applicable Products: E-SBC Series.

3.1.6 Media Features

This subsection describes the new media features.

3.1.6.1 Port Overlapping for Media Realms

This feature provides support for configuring Media Realms (in the Media Realm table) with overlapping port ranges. Up until this release, it was invalid to configure multiple Media Realms with overlapping ports.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 2600; Mediant 4000.

3.1.6.2 Overlapping IP Addresses for Network Interfaces

This feature provides support for configuring overlapping IP addresses and subnets for SIP signaling (Control) and media network interfaces. For example, two different network interfaces can be configured in the Multiple Interface table with the same IP address of 10.11.1.1 and subnet 10.11.0.0 (/16). Note that despite overlapping addresses, each network interface must be assigned a unique VLAN ID.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.6.3 SRTP without Capacity Degradation for Analog / BRI Interfaces

This feature provides support for not degrading channel capacity when SRTP sessions are present on analog and BRI interfaces.

Note that this feature was already supported in the previous release by Mediant 8xx Series.

Applicable Products: Mediant 1000B MSBR; Mediant 1000B GW & E-SBC.

3.1.6.4 Network Acoustic Echo Cancellation

This feature provides support of network acoustic echo cancellation (ACE) for SBC calls. Up until this release, ACE was supported only by Mediant 3000.

Acoustic 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).

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

Echo Canceler [IPProfile_EnableEchoCanceller]	Enables echo cancellation per IP Profile. ▪ [0] Disable ▪ [1] Enable (default) = Linear echo, handled by the Line Echo Canceller ▪ [2] Acoustic = Network acoustic echo cancellation
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 - netw = 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).

Note: To support this feature, the Forced Transcoding feature must be enabled in order for the device to use DSPs.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 2600; Mediant 4000.

3.1.6.5 AMR Payload Format – Bandwidth-Efficient / Octet-Aligned

This feature provides support for configuring the AMR payload format type to bandwidth-efficient (in addition to the already supported octet-aligned mode).

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

AMR Octet Aligned [AmrOctetAlignedEnable]	Defines the AMR payload format type. • [0] 0 = Bandwidth-Efficient mode. • [1] 1 = (Default) Octet-Aligned mode.

Note: The Mediant 1000 series and Mediant 2000 support only octet-aligned.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 3000; Mediant 2600; Mediant 4000.

3.1.6.6 DTMF Caller ID Standards Support

This feature provides support for Caller ID generation and detection signaling using DTMF. This DTMF signaling support includes ETSI, Danish, Indian, and Brazilian standards. Up until this release, only FSK signaling (Telcordia, ETSI and NTT) was supported.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 2600; Mediant 4000.

3.1.6.7 CDR and Syslog Field for Automatic Machine Detection

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

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

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

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

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

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

Applicable Products: Mediant 1000 Series; Mediant 2000; Mediant 3000.

3.1.7 Networking Features

This subsection describes the new networking features.

3.1.7.1 Multiple IP Interfaces per VLAN

This feature provides support for configuring multiple IP network interfaces with the same VLAN ID.

Notes:

- The interfaces on the shared VLAN must be configured with IP addresses on the same subnet.
- The first of these interfaces detected by the device with the VLAN ID is considered the "primary" interface.
- Only the "primary" interface's Default Gateway is used.
- Only the "primary" interface may be associated with a static route.
- The interfaces on the shared VLAN must be configured with the same DNS servers.

Applicable Products: Mediant 2600; Mediant 4000.

3.1.7.2 Network Quality Monitoring

This feature provides support for allowing two or more devices to monitor network paths between them in terms of network quality factors. The path monitoring is done by sending packets from a "sender" device to a "responder" device and calculating the round-trip time (RTT), packet loss (PL), and jitter. Since both responder and sender nodes are AudioCodes

devices, the monitoring is done by sending RTP/RTCP packets in a way that accurately predicts the WAN service-level agreement (SLA) granted for real VoIP calls by the network.

The administrator can periodically poll the device for the latest VoIP quality metrics and specify thresholds for the quality metrics mentioned above. If these thresholds are crossed, the device generates the following SNMP traps:

- NqmConnectivityAlarm: Connectivity with monitored probe destination is lost
- NqmRttAlarm: High RTP detected toward probe destination
- NqmJitterAlarm: High jitter detected toward probe destination
- NqmPacketLossAlarm: High packet loss detected toward probe destination

The following CLI commands have been added under the Configuration System mode to support this feature:

- `nqm responder-table` – adds a responder (IP address and port)
- `nqm probing-table` – defines the polling attributes (duration and frequency)
- `nqm sender-table` - adds a sender (including RTT, PL, and jitter thresholds; associates probing definition; responder address; local interface)

Applicable Products: Mediant 500 MSBR; Mediant 800 MSBR; Mediant 850 MSBR.

3.1.7.3 Increase in Maximum Number of VLANs

This feature provides support for up to 48 VLANs.

Applicable Products: Mediant 4000.

3.1.7.4 IPv6 Support for Local DNS

This feature provides support for IP address resolution for Pv6 family in its local Domain Name System (DNS) table. Up until this release, only IPv4 addresses were supported.

Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 3000.

3.1.7.5 Network Time Protocol Server Address by DNS

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

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

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

Applicable Products: All.

3.1.7.6 Disabling ICMP Redirect Messages

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

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

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

Applicable Products: MP-1xx; Mediant 600; Mediant 1000; Mediant 1000B GW & SBC; Mediant 800 GW & SBC; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.7.7 Ethernet Port-Pair Group Tx and Rx Settings

This feature provides support for configuring transmit (Tx) and receive (Rx) settings for the physical ports in a port-pair group for 1+1 physical port redundancy. This feature also enables the association of a physical port (*Port Member*) to an Ethernet Group, where a group can either be assigned one port or two ports for 1+1 redundancy (applicable only to Mediant Software E-SBC).

The port group may be configured in three different modes of operations:

- **1Rx/1Tx:** At any given time, only a single port in the group can transmit and receive. If a link exists on both ports, then the active one is either the first to have a link up or the lower-numbered port if both have the same link up from start. (This option is supported only by Mediant 1000B Gateway & SBC, Mediant 800 Gateway & SBC, Mediant 2600, and Mediant 4000).
- **2Rx/1Tx:** Both ports in the group can receive, but only one port can transmit. The transmitting port is determined by the equipment without acknowledging the user.
- **2Rx/2Tx:** Both ports in the group can receive and transmit.

To support this feature, the following new table has been added (Configuration tab > VoIP menu > Network > Ethernet Group Settings):

Ethernet Group Settings [EtherGroupTable]	FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2; [\EtherGroupTable] Where: ▪ Group = The Ethernet port-pair group. ▪ Mode = The mode of operation: ✓ [2] 1RX/1TX ✓ [3] 2RX/1TX ✓ [4] 2RX/2TX ▪ Member1 = First port in the group. ▪ Member2 = Second port in the group. Note: For the settings to take effect, a device reset is required.

Applicable Products: Mediant 1000B GW & SBC; Mediant 800 GW & SBC; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.7.8 Display of Physical Ethernet Port to Logical Port Mapping

This feature provides support for viewing the mapping of the physical Ethernet ports to the logical, ports used in the device's management tools (e.g., Web interface). The MAC address of the physical port and its status (up / down) is displayed with its corresponding logical port (e.g., "GE_1", "GE_2", "GE_3", or "GE_4").

A new CLI command **show voip ports** has been added to support this feature. Below shows an example of the results of running this command:

```
# show voip ports

 Port Num    Port Name      MAC Address      Link Status
----------  -----------  -----------------  -------------
 1           GE_1        00:1e:67:11:7c:29   UP
 2           GE_2        68:05:ca:03:6b:4e   DOWN
 3           GE_3        68:05:ca:03:6b:98   DOWN
 4           GE_4        00:1e:67:11:7c:28   DOWN
```

Applicable Products: Mediant SW E-SBC.

3.1.7.9 OAMP Services through Data-Router Interface

This feature provides support for configuring whether OAMP services (such as Syslog, Web-based management, and NTP) are accessible through the data-router interface or VoIP interface. By default, access to these services is through the data-router interface (not through the VoIP interface as in previous releases).

A new CLI command has been added to support this feature:

```
# configure system
# default-oam-services-interface <data | voip>
```

Notes:

- To maintain backward compatibility for devices upgraded to Version 6.6 from an earlier version (e.g., Version 6.4), access to OAMP services is through the VoIP interface. In other words, **default-oam-services-interface** is set to **voip**. However, if the device is later reset to factory defaults (e.g., using the **write factory** CLI command), access to OAMP services is through the data-router interface (which is the default). In other words, **default-oam-services-interface** is set to **data**.
- It is highly recommended for devices installed with a Software Feature Key with data-routing functionality enabled but which are deployed only for SBC / Gateway functionality, that their Software Feature Key be replaced to ensure that access to OAMP services is through the VoIP interface by default. Please contact your AudioCodes representatives for more information.

Applicable Products: MSBR Series.

3.1.7.10 Increase in Maximum Number of Supported Network Interface Cards

This feature provides an increase in the number of supported Network Interface Cards (NIC) to four (from two in the previous release). As a consequence, up to four port groups can be configured (where each group has only a single port member) or up to two port-pair groups can be configured for 1+1 LAN port redundancy.

Applicable Products: Mediant SW E-SBC.

3.1.8 Data-Router Features

This subsection describes the new data-router features.

3.1.8.1 DHCP Server Options

This feature provides support for Dynamic Host Configuration Protocol (DHCP) server options. DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that are stored in the Options field of the DHCP message. The data items themselves are also called options. The current set of DHCP options are documented in RFC 2131, Dynamic Host Configuration Protocol.

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

```
option [DHCP option code] ascii [ASCII string]
option [DHCP option code] hex [hexadecimal string]
option [DHCP option code] ip |IP address]
```

The following example configures DHCP option 72, which specifies the Web server 172.16.3.252 for DHCP clients:

```
option 72 ip 172.16.3.252
```

Applicable Products: MSBR Series.

3.1.8.2 DHCP Client Option 121

This feature provides support for Dynamic Host Configuration Protocol (DHCP) client option 121, according to RFC 3442 ((Classless Static Route). This feature enables the device to accept Option 121 in the DHCP response, which defines static routes for the device, from a DHCP server.

Applicable Products: MSBR Series.

3.1.8.3 Wi-Fi Interface

This feature provides support for an optional, customer-ordered Wi-Fi interface, providing wireless LAN 802.11n access point at 2.4 and 5 GHz, integrated 2 Tx / 2 Rx (Mediant 500 MSBR) and 3 Tx / 3 Rx (Mediant 800/850 MSBR), enabling data rates of up to 300 Mbps. The Wi-Fi interface also supports 802.11b/802.11g backward compatibility, allowing interoperability of multiple devices with different types of Wi-Fi 802.11 standards.

A new CLI command, `interface dot11radio` has been added to support this feature.

Applicable Products: Mediant 500 MSBR; Mediant 800 MSBR; Mediant 850 MSBR.

3.1.8.4 Multiple WAN Backup

This feature provides support for configuring LAN-side VLANs as WAN interfaces and assigning up to three WAN interfaces (e.g., optic fiber, VDSL, and 3G modem) to a backup WAN group. Priorities can be assigned to each WAN interface in the group, where priority 1 is the primary WAN interface. If this WAN fails, the device uses the WAN interface assigned with priority level 2, and so on. Only one of the group's WAN interfaces is active at any given time.

This feature can only be configured using the CLI, and with the following existing commands: `backup-group` and `backup monitoring group`.

Applicable Products: MSBR Series.

3.1.8.5 Two IP Addresses per Interface

This feature provides support for configuring up to two IP addresses per interface.

A new CLI parameter, `secondary` has been added to the existing `ip address` command to support this feature. This command is used with the existing `ip address` command.

Below shows a configuration example of two IP addresses for VLAN ID 6:

```
(conf-if-VLAN 6)#ip address 10.4.2.3 255.255.0.0
(conf-if-VLAN 6)#ip address 10.4.2.1 255.255.0.0 secondary
```

Applicable Products: MSBR Series.

3.1.8.6 LAN-WAN Bridging

This feature provides support for Ethernet bridging between LAN and WAN connections. LAN VLANs, WAN Ethernet, VLANs on WAN Ethernet, and Ethernet-over-ATM (supported on DSL connections) may be added to bridge groups.

This feature can only be configured using the CLI, using the new CLI command, `bridge-group`. This command is used in each interface's context, followed by configuration of a bridge virtual interface (BVI). Note that the BVI interface matching the bridge-group number must be in "no shutdown" mode for bridging to function.

Applicable Products: MSBR Series.

3.1.8.7 PPP Unnumbered Interface

This feature provides support for PPP interfaces to be unnumbered such that the IP address negotiated by PPP is borrowed from one of the LAN addresses.

This feature can be configured using only the CLI, with the existing `ip unnumbered` CLI command.

Applicable Products: MSBR Series.

3.1.8.8 Route Tracking using ICMP Ping

This feature provides support for configuring (using the CLI) tracking objects to periodically track the availability (reachability) of any network element, using ICMP (ping). This can be used to test the integrity of a user-defined destination route (IP address) from one of the device's source network interfaces, and if network connectivity fails, the device can use a different routing destination. This can typically be used for WAN redundancy, whereby the device checks the current WAN connection and if it fails, switches to the standby WAN interface.

A new CLI command, `track` was added to support this feature:

```
config)# track <id> IcmpEcho <ip destination address> <source
interface> [interval <value>] [retries <value>]
```

It is also possible to configure a static route which is only used if the state of the tracking object is up. To track a static route, the following CLI command is used:

```
(config)# ip route <dst> <mask> <gw> <interface> [<metric>] [track
<id>]
```

Applicable Products: MSBR Series.

3.1.8.9 WAN Configuration in NAT Translation Table if Multi-VRFs

The Multiple Interface table defines the CMX local VoIP interfaces (OAMP, control, and media). The CMX module is connected to the RMX module through a single internal interface. The RMX, as with any other router can operate in Route mode and NAT mode. When operating in NAT mode, the VoIP applications running on the CMX should know the NAT'ed IP address so that it can be assimilated in the signaling negotiation. Moreover, the RMX should be configured to perform port forwarding and static NAT binding to ensure

communication from and to the VoIP application. An additional complication is when the NAT'ed IP address is dynamically acquired (DHCP), the application should be notified of every change in the IP address.

To overcome the above mentioned issues, the device provides the following configuration:

- The physical WAN interface is selected by the user on which to convey the VoIP-WAN data ('WAN Interface Name' field in the Multiple Interface table).
- The reserved string, "WAN" is used to denote the NAT'ed IP address for SIP interfaces (SIP Interface table) and media interfaces (Media Realm table).
- Static NAT and port forwarding are done automatically by the application.

The above is applicable when there is no need to separate data and VoIP on the RMX, and only one (main) Virtual Routing and Forwarding (VRF) is configured on the RMX.

When data and VoIP are separated by VLANs, the RMX needs to be configured with multiple VRFs and the data VRF must be configured as the main VRF. As the "automated" mechanism of WAN configuration including static NAT and port forwarding are valid only for the main VRF, for multiple VRFs the user must configure port forwarding and NAT binding, and the linkage to the NAT'ed IP address. In summary, the user must configure the following:

- VRF for VoIP and Data
- VoIP LAN interfaces (OAMP, Control, and Media) in the Multiple Interface table that are related to the VoIP VRF
- VoIP WAN physical interface in the 'WAN Interface Name' field of the Multiple Interface table
- RMX, static NAT, and port forwarding
- In the NAT Translation table, bind the reserved string, "WAN" and an interface that has been configured in the Multiple Interface table

Applicable Products: MSBR Series.

3.1.9 Quality of Experience Features

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

3.1.9.1 Session Experience Manager (SEM) Product Support

The AudioCodes SEM application is now supported by MP-1xx, Mediant 2000, Mediant 2600, and Mediant 4000 E-SBC. Up until this release, it was supported only by Mediant 8xx Series, Mediant 1000 series, and Mediant 3000.

Note that SEM is not supported by Mediant 500 MSBR and Mediant Software E-SBC.

Applicable Products: Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.9.2 Bandwidth Management per Media Realm

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

This feature defines the following states for bandwidth utilization:

- Normal
- High
- Critical

The bandwidth threshold, defined in bytes per second, and hysteresis for each state can be configured, as well as the corresponding action that the device must perform upon transitions between bandwidth states. Up to two thresholds can be configured, one for each

state transition, that is, Normal-High state change and High-Critical state change. The desired action upon exceeding a user-defined threshold can be one of the following:

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

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

Bandwidth Management Table [BWManagement]	Defines bandwidth management rules per Media Realm. [BWManagement] FORMAT BWManagement_Index = BWManagement_MediaRealmIndex, BWManagement_ThresholdIndex, BWManagement_RuleAction, BWManagement_Threshold, BWManagement_Hysteresis; [\BWManagement] Where: ▪ MediaRealmIndex: Related Media Realm ▪ ThresholdIndex: Index of bandwidth threshold rule: ✓ [0] High Threshold Rule. ✓ [1] Critical Threshold Rule ▪ RuleAction: ✓ [0] Report Only (default) ✓ [1] No more calls ▪ Threshold: Bandwidth threshold in Bps ▪ Hysteresis: Fluctuation (change) from threshold value at which the device executes the action

Applicable Products: Mediant 1000 Series; Mediant 8xx Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000.

3.1.9.3 New Voice Quality Parameters for Reporting to SEM

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

The following additional voice quality parameters can now be monitored:

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

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

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

Applicable Products: Mediant 1000 Series; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.10 High-Availability Features

This subsection describes the new High-Availability (HA) features.

3.1.10.1 Monitoring IP Entity and HA Switchover upon Ping Failure

This feature provides support for monitoring a network entity by ping and performing a switchover to the redundant device if no ping response is received. A switchover occurs only if the ping was successful and then fails in any subsequent ping. The network entity is defined by IP address and the interface from which the ping is sent is done from one of the device's configured network interfaces in the Multiple Interface table. This feature can be used, for example, to check the connectivity with a nearby router (first hop) that the device uses to reach other destinations.

To support this feature, the following new parameters have been added to the existing HA Settings page:

Enable HA Network reachability [HAPingEnabled]	Enables the pinging of an active IP network destination in HA mode to test reachability from one of the device's IP network interfaces. If no reply is received from the ping, a switchover occurs to the redundant device. ▪ [0] Disabled (default) ▪ [1] Enabled
HA Network reachability destination address [HAPingDestination]	Defines the IP address of the destination that the device is to ping. The default is 0.0.0.0.
HA Network reachability source If name [HAPingSourceIfName]	Defines the device's IP network interface from where the ping is sent. The valid value is the name of the interface, as configured for the 'Interface Name' field in the Multiple Interface table. By default, no IP network is defined.
HA Network reachability ping timeout [HAPingTimeout]	Defines the timeout (in seconds) for which the ping request waits for a reply. The valid value is 1 to 60. The default is 1.
HA Network reachability ping retries [HAPingRetries]	Defines the number of ping requests that the device sends after no response from the destination, before the destination is declared unavailable. For example, if you specify 2, the destination will be declared as down after three consecutive ping requests fail to evoke a response from the destination. The valid value is 0 to 100. The default 2.
Monitor Destination Status - read only section	(Read-only) Displays the status of the connectivity to the pinged destination: ▪ "Disabled by configuration and HA state" – HA and ping are not configured. ▪ "Disabled by HA state" – same as above ▪ "Disabled by configuration" – same as above ▪ "Disabled by invalid configuration." – Invalid configuration, for example, invalid interface name or destination address (address must be different from a local address and from the redundant unit's Maintenance address) ▪ "Disabled by HA priority in use" – When HA priority is used, ping mechanism is disabled ▪ "Disabled by Eth groups error" – When number of Ethernet

	Groups in the redundant unit becomes less than in active unit, the ping mechanism is disabled. ▪ "Failed to be activated" – Internal error (failed activating the ping mechanism) ▪ "Enabled" – Ping is sent as configured Ping statistics are displayed if the service is running.

Note: The ping feature is not functional under the following conditions:

- HA is disabled (active unit is in standalone mode)
- HA Priority is used (to prevent endless loops of switchovers)
- Number of Ethernet Groups in the redundant unit that are in "up" state are less than on the active unit (to prevent endless loops of switchovers)

Applicable Products: Mediant 2600; Mediant 4000 HA.

3.1.10.2 Redundant Device Display on Web Home Page of Active Unit

This feature provides support for displaying both active and redundant devices on the Home page of the active device when High Availability (HA) mode is implemented. The active device is displayed with a green border and in addition, each device is labeled with its name, configured by the following new parameter added to the HA Settings page:

HA Device Name [HAUnitIdName]	Defines a name for the device. This name is displayed on the Home page to indicate the active device. The valid value is a string of up to 128 characters. For the default value, the device assigns either "Device1" or "Device2", such that active and redundant devices will have different default names.

The graphical display of the redundant device shows the status of its LAN ports, which if clicked opens the redundant device's Ethernet Port Information page.

Applicable Products: Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.10.3 New Trigger for E-SBC Device Switchover

This feature provides support for an additional trigger for HA switchover. If one or more physical network groups (Ethernet port link pair) of the active E-SBC disconnects (i.e., no link) and these physical network groups are connected OK on the redundant E-SBC, then a switchover occurs from the active to redundant E-SBC.

Applicable Products: Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.10.4 Automatic Snapshot of Redundant upon Snapshot of Active

This feature provides support for automatically creating a snapshot of the redundant E-SBC when taking a snapshot of the active E-SBC.

Applicable Products: Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.11 PSTN Features

This subsection describes the new PSTN features.

3.1.11.1 B-Channel Restart

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

Notes:

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.11.2 DS1 Byte-synchronous Mapping to VT1.5 (SONET / OC3)

This feature provides support for mapping DS1 signals into a VT1.5, using byte-synchronous mapping.

To enable this feature, the existing parameter, SDHFbrGrp_Mapping_Type must be set to [2]:

Mapping Type [SDHFbrGrp_Mapping_Type]	Determines the SDH/SONET mapping type (signal label and payload mapping type) for the PSTN interface. This is selected per Fiber Group. • [0] VT1.5 Asynchronous = Asynchronous VT1.5 and DS1. • [1] TU-12 Asynchronous = Asynchronous TU12 and E1. • [2] TU-11 Byte Synchronous = TU-11 Byte Synchronous mapping. • [3] Asynchronous DS3 = Asynchronous mapping of DS3 in STS1, DS3 channelized to DS1's - asynchronous mapping of channelized DS3 to OC-3, so that the actual interface is OC-3 but mapped to three DS3 trunk interfaces (DS1 > DS3 > STS-1 > OC-3). • [15] UNDEFINED = (Default) Not defined. Notes: • For this parameter to take effect, a device reset is required. • The setting of this parameter must be in coordination with the parameters SDHFbrGrp_SDHSONETMode and ProtocolType. • This parameter is applicable only when TDMBusType is set to acFRAMERS (2) and PSTNTransmissionType set to Optical SONET or SDH Transmission type(1). • When option [3] is selected, the DS3 clock source is automatically set to 'Local Board' (i.e., synchronization supplied by device) and cannot be changed.

Applicable Products: Mediant 3000 with TP-6310.

3.1.11.3 Manual D-Channel Switchover

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

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.12 Infrastructure Features

This subsection describes the new infrastructure features.

3.1.12.1 FXS Line Testing

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

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

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

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

or

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

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

- 0 for line status
- 1 for line measurements

Applicable Products: MP-124.

3.1.12.2 USB Storage

This feature provides support for USB storage capabilities using an external USB hard drive or flash disk (disk on key) connected to the device's USB port. The storage capabilities include the following:

- Saving network captures to the USB (applicable only to Mediant 500/800 MSBR). This is done using the new CLI parameter, `usb`:

  ```
  debug capture data physical stop usb
  ```

- Updating the device's firmware from the USB. This is done using the new CLI parameter, `firmware from usb`:

  ```
  copy firmware from usb://firmware.cmp
  ```

- Updating the device's configuration from the USB. This is done using the new CLI parameter, `voice-configuration from usb`:

  ```
  copy voice-configuration from usb://board.ini
  ```

- Saving current configuration to the USB. This is done using the new CLI parameter, `voice-configuration to usb`:

  ```
  copy voice-configuration to usb://board.ini
  ```

Note that only a single USB storage (formatted to FAT/FAT32) operation is supported at any given time.

Applicable Products: Mediant 500; Mediant 8xx Series.

3.1.12.3 New Format for Configuring Daylight Saving Time Period

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

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

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

Applicable Products: All.

3.1.12.4 IEEE 802.3at for Power over Ethernet

This feature provides support for Power over Ethernet (PoE) according to the IEEE 802.3at standard. This supports various power budgets - 200 Watt, 120 Watt, and 50 Watt. This feature is in addition to the IEEE 802.3af-2003 standard. When a PoE port is configured as Class 4 (i.e., 802.3at) it can deliver up to 30 Watts to the connected equipment.

A new field, 'AT Enable' has been added to the Power Over Ethernet Settings table to enable 802.3at Class 4:

Power over Ethernet Settings [POETable]	This table enables PoE per LAN port and configures the maximum power consumption allowed per port for PoE-enabled clients connected to it. [POETable] FORMAT POETable_Index = POETable_PortEnable, POETable_PortPower, POETable_PortATEnable; [\POETable]

Applicable Products: Mediant 850 MSBR.

3.1.13 General Management Features

This subsection describes the new general management features.

3.1.13.1 Zero Configuration using AudioCodes HTTPS Redirect Server

This feature provides support for Zero Configuration, enabling automatic, remote configuration of newly deployed, non-configured devices, using AudioCodes HTTPS Redirect Server. This feature offers an almost plug-and-play experience for quick-and-easy deployment of multiple devices at the end-customer premises.

The Zero Configuration feature requires only minimal configuration of the device to setup WAN connectivity. Once an Internet connection is established, all that is needed is a device reset to activate the Zero Configuration mechanism.

Once the device is powered up and connectivity to the WAN is established, it automatically sends an HTTP request to AudioCodes HTTPS Redirect server. If the device's MAC address is listed at the server, the server responds to the device with an HTTP Redirect response that contains the URL of the server (typically, a provisioning server maintained by

the Service Provider) where the configuration file is located. The device then downloads the configuration file from this provisioning server and updates its configuration.

The configuration file contains only CLI commands for configuration, which its settings are applied to the device, in addition to the device's current configuration. The device resets only if the configuration file contains an explicit command instructing it to reset.

To enable Zero Configuration, the customer needs to define the device on the HTTPS Redirect server by entering its MAC address and the configuration file URL. This may be done either through the corresponding Web interface or through SOAP/XML interface (that may be integrated with the Service Provider's provisioning system). For more information, contact AudioCodes support.

If the auto-provisioning process succeeds, the device will only repeat the Zero Configuration process if it undergoes a reset to factory defaults. If the process fails, the device will repeat this process at the next device reset or power up.

For security purposes, communication between the device and the HTTPS Redirect server is encrypted (HTTPS) and setup with mutual authentication. The device uses a special factory-set certificate to authenticate itself with the HTTPS Redirect server and to verify authenticity of the latter. If the re-direct URL (where the configuration file is stored) also uses the HTTPS protocol, the device can use a regular certificate or the Zero Configuration certificate to authenticate itself and validate the server's certificate if a trusted root certificate (regular) is configured.

Notes:

- If the regular Automatic Update feature has been configured, Zero Configuration is performed prior to starting the Automatic Update process. Only once Zero Configuration completes (successfully or not), does the Automatic Update process begin.
- If the device is configured with multiple WAN interfaces, Zero Configuration is attempted on all configured WAN interfaces, sequentially.
- The recommended method for using both Zero Configuration and Automatic Update is as follows:
  1. Zero Configuration is done to redirect the non-configured device to the URL of the provisioning server that contains the configuration of Automatic Update **only** (CLI script URL and timeout for periodic check).
  2. Once the Zero Configuration process completes (i.e., Automatic Update configuration is applied to the device), without undergoing a reset, the Automatic Update mechanism begins.

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

CLI: configure system > automatic-update > set zero-conf on|off	Enables the Zero Configuration feature. ▪ on (default) ▪ off
configure system > automatic-update > set zero-conf-server <url>	Defines the URL of AudioCodes HTTPS Redirect server. The valid value is a string of up to 256 characters. The default is: https://redirect.audiocodes.com/<MAC address>

Applicable Products: MSBR Series.

3.1.13.2 Automatic Update using Zero Configuration Certificate

This feature provides support for enabling the regular Automatic Update feature to use the same client-server certificate as used for the Zero Configuration feature instead of the "regular" certificate used for Automatic Update.

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

CLI: auto-update-use-zero-conf-certs [AupdUseZeroConfCerts]	Enables the device to use the same certificate for Automatic Update feature as used for Zero Configuration. ▪ [0] = (Default) The device uses the "regular" certificate

	for Automatic Update. ▪ [1] = The device uses the Zero Configuration certificate for the Automatic Update feature.

Applicable Products: MSBR Series.

3.1.13.3 Automatic Update using CLI Scripts

This feature provides support for automatically provisioning the device using CLI scripts, enabling automatic provisioning for the device's Data-Routing functionality as well. Up until this release, automatic provisioning could only be done using an ini file, which supports only System and VoIP configuration. The CLI script file contains the regular CLI commands for configuring the System, VoIP, and Data-Routing functionalities.

Two different types of CLI script files can be used, the only difference being in the way they configure the device:

- **CLI script file:** This file updates the device's configuration **only** according to the file's configuration settings. The device's other existing configuration settings (not included in the file) are retained.
- **Startup CLI script file:** This file updates the device's configuration according to the file's configuration settings and sets all other parameters (not included in the file) to factory defaults. (This script file causes two device resets.)

Once one of these files is created with the desired device configuration and stored on a provisioning server, the device retrieves the file from the URL of the server, configured using the following new *ini* file parameters:

[AUPDCliScriptURL] CLI: copy cli-script from <URL>	Defines the URL of the server where the CLI Script file containing device configuration is located. This file is used in automatic provisioning.
[AUPDStartupScriptURL] CLI: copy startup-script from <URL>	Defines the URL of the server where the CLI Startup Script file containing device configuration is located. This file is used in automatic provisioning.

The following new CLI command can be included in the CLI script files:

- **`reload if-needed`**: Resets the device if configuration changes require this for the new settings to take effect. This command must be added at the end of the CLI script file.

Applicable Products: MSBR Series.

3.1.13.4 Automatic Update through WAN Interface

This feature provides support for enabling automatic update through any WAN interface configured on the device. Up until this release, automatic update was possible only through the LAN interface.

Applicable Products: MSBR Series.

3.1.13.5 Configuration of Automatic Update using CLI

This feature provides support for configuring (enabling) the Automatic Update feature using the device's CLI. Up until this release, the Automatic Update feature could only be configured using the ini file.

To support this feature, the **`automatic-update`** CLI command has been added under the System mode, with the following optional sub-commands:

```
#(automatic-update)# set
  call-progress-tones  ; Defines URL of Call Progress Tone file
```

```
cas-table             ; Defines URL to CAS table file
cli-script            ; Defines URL to CLI script file
coder-table           ; Defines URL to Coder table file
crc-check             ; Enables CRC for Configuration files
data-configuration    ; Defines URL of Data configuration file
dial-plan             ; Defines URL of Dial Plan file
firmware              ; Defines URL of CMP file
prerecorded-tones     ; Defines URL of Prerecorded Tone file
startup-script        ; Defines URL of Startup script file
tls-cert              ; Defines URL of TLS certificate file
tls-private-key       ; Defines URL of TLS private key file
tls-root-cert         ; Defines URL of TLS root CA file
voice-configuration   ; Defines URL of Voice configuration file
voice-prompts         ; Defines URL of Voice Prompts file
voice-xml             ; Defines URL of Voice XML file
zero-conf             ; Described previously for Zero Conf
zero-conf-server      ; Described previously for Zero Conf
```

Applicable Products: MSBR Series.

3.1.14 Web Management Features

This subsection describes the new Web interface features.

3.1.14.1 Web Access from Any Interface

This feature provides support for enabling access to the device's Web-based management interface from any of the device's IP network interfaces (i.e., OAMP, Control, and/or Media). If this feature is disabled, Web access can only be done on the OAMP interface. This feature applies to HTTP and HTTPS protocols.

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

Web: Enable web access from all interfaces [EnableWebAccessFromAllInterfaces]	Enables Web access from any of the device's IP network interfaces (i.e., OAMP, Control, and/or Media interfaces). ▪ [0] = (Default) Disable – Web access is only through the OAMP interface. ▪ [1] = Enable - Web access is through any network interface.

Applicable Products: Mediant 800 GW & SBC; Mediant 1000B GW & SBC; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.14.2 Clear History Alarms Table

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

Applicable Products: All.

3.1.14.3 Mozilla Firefox Web Browser Support

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

Applicable Products: All.

3.1.14.4 New Web "Master" User Level

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

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

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

Applicable Products: All.

3.1.14.5 Enhanced Management of Web Users

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

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

- Master User
- Security Administrator
- Admin
- Monitor

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

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

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

Applicable Products: All.

3.1.14.6 New Table Design Format

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

- Power Over Ethernet Settings
- SNMPv3 Users
- Firewall Settings
- IP Security Proposals Table
- IP Security Associations Table
- Physical Ports Table
- Internal DNS Table
- Internal SRV Table

- DSP Templates
- SIP Interface Table
- IP Group Table
- NAT Translation Table
- Destination Phone Number Manipulation Table for IP -> Tel Calls
- Destination Phone Number Manipulation Table for Tel -> IP Calls
- Source Phone Number Manipulation Table for IP -> Tel Calls
- Source Phone Number Manipulation Table for Tel -> IP Calls
- Redirect Number Tel -> IP
- Redirect Number IP -> Tel
- Forward On Busy Trunk Destination
- Tone Index Table
- Admission Control
- Condition Table
- Message Manipulations
- IP to IP Inbound Manipulation
- IP to IP Outbound Manipulation

Applicable Products: All (according to relevant page).

3.1.14.7 Syslog Message Display

This feature provides support for viewing Syslog messages in the Web interface for the MSBR product line (already supported in all other products). A new page, Message Log was added to support this feature. This page is accessed using the following path: **Status & Diagnostics** tab > **System Status** menu > **Message Log**. These Syslog messages are sent from the device's OAMP IP address.

Applicable Products: MSBR Series.

3.1.14.8 New Web Login Screen for Enhanced Security

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

Applicable Products: All.

3.1.14.9 Status Display of D-Channels and NFAS Groups

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

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

Applicable Products: Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

3.1.14.10 Loopback Creation for DS1 Lines

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

Applicable Products: Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

3.1.14.11 Remote Loopback Creation for DS3 Lines

This feature provides support for creating (and removing) remote loopback for DS3 lines. A new button – **Create Loopback** (and **Remove Loopback**) – was added to the Trunk Settings page to support this feature.

Applicable Products: Mediant 3000 with TP-6310.

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

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

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

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

Applicable Products: Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

3.1.14.13 Relocation of Message Policy & Message Manipulations Tables

The Message Policy and Message Manipulations tables are now located under the **SIP Definitions** folder in the Navigation pane. Up until now, they were located under the **SBC** folder. This new location enables message policy and message manipulation configuration for the Gateway/IP-to-IP application, in addition to SBC.

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

3.1.14.14 SS7-Related Web Pages Removed

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

Applicable Products: All.

3.1.14.15 Hotline Duration Configurable in Web

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

Applicable Products: MP-1xx; Mediant 600; Mediant 1000 Series; Mediant 8xx Series.

3.1.15 SNMP Features

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

3.1.15.1 Quality of Service using MIBs

This feature provides support for a new MIB, AC-QOS-MIB that provides SNMP interface for viewing Quality of Service (QoS) related routing configuration and statistics. The following tables are included in this MIB:

- QosMatchMap – each entry represents QoS Match Map
- QosMatch – each entry represents Match statement of Match Map; defines network stream for QoS handling
- QosSet - each entry represents Set statement of Match Map; defines QoS marking and shaping rules applied to the selected network stream
- QosServiceMap – each entry represents QoS Service Map; defines traffic shaping policy for specific network interface
- QosQueue – each entry represents QoS Queue (class)
- QosQueueAction – each entry represents traffic shaping policies applied to the specific QoS Queue
- QosQueueStats – shows statistics of QoS Queue (class)

For a detailed description of each table, refer to the AC-QOS-MIB.

This feature is already supported for CLI, where these tables can be viewed using the `show data qos commands` (`show data qos match-map`, `show data qos service-map`, `show data qos queue`).

Applicable Products: MSBR Series.

3.1.15.2 Information on Physical Configuration

This feature provides support for getting information on the physical configuration of the device, according to RFC 2737. This information includes, for example, installed modules and their chassis slot numbers, and port interface types.

To support this feature, the SNMP EntityPhysical table has been added.

Note that this table is already supported on other products.

Applicable Products: Mediant 500.

3.1.15.3 Encrypted Traps per SNMPv3 User

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

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

Applicable Products: All.

3.1.15.4 New MIB-II Counters

This feature provides support for the following new MIB-II counters:

- TCP:
  - tcpRtoAlgorithm
  - tcpRtoMin
  - tcpRtoMax

- tcpMaxConn
- tcpActiveOpens
- tcpPassiveOpens
- tcpAttemptFails
- tcpEstabResets
- tcpCurrEstab
- tcpInSegs
- tcpOutSegs
- tcpRetransSegs
- tcpInErrs
- tcpOutRsts
- tcpHCInSegs
- tcpHCOutSegs

- UDP:
  - udpInDatagrams
  - udpNoPorts
  - udpInErrors
  - udpOutDatagrams
  - udpHCInDatagrams
  - udpHCOutDatagrams
- IP:
  - ipForwarding
  - ipDefaultTTL
  - ipInReceives
  - ipInHdrErrors
  - ipInAddrErrors
  - ipForwDatagrams
  - ipInUnknownProtos
  - ipInDiscards
  - ipInDelivers
  - ipOutRequests
  - ipOutDiscards
  - ipOutNoRoutes
  - ipReasmTimeout
  - ipReasmReqds
  - ipReasmOKs
  - ipReasmFails
  - ipFragCreate
- ICMP:
  - icmpInMsgs
  - icmpInErrors
  - icmpInDestUnreachs
  - icmpInTimeExcds
  - icmpInParmProbs

- icmpInSrcQuenchs
- icmpInRedirects
- icmpInEchos
- icmpInEchoReps
- icmpInTimestamps
- icmpInTimestampReps
- icmpInAddrMasks
- icmpInAddrMaskReps
- icmpOutMsgs
- icmpOutErrors
- icmpOutDestUnreachs
- icmpOutTimeExcds
- icmpOutParmProbs
- icmpOutSrcQuenchs
- icmpOutRedirects
- icmpOutEchos
- icmpOutEchoReps
- icmpOutTimestamps
- icmpOutTimestampReps
- icmpOutAddrMasks
- icmpOutAddrMaskReps

■ IF:

- ifInOctets
- ifInUcastPkts
- ifInDiscards
- ifInErrors
- ifOutOctets
- ifOutUcastPkts
- ifOutErrors
- ifInMulticastPkts
- ifInBroadcastPkts
- ifOutMulticastPkts
- ifOutBroadcastPkts

Applicable Products: MSBR Series.

3.1.15.5 Restarting B-Channels

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

Applicable Products: Mediant 600; Mediant 1000 Series; Mediant 500 MSBR; Mediant 8xx Series; Mediant 2000; Mediant 3000.

3.1.15.6 ISDN Alarms Consolidation

This feature provides support for consolidating Trunk alarms pertaining to an NFAS group. When a trunk alarm is raised, the D-channel and B-channel alarms are automatically cleared. When the trunk alarm is cleared, the D-channel and B-channel alarms are restored (raised again).

Applicable Products: Mediant 3000.

3.1.15.7 SNMP Alarm for Ethernet Port Redundancy

This feature provides support for a new SNMP alarm, acEthernetGroupAlarm to indicate Ethernet port group (1+1) protection status. This alarm is raised when both ports in the group are down, and cleared when at least one port is up.

Applicable Products: Mediant 800 GW & E-SBC; Mediant 1000B GW & E-SBC.

3.1.15.8 SNMP Trap for TLS Server Certificate Expiry

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

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

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

Applicable Products: MP-1xx; Mediant 500 MSBR; Mediant 8xx Series; Mediant 3000.

3.1.15.9 AudioCodes EMS SNMP-based Management Tool Support

The AudioCodes EMS application is now supported by Mediant 4000 E-SBC (and Mediant 2600). Up until this release, it was supported only by MP-1xx, Mediant 600, Mediant 8xx Series, Mediant 1000 series, Mediant 2000, and Mediant 3000.

Applicable Products: Mediant 2600; Mediant 4000.

3.1.16 CLI Features

This subsection describes the new command-line interface (CLI) features.

3.1.16.1 New show Commands

This feature provides support for the following new show CLI commands that display various statistics and call counters relating to the Gateway (analog and digital PSTN) application:

- **`show voip gw statistics basic-statistics:`** Displays performance monitoring, for example:

```
# show voip gw statistics basic-statistics
 Active TDM channels                  2
 Active DSP resources                 2
 Active analog channels               0
 Active G.711 channels                1
 Average voice delay (ms)             0
 Average voice jitter (ms)            0
 Total RTP packets TX                 125
```

```
 Total RTP packets RX                  140
 Total call attempts                   2
```

- **show voip gw calls-count tel2ip:** Displays various Tel-to-IP call counters, for example:

```
# show voip gw calls-count tel2ip
 Number of attempted calls: 5
 Number of established calls: 5
 Percentage of successful calls(ASR): 100.000000
 Number of calls terminated due to a busy line: 0
 Number of calls terminated due to no answer: 0
 Number of calls terminated due to forward: 0
 Number of calls terminated due to no route: 0
 Number of calls terminated due to no matched capabilities: 0
 Number of calls terminated due to no resources: 0
 Number of calls terminated due to other failures: 0
 Average call duration (ACD) [sec]: 103
 Attempted fax calls counter: 0
 Successful fax calls counter: 0
```

- **show voip gw calls-count ip2tel:** Displays various IP-to-Tel call counters, for example:

```
# show voip gw calls-count ip2tel
 Number of attempted calls: 5
 Number of established calls: 5
 Percentage of successful calls(ASR): 100.000000
 Number of calls terminated due to a busy line: 0
 Number of calls terminated due to no answer: 0
 Number of calls terminated due to forward: 0
 Number of calls terminated due to no route: 0
 Number of calls terminated due to no matched capabilities: 0
 Number of calls terminated due to no resources: 0
 Number of calls terminated due to other failures: 0
 Average call duration (ACD) [sec]: 18
 Attempted fax calls counter: 0
 Successful fax calls counter: 0
```

Applicable Products: MSBR Series.

3.1.16.2 Show VoIP DSP Status Commands

This feature provides support for displaying the VoIP DSP status. To support this feature, the following new CLI commands have been added:

- **show voip dsp perf:** Displays performance monitoring of DSP data, for example:

```
# show voip dsp perf
DSP Statistics (statistics for 144 seconds):
Active DSP resources: 0
Total DSP resources: 76
DSP usage : 0
```

- **show voip dsp status:** Displays the current DSP status, for example:

```
# show voip dsp status
Group:0 DSP firmware:624AE3 Version:0660.04 - Used=60 Free=12
Total=72
  DSP device   0:  Active    Used= 5   Free= 1   Total= 6
```

```
  DSP device   1:  Active    Used= 5   Free= 1   Total= 6
  DSP device   2:  Active    Used= 5   Free= 1   Total= 6
  DSP device   3:  Active    Used= 5   Free= 1   Total= 6
  DSP device   4:  Active    Used= 5   Free= 1   Total= 6
  DSP device   5:  Active    Used= 5   Free= 1   Total= 6
  DSP device   6:  Active    Used= 5   Free= 1   Total= 6
  DSP device   7:  Active    Used= 5   Free= 1   Total= 6
Group:2 DSP firmware:204IM Version:0660.04 - Used=2 Free=2
Total=4
  DSP device  12:  Active    Used= 2   Free= 2   Total= 4
```

Applicable Products: MSBR Series.

3.1.16.3 Enhanced Display of Syslog Messages

This feature provides support for the following additional CLI commands for Syslog messages:

- `# show system log` Displays Syslog history from device startup
- `# show system log tail` Displays the last 10 Syslog messages
- `# show system log tail [n]` Displays the last n Syslog messages

Applicable Products: MSBR Series.

3.1.16.4 PoE Configuration per Port

This feature provides support for configuring a specific port for PoE, using CLI.

A new CLI command was added to support this feature:

```
# (config-system) interface poe-table <port index>
```

Applicable Products: Mediant 800 MSBR; Mediant 850 MSBR.

3.1.16.5 Bridge MAC Table Display

This feature provides support for viewing MAC addresses in the MAC table for a specific bridge interface.

A new CLI command was added to support this feature:

```
# (config-data) show data mac-address-table interface BVI <1-255>
```

Applicable Products: MSBR Series.

3.1.16.6 Software License Key Upgrade

This feature provides support for upgrading the device's Software License Key through the CLI. A new CLI command, `feature-key` has been added to support this feature. This command is run from the **System** CLI mode, as shown below. The entered Software License Key must be enclosed in double apostrophe:

```
(config-system)# feature-key
"r6wmr5to25smaB12d21aiSl94yMCf3lsfjBjagcch1kq9AZ9MJqqCOw44ywFcMlIb
iBaeNcsjh878ld1f2wKbY3IXJj1SOlcbiBfc6FBj1fROlJ9XvAw8k1IXdoFcOpeQJp
2e0sti1s0blNecypomhgU5yTlPREPQtl2e1wpiNgx7lRfeyXV?2s9@coFcOhdayWjW
hQuJeIgb5VbfyENc2w46O6OG3lf7NJnbkF5mxkka5xccyoVedYq1gMc"
```

This feature also supports the display of the currently installed Software License Key (in textual format) through the CLI. A new CLI command, **`show system feature-key`** has been added to support this feature. The Software License Key is displayed in textual format.

Applicable Products: MSBR Series.

3.1.16.7 Display of MAC Addresses on LAN Ports

This feature provides support for displaying MAC addresses discovered by the LAN ports. A new CLI command was added to support this feature:

```
show data mac-address-table count
show data mac-address-table print
clear data mac-address-table
```

Applicable Products: MSBR Series.

3.1.16.8 CLI Command set media-channels Relocated

The `set media-channels` command is now also located under `voip-media general`, for user convenience:

```
# configure voip
(config-voip)# media general
(media-general)# list
Commands available:
    set media-channels
```

In this location, the command is configurable without requiring a Feature Key. In contrast, under the specific CLI location `ip media settings`, it requires a Feature Key.

Changing the value of the command in any location, changes the value in all other locations. For example, if the value configured for the `set media-channels` parameter located under `sbc general-setting` is changed, the value of the parameter under `voip-media general` changes accordingly.

Applicable Products: MSBR Series.

3.1.16.9 Existing INI Parameters now Configurable in CLI

This feature provides support for CLI configuration of the following parameters that up until this release could only be configured using other management tools (e.g., Web interface and ini file):

CLI Command	CLI Path	*ini* File Parameter
p-assrtd-usr-name	re voip/sip-definition advanced-settings	PAssertedUserName
xfer-prefix-ip2tel	config-voip/gw/digitalGW/digital gateway params	XferPrefixIP2Tel
blind-xfer-add-prefix	config-voip/gw/digitalGW/digital gateway params	KeyBlindTransferAddPrefix
blind-xfer-disc-tmo	config-voip/gw/digitalGW/digital gateway params	BlindTransferDisconnectTimeout
etsi-diversion	config-voip/gw/digitalGW/digital gateway params	EnableETSIDiversion
tel2ip-dflt-redir-rsn	config-voip/gw/digitalGW/digital gateway params	Tel2IPDefaultRedirectReason
prfm-ip2tel-dst-manipul	config-voip/gw/manipulations/general setting	PerformAdditionalIP2TELDestinationManipulation
prfm-ip2tel-src-manipul	config-voip/gw/manipulations/general setting	PerformAdditionalIP2TELSourceManipulation
sbc-max-fwd-limit	config-voip/sbc-gnrl-	SBCMaxForwardsLimit

	setting	
sbc-bye-auth	config-voip/sbc-gnrl-setting	SBCEnableByeAuthentication
sbc-direct-media	config-voip/sbc-gnrl-setting	SBCDirectMedia
enablesbcmediasync	config-voip/sbc-gnrl-setting	EnableSBCMediaSync
call-forward	config-voip/gw analoggw	Info
call-waiting-per-port	config-voip/gw analoggw	CallWaitingPerPort
authentication	config-voip/gw analoggw	Authentication
enable-caller-id	config-voip/gw analoggw	EnableCallerID
caller-display-info	config-voip/gw analoggw	CallerDisplayInfo
targetofchannel	config-voip/gw analoggw	TargetOfChannel

Applicable Products: MSBR Series.

3.1.16.10 Command Name Change of Routing Tables

The names of the following CLI commands were changed:

Old CLI Command	New CLI Command	ini File Parameter
inbound-ip-routing	ip2tel-routing	PstnPrefix
outbound-ip-routing	tel2ip-routing	Prefix

Applicable Products: MSBR Series.

3.1.17 TR-069 / TR-104

This subsection describes the new TR-069 / TR-104 features.

3.1.17.1 Auto-Configuration Server Discovery via DHCP

This feature provides support for sending a DHCP response with the URL of an Auto-Configuration Server (ACS) in reply to a DHCP request received from a client with the "dslforum.org" string in the Vendor Class Identifier (DHCP option 60). The device sends the URL in the Vendor Specific Information (DHCP option 43).

This feature is applicable when the device is configured as a DHCP server and is used for TR-069 provisioning.

To support this feature, the following CLI command has been added to define the ACS URL:

```
tr069-acs-server-name <URL>
```

Note that this command can be reached from different configuration interfaces, for example:

```
(dhcp-vlan 2)# tr069-acs-server-name <URL>
(conf-if-VLAN 2)# ip dhcp-server tr069-acs-server-name <URL>
```

Applicable Products: MSBR Series.

3.1.17.2 TR-104 Support

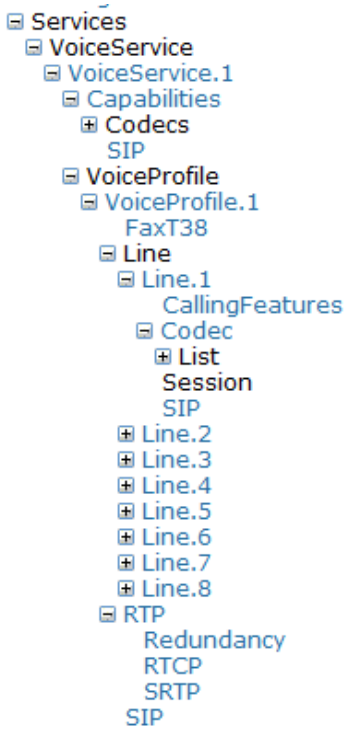
This feature provides support for configuring the device using TR-104 parameters and functionality. This support is for the SIP (VoIP) application layer and applies to FXS interfaces (lines) only.

TR-069 (short for Technical Report 069) is a specification published by Broadband Forum (www.broadband-forum.org) entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. TR-069 uses a

bidirectional SOAP/HTTP protocol for communication between customer premises equipment (CPE) and Auto-Configuration Servers (ACS). Communication between ACS and CPE is defined via Remote Procedure Call (RPC) methods.

TR-104 defines "data model" template for TR-069 enabled devices. The "data model" that is applicable to AudioCodes MSBR devices are defined in the DSL Forum TR-104 – "DSLHome™ Provisioning Parameters for VoIP CPE" at http://www.broadband-forum.org/technical/download/TR-104.pdf.

The hierarchical tree structure of the supported TR-104 objects is shown below:



- InternetGatewayDevice.Services.VoiceService: Top-level object.
- InternetGatewayDevice.Services.VoiceService.1.Capabilities: (Read-Only) Displays the overall capabilities of the device.
  - InternetGatewayDevice.Services.VoiceService.1.Capabilities.Codecs: (Read-Only) Lists supported codecs (according to devices installed Software Feature Key).
  - InternetGatewayDevice.Services.VoiceService.1.Capabilities.SIP: (Read-Only) Displays various SIP settings such as SIP transport type.
- InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1: Corresponds to one or more FXS lines that share the same basic configuration:
  - InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.FaxT38: Configures fax T.38 relay.
  - InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line: Corresponds to an FXS line (as configured in the Trunk Group table). It enables and configures each FXS line (number).
    - InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.{i}.Codec.List.{i}: Configures voice coder used by specific FXS line.
    - InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.{i}.CallingFeatures: Configures voice parameters per FXS line such as caller ID.
    - InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.{i}.SIP: Configures username/password per FXS line. AudioCodes maps this object to the corresponding entry in the Authentication table
  - InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.SIP: Configures SIP parameters specific to the UA such as Proxy server.

- InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.RTP: Configures various RTP parameters for the FXS lines such as RTCP and SRTP.

Applicable Products: MSBR Series.

3.1.17.3 TR-069 Support

This feature provides support for remote management of the device using TR-069. As a bi-directional SOAP/HTTP-based protocol, it provides the communication between the device and Auto Configuration Servers (ACS), which enables auto-configuration of the device. The TR-069 connection to the ACS can be done on the LAN or WAN interface.

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

TR069 CLI: service [TR069ServiceEnable]	Enables TR-069 management. ▪ [0] Disable (Default) ▪ [1] Enable Note: For this parameter to take effect, a device reset is required.
CLI: debug-mode [TR069DebugMode]	Defines the debug mode level. The valid value is between 0 and 3. The default is 0.
URL CLI: acl-url [TR069AcsUrl]	Defines the URL address of the Auto Configuration Servers (ACS) to which the device connects. For example, http://10.4.2.1:10301/acs/. By default, no URL is defined.
User Name CLI: acs-user-name [TR069AcsUsername]	Defines the login username that the device uses for authenticated access to the ACS. The valid value is a string of up to 256 characters. By default, no username is defined.
Password CLI: acs-password [TR069AcsPassword]	Defines the login password that the device uses for authenticated access to the ACS. The valid value is a string of up to 256 characters. By default, no password is defined.
User Name CLI: connection-request-user-name [TR069ConnectionRequestUsername]	Defines the connection request username used by the ACS to connect to the device. The valid value is a string of up to 256 characters. By default, no username is defined.
Password CLI: connection-request-password [TR069ConnectionRequestPassword]	Defines the connection request password used by the ACS to connect to the device. The valid value is a string of up to 256 characters. By default, no password is defined.
URL CLI: connection-request-url [TR069ConnectionRequestUrl	Defines the URL for the ACS connection request. For example, http://10.31.4.115:82/tr069/.
Inform Interval CLI: inform-interval [TR069PeriodicInformInterval]	Defines the periodic inform interval at which the device will communicate with the ACS. The valid value is 0 to 4294967295. The default is 60.

Connection Interface CLI: interface-name [TR069NetworkSource]	Defines the device's network interface for the TR069 connection. ▪ [0] LAN ▪ [1] WAN (default)
Minimum wait interval CLI: [TR069RetryinimumWaitInterval]	Defines the minimum wait interval (in seconds). The valid value is 1 to 65535. The default is 5.

Applicable Products: MSBR Series.

3.1.18 Obsolete Parameters

The table below lists parameters from the previous release that are now obsolete in Release 6.6.

Table 3-1: Obsolete Parameters

Obsolete Parameter	Comment
V1501SSEPayloadTypeTx	This payload type is obtained from the offered SDP of the remote side.
V1501SPRTPayloadTypeRx	This payload type is obtained from the Payload Type field in the Coders table.
V1501SPRTPayloadTypeTx	This payload type is obtained from the remote side offered SDP.
EnableFaxRerouting	This parameter has been replaced by the new parameter, FaxReroutingMode.
acCPQualityOfExperienceUseMosLQ	This SNMP parameter has been replaced by the new parameter, acCPQualityOfExperienceMOSCalculationAlgorithm
CoderName	This parameter has been replaced by the CodersGroup parameter.
search-dn	This CLI command has been replaced by the CLI command, search-dns-in-parallel.
SBCMinSE	This parameter has been replaced by the SBCSessionExpires parameter.

3.2 Version 6.60A.312.003

No new features for this patch version.

3.3 Version 6.60A.314.004

The section lists new features introduced in this patch version.

3.3.1 RTCP XR Sent to IP Group

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

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

Applicable Products: MP-1xx; Mediant 600; Mediant 5xx; Mediant 8xx; Mediant 1000; Mediant 2000; Mediant 3000.

3.4 Version 6.60A.317.001

The section lists new features introduced in this patch version.

3.4.1 Enhanced FXS Channel Cut-Through in Off-Hook

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

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

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

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

Applicable Products: Analog.

3.4.2 Simultaneous DTMF Transport in SIP INFO and RFC 2833

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

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

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

Applicable Products: Analog.

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

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

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

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

Applicable Products: Gateway.

3.5 Version 6.60A.319.003

No new features for this patch version.

3.6 Version 6.60A.322

The section lists new features introduced in this patch version.

3.6.1 RTCP XR per Media Segment

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

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

Applicable Products: Gateway.

3.6.2 Upgraded OpenSSL Library

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

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

Applicable Products: Gateway.

3.7 Version 6.60A.323.005

No new features for this patch version.

4 DSP Firmware Templates and Channel Capacity

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

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 Maximum Registered Users, SBC & IP-to-IP Sessions

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

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

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

Table 4-1: Maximum Registered Users and Call Sessions

Product	Registered Users SAS/SBC/CRP/ IP-to-IP	IP-to-IP Mode Codec Transcoding	SBC Sessions	
			RTP-to-RTP	SRTP-RTP
MediaPack 1xx	25	-	-	-
Mediant 600	600	-	-	-
Mediant 500 MSBR	200	-	60	60
Mediant 800 MSBR	200	30	60	60
Mediant 800 GW & E-SBC	200	30	60	60
Mediant 850 MSBR	200	30	60	60
Mediant 1000	600	60	-	-

Product	Registered Users SAS/SBC/CRP/ IP-to-IP	IP-to-IP Mode Codec Transcoding	SBC Sessions	
			RTP-to-RTP	SRTP-RTP
Mediant 1000B MSBR	600	60	150	120
Mediant 1000B GW & E-SBC	600	60	150	120
Mediant 2000	250	120	-	-
Mediant 3000	3,000 (5,000 Depop.)	1,008	1,008	1,008
Mediant 2600	8,000	350	600	600
Mediant 4000	20,000	1,092	4,000	2,000
Mediant SW E-SBC	20,000	-	1,000	500

4.2 MediaPack 1xx

The table below lists the maximum supported channel capacity.

Table 4-2: Maximum Channel Capacity for MP-11x and MP-124 Rev. D

	DSP Template			
	0		1	
	Maximum Channels			
Model	**Default (no SRTP**	**SRTP Enabled**	**Default (no SRTP**	**SRTP Enabled**
MP-112 FXS/FXO	2	2	2	2
MP-114 FXS/FXO	4	3	3	3
MP-118 FXS/FXO	8	6	6	6
MP-124 Rev. D	24	18	18	18
Voice Coder				
G.711 A/Mu-law PCM	√	√	√	√
G.726 ADPCM	√	√	√	√
G.727 ADPCM	√	√	√	√
G.723.1	√	√	√	√
G.729 A, B	√	√	√	√
EG.711	√	√	-	-
G.722	-	-	√	√

Table 4-3: Maximum Channel Capacity for MP-124 Rev. E

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

4.3 Mediant 500 MSBR

The DSP capabilities for Mediant 500 MSBR for Release 6.6 are shown in the table below.

Table 4-4: Channel Capacity and Capabilities for Mediant 500 MSBR

Telephony Interface Assembly	DSP Channels on Physical Interface	Advanced DSP Capabilities[1]						SBC Sessions
		IPM Detectors[2]	AMR WB	SILK	SILK WB	V.150.1[3]	Conference Participants[4]	
2 x BRI	4	√	√	√	√	-	4	56
Without Telephony Interfaces	-	-	-	-	-	-	-	60

[1] 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.
[2] IPM Detectors include Automatic Gain Control (AGC) and Answer Detector (AD).
[3] V.150.1 is supported only for the US Department of Defense (DoD).
[4] Number of participants in one or more conference (bridge), where each conference may include three or more participants. Conferences are supported on all configurations. Please contact AudioCodes for the maximum number of participants per configuration.

4.4 Mediant 8xx Series

The DSP capabilities for Mediant 800 Gateway & E-SBC, Mediant 800 MSBR, and Mediant 850 MSBR for Release 6.6 are shown in the table below.

Table 4-5: Channel Capacity and Capabilities for Mediant 8xx Series

Telephony Interface Assembly	DSP Channels on Physical Interface	Advanced DSP Capabilities[5]								
		SBC Enhancements[6]	IPM Detectors[7]	AMR WB	SILK	SILK WB	V.150.1[8]	Transcoding Sessions[9]	Conference Participants[10]	SBC Sessions
2 x E1/T1	60 / 48	-	-	-	-	-	-	0 / 6	-	0 / 12
2 x T1	48	-	√	-	-	-	√	6	-	12
1 x E1/T1 & FXS / FXO Mix x 8	38 / 32	-	√	-	-	-	-	4 / 7	-	22 / 28
	38 / 32	-	√	-	√	-	-	2 / 5	-	22 / 28
1 x E1/T1	30 / 24	-	√	-	√	-	√	6 / 8	-	30 / 36
4 x BRI & 4 x FXS & 4 x FXO	16	-	√	-	-	-	-	2	-	48
8 x BRI	16	-	√	-	-	-	-	2	-	44
12 x FXS	12	-	√	-	√	-	√	1	-	48
4 x FXS & 8 x FXO	12	-	√	-	√	-	-	1	-	48
4 x BRI & 4 x FXS	12	-	√	-	√	-	-	1	-	48
4 x FXS & 4 x FXO	8	-	-	-	-	-	-	4	6	52
	8	-	√	-	√	-	-	3	-	52
4 x BRI	8	-	-	-	-	-	-	4	6	52
	8	-	√	-	√	-	-	3	-	52
6 x E&M[11]	6	-	-	-	-	-	-	8	-	54
4 x FXS or 4 x FXO	4	-	-	-	√	-	√	6	-	56
	4	-	-	-		-	-	5	8	56
	4	-	-	-	√	-	-	3	7	56
	4	-	√	√	√	-	-	2	4	56
	4	-	√	√	√	√	-	2	4	56
SBC (Telephony	-	-	-	-	-	-	-	11	-	60

[5] 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.
[6] SBC enhancements include the network Acoustic Echo Suppressor.
[7] IPM Detectors include Automatic Gain Control (AGC) and Answer Detector (AD).
[8] V.150.1 is supported only for the US Department of Defense (DoD).
[9] Transcoding Sessions are part of the total SBC Sessions.
[10] Number of participants in one or more conference (bridge), where each conference may include 3 or more participants. Note that conferences are supported on all above configurations. Please contact AudioCodes for the maximum number of participants per configuration.
[11] E&M signaling interface is applicable only to Mediant 800 Gateway & E-SBC.

Telephony Interface Assembly	DSP Channels on Physical Interface		Advanced DSP Capabilities[5]							
		SBC Enhancements[6]	IPM Detectors[7]	AMR WB	SILK	SILK WB	V.150.1[8]	Transcoding Sessions[9]	Conference Participants[10]	SBC Sessions
Interfaces may be Present, but are Inactive)										
Without Telephony Interfaces	-	-	-	-	-	-	-	30	-	60
	-	√	-	-	-	-	-	25	-	60
	-	-	-	-	√	-	-	21	-	60
	-	-	-	√	√	√	-	18	-	60
	-	√	-	-	√	-	-	16	-	60
	-	√	-	√	√	√	-	13	-	60

Note: For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

4.5 Mediant 600 and Mediant 1000

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

- Analog (FXS/FXO) – see Section 4.5.1 on page 134
- Digital interfaces – see Section 4.5.3 on page 136
- Media processing interfaces (MPM module) – see Section 4.5.4 on page 137

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

4.5.1 Analog (FXS/FXO) Interfaces

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

Table 4-6: DSP Firmware Templates for Mediant 600 & Mediant 1000 Analog 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	√	√
G.727	√	√
G.726 ADPCM	√	√
G.723.1	√	√
G.729 A, B	√	√
G.722	-	√

4.5.2 BRI Interfaces

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

Table 4-7: DSP Firmware Templates for Mediant 600 & Mediant 1000 BRI Interfaces

	DSP Template					
	0, 1, 2, 4, 5, 6			10, 11, 12, 14, 15, 16		
	Number of BRI Spans					
	4	8	20	4	8	20
	Number of Channels					
Default Settings	8	16	40	6	12	30
With SRTP	6	12	30	6	12	30
Voice Coder						
G.711 A/Mu-law PCM	√			√		
G.727	√			√		
G.726 ADPCM	√			√		
G.723.1	√			√		
G.729 A, B	√			√		
G.722	-			√		

4.5.3 E1/T1 Interfaces

The table below lists the supported channel capacity per DSP firmware template for E1/T1 interfaces:

Table 4-8: DSP Firmware Templates for Mediant 600 / Mediant 1000 E1/T1 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		-	-	24	36	60	24	36	60	31	48	80
With IPM Features[12]	31	60	100	-	-	-	-	-	-	-	-	-	31	60	100
With IPM Features & SRTP	31	48	80	-	-	-	-	-	-	-	-	-	31	48	80
Voice Coder															
G.711 A-law/Mμ-law PCM	✓			✓			✓			✓			✓		
G.727	✓			✓			✓			✓			-		
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.

4.5.4 Media Processing Interfaces

The table below lists the supported channel capacity per DSP firmware template for media processing (provided by the MPM module):

Notes:

- The MPM module is applicable only to Mediant 1000.
- 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 4-9: DSP Firmware Templates for Mediant 1000 MPM Module

			DSP Template									
			0 or 10		1 or 11		2 or 12		5 or 15		6 or 16	
			Assembly Slot									
			1-5	6	1-5	6	1-5	6	1-5	6	1-5	6
Supplementary Capabilities			Number of Channels									
SRTP	IPM Detectors	Conference										
-	-	-	48	-	32	-	24	-	24	-	40	-
✓	-	-	40	-	-	-	24	-	24	-	40	-
-	✓	-	40	-	-	-	-	-	-	-	40	-
✓	✓	-	32	-	-	-	-	-	-	-	32	-
-	-	✓	40	20	32	16	24	12	24	12	40	20
✓	-	✓	32	16	-	-	24	12	24	12	32	16
✓	✓	✓	32	16	-	-	-	-	-	-	32	16
Voice Coder												
G.711 A-law/Mμ-law PCM			✓		✓		✓		✓		✓	
G.727			✓		✓		✓		✓		-	
G.726 ADPCM			✓		✓		✓		✓		-	
G.723.1			✓		-		-		-		-	
G.729 A, B			✓		✓		✓		✓		✓	
GSM FR			✓		✓		-		-		-	
MS GSM			✓		✓		-		-		-	
iLBC			-		-		-		✓		-	
EVRC			-		-		✓		-		-	
QCELP			-		-		✓		-		-	

	DSP Template									
	0 or 10		1 or 11		2 or 12		5 or 15		6 or 16	
	Assembly Slot									
	1-5	6	1-5	6	1-5	6	1-5	6	1-5	6
Supplementary Capabilities										
SRTP / **IPM Detectors** / **Conference**	**Number of Channels**									
AMR	-		✓		-		-		-	
GSM EFR	-		✓		-		-		-	
G.722	-		-		-		-		✓	
Transparent	✓		✓		✓		✓		✓	

4.6 Mediant 1000B MSBR and Mediant 1000B GW & E-SBC

This section lists the Mediant 1000B MSBR and Mediant 1000B GW & E-SBC DSP templates for the following interfaces:

- Analog (FXS/FXO) – see Section 4.6.1 on page 139
- Digital interfaces – see Section 4.6.2 on page 140
- Media processing interfaces (MPM module) – see Section 4.6.4 on page 142

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

4.6.1 Analog (FXS/FXO) Interfaces

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

Table 4-10: DSP Firmware Templates for Mediant 1000B MSBR / Mediant 1000B GW & E-SBC Analog Interfaces

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

4.6.2 BRI Interfaces

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

Table 4-11: DSP Firmware Templates for Mediant 600 & Mediant 1000 BRI Interfaces

	DSP Template					
	0, 1, 2, 4, 5, 6			10, 11, 12, 14, 15, 16		
	Number of BRI Spans					
	4	8	20	4	8	20
	Number of Channels					
Default Settings	8	16	40	6	12	30
With SRTP	8	16	40	6	12	30
Voice Coder						
G.711 A/Mu-law PCM	√			√		
G.727	√			√		
G.726 ADPCM	√			√		
G.723.1	√			√		
G.729 A, B	√			√		
G.722	-			√		

4.6.3 E1/T1 Interfaces

The table below lists the supported channel capacity per DSP firmware template for E1/T1 interfaces:

Table 4-12: DSP Firmware Templates for Mediant 1000B MSBR / Mediant 1000B E1/T1 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	62	120	31	48	80	24	36	60	24	36	60	31	60	100
With IPM Features[13]	31	60	100	-	-	-	-	-	-	-	-	-	31	60	100
With IPM Features & SRTP	31	60	100	-	-	-	-	-	-	-	-	-	31	60	100
Voice Coder															
G.711 A-law/Mμ-law PCM	✓			✓			✓			✓			✓		
G.727	✓			✓			✓			✓			-		
G.726 ADPCM	✓			✓			✓			✓			-		
G.723.1	✓			-			-			-			-		
G.729 A, B	✓			✓			✓			✓			✓		
GSM FR	✓			✓			-			-			-		
MS GSM	✓			✓			-			-			-		
iLBC	-			-			-			✓			-		
EVRC	-			-			✓			-			-		
QCELP	-			-			✓			-			-		
AMR	-			✓			-			-			-		
GSM EFR	-			✓			-			-			-		
G.722	-			-			-			-			✓		
Transparent	✓			✓			✓			✓			✓		

[13] 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.

4.6.4 Media Processing Interfaces

The table below lists the supported channel capacity per DSP firmware template for media processing (provided by the MPM module):

Notes:

- 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 4-13: DSP Firmware Templates for Mediant 1000B MSBR / Mediant 1000B MPM Module

			DSP Template									
			0 or 10		1 or 11		2 or 12		5 or 15		6 or 16	
			Assembly Slot									
			1-5	6	1-5	6	1-5	6	1-5	6	1-5	6
Supplementary Capabilities			Number of Channels									
SRTP	IPM Detectors	Conference										
-	-	-	48	-	32	-	24	-	24	-	40	-
✓	-	-	48	-	32	-	24	-	24	-	40	-
-	✓	-	40	-	-	-	-	-	-	-	40	-
✓	✓	-	40	-	-	-	-	-	-	-	40	-
-	-	✓	40	20	32	16	24	12	24	12	40	20
✓	-	✓	40	20	-	-	24	12	24	12	40	20
✓	✓	✓	40	20	-	-	-	-	-	-	40	20
Voice Coder												
G.711 A-law / Mμ-law PCM			✓		✓		✓		✓		✓	
G.727			✓		✓		✓		✓		-	
G.726 ADPCM			✓		✓		✓		✓		-	
G.723.1			✓		-		-		-		-	
G.729 A, B			✓		✓		✓		✓		✓	
GSM FR			✓		✓		-		-		-	
MS GSM			✓		✓		-		-		-	
iLBC			-		-		-		✓		-	
EVRC			-		-		✓		-		-	
QCELP			-		-		✓		-		-	
AMR			-		✓		-		-		-	
GSM EFR			-		✓		-		-		-	

G.722	-	-	-	-	✓
Transparent	✓	✓	✓	✓	✓

4.7 Mediant 2000

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

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

Table 4-14: DSP Firmware Templates for Mediant 2000

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

4.8 Mediant 2600 E-SBC

The maximum number of supported SBC sessions is shown in Section 4.1 on page 129. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below:

Table 4-15: Channel Capacity and Capabilities

Basic DSP Capabilities	Advanced DSP Capabilities					Min. DSP Sessions	
	SBC Enhancements	G.722	AMR WB	SILK	SILK WB	MPM	No MPM
✓	-	-	-	-	-	350	175
✓	-	✓	-	-	-	300	150
✓	-	✓	-	✓	-	200	100
✓	-	✓	✓	✓	✓	150	75
✓	✓	✓	✓	✓	✓	150	75
✓	✓	✓	-	✓	-	200	100
✓	✓	✓	-	-	-	250	125
✓	✓	-	-	-	-	250	125

Notes:

- *Min. DSP Sessions* refers to the minimum number of sessions available when using the selected DSP capabilities. When using only some of the DSP capabilities or using them only on some channels, the number of available DSP sessions may increase.
- *SBC Enhancements* refers to the Network Acoustic Echo Suppressor.
- *Basic DSP Capabilities* refers to the following channel capabilities that require DSP resources: IBS, Silence Compression, T.38, G.711, G.726, G.729, G.723.1, and AMR.
- *MPM* refers to the optional Media Processing Module.

4.9 Mediant 3000

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

- Mediant 3000 full chassis – see Section 4.9.1 on page 144
- Mediant 3000 with 16 E1 / 21 T1 – see Section 4.9.2 on page 146
- Mediant 3000 with single T3 – see Section 4.9.3 on page 148
- DSP template mix feature – see Section 4.9.4 on page 149

4.9.1 Mediant 3000 Full Chassis

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

For Release 6.6, 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 4-16: DSP Firmware Templates for Mediant 3000

Supplementary Capabilities					DSP Template										
					0	1	2	4	5	7	9	10	11	12	13
SRTP	ARIA	RTCP XR	IPM Detectors	Acoustic Echo Suppressor	Number of Channels										
-	-	-	-	-	2016	2016	1764	1260	1260	1638	1008	1512	630	756	378
-	-	✓	✓	-	1890	1890	1638	1134	1134	1638	1008	1512	630	756	378
-	-	-	-	✓	1134	1134	1134	630	1008	882	252	1134	252	378	378
✓	-	-	-	-	1764	1638	-	1008	-	1638	1008	-	630	-	-
✓	-	✓	✓	-	1638	1638	-	1008	-	1512	1008	-	630	-	-
✓	✓	-	-	-	1638	1638	-	1008	-	1386	1008	-	504	-	-
✓	✓	✓	✓	-	1638	1638	-	1008	-	1386	1008	-	504	-	-
✓	✓	✓	✓	✓	1134	1134	-	1008	-	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.727					✓	✓	✓	✓	✓	✓	-	-	-	-	-
G.729 A, B					✓	✓	✓	✓	✓	✓	✓	✓	✓	-	-
G.729.1 (up to 12 kbps)					-	-	-	-	-	-	-	-	-	-	-
GSM EFR					-	✓	-	✓	-	-	-	-	-	-	-
GSM FR					✓	✓	-	✓	-	-	-	-	-	-	-
iLBC					-	-	-	-	-	✓	-	-	-	-	-
MS GSM					✓	✓	-	✓	-	-	-	-	-	-	-
MS-RTA (NB)					-	-	-	-	-	-	✓	-	✓	-	-
MS-RTA (WB)					-	-	-	-	-	-	-	-	✓	-	-
SPEEX NB					-	-	-	-	-	-	-	-	-	✓	✓
SPEEX WB					-	-	-	-	-	-	-	-	-	-	✓
T.38 Version 3					-	-	-	-	-	-	-	✓	-	-	-

4.9.2 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 4-17: DSP Firmware Templates for Mediant 3000 16 E1 / 21 T1

Supplementary Capabilities					DSP Template								
					0	1	2	4	5	7	9	10	11
SRTP	ARIA	RTCP XR	IPM Detectors	Acoustic Echo Suppressor	Number of Channels								
-	-	-	-	-	504	504	504	360	360	468	288	432	180
-	-	✓	✓	-	504	504	468	324	324	468	288	432	180
-	-	-	-	✓	324	324	324	180	288	252	72	324	72
✓	-	-	-	-	504	468	-	288	-	468	288	-	180
✓	-	✓	✓	-	468	468	-	288	-	432	288	-	180
✓	✓	-	-	-	468	468	-	288	-	396	288	-	144
✓	✓	✓	✓	-	468	468	-	288	-	396	288	-	144
✓	✓	✓	✓	✓	324	324	-	180	-	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.727					✓	✓	✓	✓	✓	✓	-	-	-
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					-	-	-	-	-	-	-	✓	-

4.9.3 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 4-18: 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	432	432	240	384	336	96	432	96
✓	-	-	-	-	672	624-	-	384	-	624	384	-	240
✓	-	✓	✓	-	624	624	-	384	-	576	384	-	240
✓	✓	-	-	-	624	624	-	384	-	528	384	-	192
✓	✓	✓	✓	-	624	624	-	384	-	528	384	-	192
✓	✓	✓	✓	✓	432	432	-	240	-	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.727					✓	✓	✓	✓	✓	✓	-	-	-
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					-	-	-	-	-	-	-	✓	-

4.9.4 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 4-19: 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

4.10 Mediant 4000 E-SBC

The maximum number of supported SBC sessions is shown in Section 4.1 on page 129. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the table below:

Table 4-20: Channel Capacity and Capabilities for Mediant 4000 E-SBC

Basic DSP Capabilities	Advanced DSP Capabilities					Min. DSP Sessions	
	SBC Enhancements	G.722	AMR WB	SILK	SILK WB	MPM	No MPM
✓	-	-	-	-	-	1050	350
✓	-	✓	-	-	-	950	300
✓	-	✓	-	✓	-	700	200
✓	-	✓	✓	✓	✓	550	150
✓	✓	✓	✓	✓	✓	450	150
✓	✓	✓	-	✓	-	600	200
✓	✓	✓	-	-	-	800	250
✓	✓	-	-	-	-	850	250

Notes:

- *Min. DSP Sessions* refers to the minimum number of sessions available when using the selected DSP capabilities. When using only some of the DSP capabilities or using them only on some channels, the number of available DSP sessions may increase.
- *SBC Enhancements* refers to the Network Acoustic Echo Suppressor.
- *Basic DSP Capabilities* refers to the following channel capabilities that require DSP resources: IBS, Silence Compression, T.38, G.711, G.726, G.729, G.723.1, and AMR.
- *MPM* refers to the optional Media Processing Module.

4.11 Mediant Software E-SBC

Note: Mediant Software E-SBC does not implement digital signal processing (DSP). Therefore, it supports only SBC functionalities that do not require media signal processing.

5 Known Constraints in Release 6.6

This section lists known constraints in Release 6.6.

5.1 Version GA

This section lists known constraints discovered in the GA version.

5.1.1 SIP Constraints

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

1. Ring to Hunt Group feature is not functioning when Early Media is enabled.

   Applicable Products: Mediant 500 MSBR; Mediant 8xx Series.

2. The Gateway / IP-to-IP application is not supported.

   Applicable Products: Mediant 2600; Mediant 4000; Mediant SW E-SBC.

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

   Applicable Products: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

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

   Applicable Products: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

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

   Applicable Products: Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

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

   Applicable Products: Mediant 500 MSBR; Mediant 8xx Series.

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

   - The following SIP Methods are omitted by the IP-to-IP application:
     - MESSAGE
     - PUBLISH
     - SUBSCRIBE
     - NOTIFY
     - Out-of-dialog REFER
     - Any other proprietary Method

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

Applicable Products: Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

8. Publishing of RTCP XR is sent only at call termination.

   Applicable Products: Mediant 3000.

5.1.2 Media Constraints

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

1. RTCP XR is not supported for RTP Redundancy. In addition, the RTCP XR reports may not be completely accurate in some scenarios when using variable-rates vocoders (such as EVRC, AMR, RTA, and SILK).

   Applicable Products: Mediant 500 MSBR; Mediant 8xx Series; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

2. When SRTP is enabled, RTP Redundancy and M-factor cannot operate together. In other words, SRTP can operate with RTP Redundancy greater than 0 or with m-factor greater than 1, but not with both.

   Applicable Products: Mediant 1000B MSBR; Mediant 1000B GW & E-SBC.

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

   Applicable Product: Mediant SW E-SBC.

4. 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 500 MSBR; Mediant 8xx Series.

5. 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 500 MSBR; Mediant 8xx Series.

6. SBC RTP call forwarding 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, MS RTA, EVRC, AMR, QCELP, SILK, and Speex. A workaround is to use SRTP full encryption / decryption on the forwarding calls.

   Applicable Products: Mediant 1000; Mediant 1000B GW & E-SBC; Mediant 3000.

7. 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 GW & E-SBC; Mediant 500 MSBR; Mediant 1000B MSBR; Mediant 8xx Series; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

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

   Applicable Products: Mediant 3000.

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

   Applicable Products: Mediant 600; Mediant 1000; Mediant 1000B GW & E-SBC; Mediant 3000.

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

    Applicable Products: All.

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: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; 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 wideband 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: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; 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: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; 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: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; 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: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; 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; Mediant 1000B MSBR.

5.1.3 PSTN Constraints

This release includes the following known PSTN constraints:

1. Running the CLI command **`write system-voip-defaults`** requires a device reset before continuing with PSTN provisioning. In other words, two resets are required; one to activate this command and the next after PSTN provisioning.

   Applicable Products: MSBR Series.

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

   Applicable Products: Mediant 8xx Series; Mediant 1000 Series; Mediant 3000.

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

   Applicable Products: Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

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

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

   Applicable Products: Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

5. 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.

5.1.3.1 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.

5.1.3.2 SONET / SDH Constraints

This release includes the following known SDH constraints:

1. The BIT voice path may fail when using the SONET interface in byte-synchronous mode.

   Applicable Products: Mediant 3000 with TP-6310.

2. For SDH/SONET and DS3 interfaces, if a trunk is in LOF alarm and the alarm is 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.

5.1.4 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; Mediant 1000B MSBR.

2. Voice Prompt 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; Mediant 1000B MSBR.

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; Mediant 1000B MSBR.

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; Mediant 1000B MSBR.

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; Mediant 1000B MSBR.

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

   Applicable Products: Mediant 1000; Mediant 1000B MSBR.

5.1.5 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 2600; Mediant 4000.

2. 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 GW & E-SBC; Mediant 1000B GW & E-SBC; Mediant 2600; Mediant 4000.

3. 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; Mediant 3000.

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

   Applicable Products: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

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

   Applicable Products: All.

6. Debug Recording:

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

   Applicable Products: All.

7. T1 WAN interface is not supported.

   Applicable Products: MSBR Series.

8. Configured VPN L2TP servers are automatically deleted when updating the device's software. A workaround to this problem is to reconfigure the L2TP servers after updating the firmware.

   Applicable Products: MSBR Series.

9. When the device is setup with WAN ADSL/VDSL, L2TP connections cannot be disconnected through the Web interface when the device operates as an L2TP server.

   Applicable Products: MSBR Series.

10. When the device is setup with WAN ADSL/VDSL, CLI commands are missing for L2TP server interface configurations.

    Applicable Products: MSBR Series.

11. Sometimes after configuration of IPSec SA in transport mode, the SA must be disabled and then re-enabled in order to establish the IPSec connection.

    Applicable Products: MSBR Series.

12. PPTP server is not supported.

    Applicable Products: MSBR Series.

13. The CLI command `NAPT` does not function on packets from sources that are not directly connected on the LAN side (e.g., from sources behind other routers on the LAN).

    Applicable Products: MSBR Series.

5.1.6 High Availability Constraints

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

1. 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.

2. 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.

3. 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.

5.1.7 Infrastructure Constraints

This release includes the following known infrastructure constraints:

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

   Applicable Products: MP-124.

2. 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 2600; Mediant 4000.

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

   Applicable Products: Mediant 800 GW & E-SBC.

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: All.

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

   Applicable Products: All.

5.1.8 Web Constraints

This release includes the following known Web constraints:

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

   Applicable Products: All.

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

   Applicable Products: All.

3. The Web and CLI management interfaces are not synchronized; some parameters configured through the Web (such as Syslog) are not shown in the CLI (**show** commands).

   Applicable Products: MSBR Series.

4. After manual switchover in HA Revertive Mode, the Web Home page isn't refreshed. A workaround is to refresh the Home page to get the updated status.

   Applicable Products: Mediant 2600; Mediant 4000.

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

   Applicable Products: All.

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: Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

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

   Applicable Products: MSBR Series.

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

   Applicable Products: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000.

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

   Applicable Products: All.

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

    Applicable Products: All.

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

    Applicable Products: Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

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

    Applicable Products: Mediant 600; Mediant 1000; Mediant 3000.

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

    Applicable Products: Mediant SW E-SBC.

14. RADIUS is not supported.

    Applicable Products: Mediant SW E-SBC.

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

    Applicable Products: All.

16. 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: MSBR Series.

17. 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: MSBR Series.

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

    Applicable Products: MP-1xx; Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

19. The WAN priority cannot be configured on ATM / EFM interfaces, using the Web management tool.

    Applicable Products: MSBR Series.

5.1.9 SNMP Constraints

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

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

   Applicable Products: All.

2. Offline IP addresses appear as "ONLINE" in the Interface table.

   Applicable Products: E-SBC Series.

3. SNMP is not supported.

   Applicable Products: Mediant SW E-SBC.

4. When configuring acSysInterfaceTable using SNMP or the Web interface, validation is done only after a 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 objects, dsx3IntervalPSESs and dsx3IntervalSEFSs are not supported.

   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: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000.

5.1.10 EMS Constraints

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

1. EMS Version 6.6 is not supported on Mediant 500 MSBR and Mediant SW E-SBC.

   Applicable Products: Mediant 500 MSBR; Mediant SW E-SBC.

2. EMS Version 6.4 GA is not supported:

   Applicable Products: Mediant 1000B GW & E-SBC; Mediant 8xx Series; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

5.1.11 CLI Constraints

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

1. The CLI script files (CLI Script file and Startup script file) used in automatic configuration do not support the **`copy`** command and it must not be included in the files.

   Applicable Products: MSBR Series.

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

   Applicable Products: Mediant SW E-SBC.

3. 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; Mediant 3000.

5.2 Version 6.60A.312.003

No new constraints for this patch version.

5.3 Version 6.60A.314.004

No new constraints for this patch version.

5.4 Version 6.60A.317.001

No new constraints for this patch version.

5.5 Version 6.60A.319.003

No new constraints for this patch version.

5.6 Version 6.60A.322

No new constraints for this patch version.

5.7 Version 6.60A.323.005

No new constraints for this patch version.

This page is intentionally left blank.

6 Resolved Constraints in Release 6.6

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

6.1 Version GA

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

6.1.1 SIP Resolved Constraints

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

1. The SIP user registration database is not replicated as part of the switchover from active to redundant device.

   Applicable Products: Mediant 2600; Mediant 4000; Mediant SW E-SBC.

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

   Applicable Products: All.

3. The SBC registration time parameters can only be configured using *ini* file parameters.

   Applicable Products: E-SBC Series.

4. Termination of SIP REFER, 3xx, Hold, and re-INVITE is supported only by the IP-to-IP application.

   Applicable Products: MSBR Series; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

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: All.

6. Least Cost Routing is supported only for the Gateway and IP-to-IP applications and will be supported for the SBC application in the next applicable release. This is now also supported by the SBC application.

   Applicable Products: Mediant 8xx Series; Mediant 1000B MSBR; Mediant 1000B GW & E-SBC; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

7. RTP-SRTP transcoding for video streams are not supported.

   Applicable Products: E-SBC Series.

8. During HA switchover from active to redundant, the SBC registered users database is not copied to the redundant side.

   Applicable Products: Mediant 3000; Mediant 2600; Mediant 4000.

9. The SAS application is not supported on Mediant 3000 HA.

   Applicable Products: Mediant 3000 HA.

6.1.2 Media Resolved Constraints

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

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

   Applicable Product: Mediant 2600; Mediant 4000.

2. 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 8xx Series.

3. 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 8xx Series.

4. 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 1000B MSBR; Mediant 1000B GW & E-SBC.

6.1.3 Networking Resolved Constraints

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

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

   Applicable Products: Mediant SW E-SBC.

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

   Applicable Products: MSBR Series.

6.1.4 High Availability Resolved Constraints

The following High Availability constraints from the previous release have been resolved:

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 2600; Mediant 4000; Mediant SW 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 devices.

   Applicable Products: Mediant SW 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. Automatic update using NFS is not supported on the HA system. Configuring NFS entries in the HA system may prevent the redundant unit from loading.

   Applicable Products: Mediant 2600; Mediant 4000; Mediant SW E-SBC.

6.1.5 PSTN Resolved Constraints

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

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

   Applicable Products: Mediant 3000 with TP-6310.

6.1.6 Infrastructure Resolved Constraints

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

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

   Applicable Products: MSBR Series.

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

   Applicable Products: All.

6.1.7 Web Resolved Constraints

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

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

   Applicable Products: All.

2. In the 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 GW & E-SBC; Mediant 1000B GW & 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: MP-1xx; Mediant 600; Mediant 500 MSBR; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

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

   Applicable Products: Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000; Mediant SW E-SBC.

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

   Applicable Products: All.

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

   Applicable Products: All.

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

   Applicable Products: Mediant 800 GW & E-SBC; Mediant 1000B GW & E-SBC; Mediant 2600; Mediant 4000.

8. When accessing the ADSL/VDSL Web page, the device crashes.

   Applicable Products: MSBR Series.

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

   Applicable Products: MP-1xx; Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000.

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

    Applicable Products: MP-1xx; Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000.

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

Applicable Products: MP-1xx; Mediant 600; Mediant 8xx Series; Mediant 1000 Series; Mediant 2000; Mediant 3000; Mediant 2600; Mediant 4000.

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

    Applicable Products: Mediant 8xx Series.

13. 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: MSBR Series; Mediant 3000.

14. 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.

6.1.8 SNMP Resolved Constraints

The following SNMP constraints from the previous release have now been resolved:

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

   Applicable Products: Mediant 3000 with TP-6310.

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

   Applicable Products: Mediant 8xx Series.

6.1.9 CLI Resolved Constraints

The following CLI constraints from the previous release have now been resolved:

1. The NFS table cannot be configured through the CLI.

   Applicable Products: MSBR Series.

6.2 Version 6.60A.312.003

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

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

   The constraint has now been resolved.

   SR: 762543

   Applicable Products: All.

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

   The constraint has now been resolved.

   SR: 749395

   Applicable Products: All.

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

   The constraint has now been resolved.

   SR: 756607

   Applicable Products: MP-1xx.

4. The device crashes when a specific timer expires (rare scenario).

   The constraint has now been resolved.

   SR: 750923

   Applicable Products: Mediant 3000.

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

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 600; Mediant 5xx; Mediant 8xx; Mediant 1000; Mediant 2000; Mediant 3000.

6.3 Version 6.60A.314.004

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

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

   The constraint has now been resolved.

   SR: 769333

   Applicable Products: Mediant Gateways.

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

   The constraint has now been resolved.

   SR: 769253

   Applicable Products: Mediant Gateways.

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

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: All.

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

   The constraint has now been resolved.

   SR: 767763

   Applicable Products: All.

5. The device erroneously crashes (and resets) upon a rare exception.

   The constraint has now been resolved.

   SR: 767099

   Applicable Products: All.

6. Explicit Call Transfer (ECT) does not work with BRI trunks (TrunkTransferMode parameter set to 2).

   The constraint has now been resolved.

   SR: 768019

   Applicable Products: Mediant 600; Mediant 5xx; Mediant 8xx; Mediant 1000/B

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

   The constraint has now been resolved.

   SR: 766717

   Applicable Products: MP-1xx; Mediant Gateways.

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

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant Gateways.

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

   The constraint has now been resolved.

   SR: 764397

   Applicable Products: All.

6.4 Version 6.60A.317.001

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

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

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: All.

2. The ini file parameter, TDMHairPinning is limitated to 199 characters and therefore, only up to 54 trunks can be added to the parameter (for TDM hair-pinning).

   The constraint has now been resolved (up to 399 characters).

   SR:

   Applicable Products: Mediant 3000.

3. A password (command shell) is required to load Customer coefficient files to the device.

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

   SR: 769681

   Applicable Products: MP-1xx; Mediant 8xx; Mediant 1000.

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

   The constraint has now been resolved.

   SR: 769253

   Applicable Products: MP-1xx; Mediant 8xx; Mediant 1000; Mediant 3000.

5. If the device loses connectivity with the SEM, it sends many RTCP-XR errors to the Syslog server.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: SBC.

6. When performing a Hitless software upgrade from Version 6.60A.270.010 to Version 6.60A.309.001, an upgrade failure occurs due to the installed Pre-recorded Tones (PRT) file. A workaround is to remove the PRT file before upgrade.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 3000.

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

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: All.

6.5 Version 6.60A.319.003

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

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

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateway.

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

   The constraint has now been resolved.

   SR: 754731

   Applicable Products: All.

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

   The constraint has now been resolved.

   SR: 769613

   Applicable Products: MP-1xx.

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

   The constraint has now been resolved.

   SR: 769983

   Applicable Products: Digital Gateway.

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

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateway.

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

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateway.

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

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: All.

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

   The constraint has now been resolved.

   SR: 767141

   Applicable Products: All.

6.6 Version 6.60A.322

No resolved constraints for this patch version.

6.7 Version 6.60A.323.005

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

Table 6-1: Resolved Constraints for Patch Version 6.60A.323.005

Incident	Description
135012	When loading a .cmp file through the automatic update process, the device downloads a .cmp file and then attempts erroneously to download another .cmp file, resulting in software upgrade failure. This is due to lack of device memory resources. **Applicable Products:** Gateway.
134631	When the device requests an ini file during the automatic update process, it always sends the MAC address (in the ini file URL) in upper case letters. If the ini file is defined in lower case on the HTTP server, ini file download fails as the HTTP server adheres to case sensitivity. This has been resolved: If the ini file URL includes "<MAC>", the device sends the MAC address in upper case; if it includes "<mac>", it sends it in lower case. **Applicable Products:** Gateway.
134630	During the automatic update process, even though the AutoUpdateCmpFile parameter is configured to 0, the device erroneously attempts to download the .cmp file (which fails). **Applicable Products:** Gateway.
134542	When ISDN tunneling is enabled, the device attempts to re-negotiate the B-channel instead of using the B-channel on which the call was initially established. As a result, call failure occurs. **Applicable Products:** Gateway.

Incident	Description
133962	When the device operates for over 620 days, one of the counters overflow and causes all PSTN timers to expire sooner than normal (e.g. 5 seconds instead of 50 seconds). As a result, calls are untimely disconnected. A workaround is to reset the device. **Applicable Products:** Gateway.
132481	When the device sends SIP PUBLISH messages for call segments (calls whose media parameters such as a coder has changed during the call), the SSRC for local and remote streams in the first PUBLISH is always "0xffffffff", resulting in incorrect quality report information. **Applicable Products:** Gateway.

7 Supported SIP Standards

7.1 Supported RFCs

The table below lists the supported RFCs.

Table 7-1: Supported RFCs

RFC	Description	Gateway	SBC
RFC 2327	SDP	Yes	Yes
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication	Yes	Yes
RFC 2782	A DNS RR for specifying the location of services	Yes	Yes
RFC 2833	Telephone event	Yes	Yes
RFC 3261	SIP	Yes	Yes
RFC 3262	Reliability of Provisional Responses	Yes	Yes
RFC 3263	Locating SIP Servers	Yes	Yes
RFC 3264	Offer/Answer Model	Yes	Yes
RFC 3265	(SIP)-Specific Event Notification	Yes	Yes
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)	Yes	No
RFC 3311	UPDATE Method	Yes	Yes
RFC 3323	Privacy Mechanism	Yes	Yes
RFC 3325	Private Extensions to the SIP for Asserted Identity within Trusted Networks	Yes	Yes
RFC 3326	Reason header	Yes	Yes - forwarded transparently
RFC 3327	Extension Header Field for Registering Non-Adjacent Contacts	Yes	No
RFC 3361	DHCP Option for SIP Servers	Yes	No
RFC 3372	SIP-T	Yes	Yes - forwarded transparently
RFC 3389	RTP Payload for Comfort Noise	Yes	Yes - forwarded transparently
RFC 3420	Internet Media Type message/sipfrag	Yes	Yes
RFC 3455	P-Associated-URI	Yes	Yes - using user info \ account
RFC 3489	STUN - Simple Traversal of UDP	Yes	No

RFC	Description	Gateway	SBC
RFC 3550	RTP: A Transport Protocol for Real-Time Applications	Yes	Yes
RFC 3515	Refer Method	Yes	Yes
RFC 3578	Interworking of ISDN overlap signalling to SIP	Yes	No
RFC 3581	Symmetric Response Routing - rport	Yes	Yes
RFC 3605	RTCP attribute in SDP	Yes	Yes - forwarded transparently
RFC 3608	SIP Extension Header Field for Service Route Discovery During Registration	Yes	No
RFC 3611	RTCP-XR	Yes	No
RFC 3665	SIP Basic Call Flow Examples	Yes	Yes
RFC 3666	SIP to PSTN Call Flows	Yes	Yes - forwarded transparently
RFC 3680	A SIP Event Package for Registration (IMS)	Yes	No
RFC 3711	The Secure Real-time Transport Protocol (SRTP)	Yes	Yes
RFC 3725	Third Party Call Control	Yes	Yes
RFC 3824	Using E.164 numbers with SIP (ENUM)	Yes	Yes
RFC 3842	MWI	Yes	Yes
RFC 3891	"Replaces" Header	Yes	Yes
RFC 3892	The SIP Referred-By Mechanism	Yes	Yes
RFC 3903	SIP Extension for Event State Publication	Yes	Yes
RFC 3911	The SIP Join Header	Partial	No
RFC 3959	The Early Disposition Type for SIP	Yes	No
RFC 3960	Early Media and Ringing Tone Generation in SIP	Partial	Partial
RFC 3966	The tel URI for Telephone Numbers	Yes	Yes
RFC 4028	Session Timers in the Session Initiation Protocol	Yes	Yes
RFC 4040	RTP payload format for a 64 kbit/s transparent call - Clearmode	Yes	Yes - forwarded transparently
RFC 4117	Transcoding Services Invocation	Yes	No
RFC 4235	Dialog Event Package	Partial	Partial
RFC 4240	Basic Network Media Services with SIP - NetAnn	Yes	Yes - forwarded transparently
RFC 4244	An Extension to SIP for Request History Information	Yes	Yes

RFC	Description	Gateway	SBC
RFC 4320	Actions Addressing Identified Issues with SIP Non-INVITE Transaction	Yes	Yes
RFC 4321	Problems Identified Associated with SIP Non-INVITE Transaction	Yes	Yes
RFC 4411	Extending SIP Reason Header for Preemption Events	Yes	Yes - forwarded transparently
RFC 4412	Communications Resource Priority for SIP	Yes	Yes - forwarded transparently
RFC 4458	SIP URIs for Applications such as Voicemail and Interactive Voice Response	Yes	Yes - forwarded transparently
RFC 4475	SIP Torture Test Messages	Yes	Yes
RFC 4497 or ISO/IEC 17343	Interworking between SIP and QSIG	Yes	Yes - forwarded transparently
RFC 4568	SDP Security Descriptions for Media Streams for SRTP	Yes	Yes
RFC 4715	Interworking of ISDN Sub Address to sip isub parameter	Yes	Yes - forwarded transparently
RFC 4730	A SIP Event Package for Key Press Stimulus (KPML)	Partial	No
RFC 4733	RTP Payload for DTMF Digits	Yes	Yes
RFC 4904	Representing trunk groups in tel/sip URIs	Yes	Yes - forwarded transparently
RFC 4961	Symmetric RTP and RTCP for NAT	Yes	Yes
RFC 5022	Media Server Control Markup Language (MSCML)	Yes	No
RFC 5079	Rejecting Anonymous Requests in SIP	Yes	Yes
RFC 5627	Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP	Yes	Yes - forwarded transparently
RFC 5628	Registration Event Package Extension for GRUU	Yes	No
RFC 5806	Diversion Header, same as draft-levy-sip-diversion-08	Yes	Yes
RFC 6035	SIP Package for Voice Quality Reporting Event, using sip PUBLISH	Yes	No
ECMA-355, ISO/IEC 22535	QSIG tunneling	Yes	Yes - forwarded transparently

RFC	Description	Gateway	SBC
draft-ietf-sip-privacy-04.txt	SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header	Yes	Yes
draft-levy-sip-diversion-08	Diversion Indication in SIP	Yes	Yes
draft-ietf-sipping-cc-transfer-05	Call Transfer	Yes	Yes
draft-ietf-sipping-realtimefax-01	SIP Support for Real-time Fax: Call Flow Examples	Yes	Yes - forwarded transparently
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection	Yes	Yes
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol	Yes	Yes
draft-ietf-sip-connect-reuse-06	Connection Reuse in SIP	Yes	Yes
draft-johnston-sipping-cc-uui-04	Transporting User to User Information for Call Centers using SIP	Yes	Yes - forwarded transparently
draft-mahy-iptel-cpc-06	The Calling Party's Category tel URI Parameter	Yes	Yes - forwarded transparently

7.2 SIP Message Compliancy

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

7.2.1 SIP Functions

The device supports the following SIP Functions:

Table 7-2: Supported SIP Functions

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

7.2.2 SIP Methods

The device supports the following SIP Methods:

Table 7-3: Supported SIP Methods

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

7.2.3 SIP Headers

The device supports the following SIP Headers:

Note: The following SIP headers are not supported:

- Encryption
- Organization

- Accept
- Accept–Encoding
- Alert-Info
- Allow
- Also
- Asserted-Identity
- Authorization
- Call-ID
- Call-Info
- Contact
- Content-Disposition

- Content-Encoding
- Content-Length
- Content-Type
- Cseq
- Date
- Diversion
- Expires
- Fax
- From
- History-Info
- Join
- Max-Forwards
- Messages-Waiting
- MIN-SE
- P-Associated-URI
- P-Asserted-Identity
- P-Charging-Vector
- P-Preferred-Identity
- Priority
- Proxy- Authenticate
- Proxy- Authorization
- Proxy- Require
- Prack
- Reason
- Record- Route
- Refer-To
- Referred-By
- Replaces
- Require
- Remote-Party-ID
- Response- Key
- Retry-After
- Route
- Rseq
- Session-Expires
- Server
- Service-Route
- SIP-If-Match
- Subject
- Supported
- Target-Dialog
- Timestamp
- To
- Unsupported

- User- Agent
- Via
- Voicemail
- Warning
- WWW- Authenticate

7.2.4 SDP Fields

The device supports the following SDP fields:

Table 7-4: Supported SDP Fields

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

7.2.5 SIP Responses

The device supports the following SIP responses:

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

7.2.5.1 1xx Response – Information Responses

Table 7-5: Supported 1xx SIP Responses

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

7.2.5.2 2xx Response – Successful Responses

Table 7-6: Supported 2xx SIP Responses

2xx Response	
200	OK
202	Accepted

7.2.5.3 3xx Response – Redirection Responses

Table 7-7: Supported 3xx SIP Responses

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

7.2.5.4 4xx Response – Client Failure Responses

Table 7-8: Supported 4xx SIP Responses

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

4xx Response		Comments
420	Bad Extension	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
423	Interval Too Brief	The device does not generate this response. On reception of this message the device uses the value received in the Min-Expires header as the registration time.
433	Anonymity Disallowed	If the device receives a 433 Anonymity Disallowed, it sends a DISCONNECT message to the PSTN with a cause value of 21 (Call Rejected). In addition, the device can be configured, using the Release Reason Mapping, to generate a 433 response when any cause is received from the PSTN side.
480	Temporarily Unavailable	If the device receives a 480 Temporarily Unavailable response, it notifies the User with a Reorder Tone. This response is issued if there is no response from remote.
481	Call Leg/Transaction Does Not Exist	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
482	Loop Detected	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
483	Too Many Hops	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
484	Address Incomplete	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
485	Ambiguous	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
486	Busy Here	The SIP device generates this response if the called party is off-hook and the call cannot be presented as a call waiting call. Upon receipt of this response, the device notifies the User and generates a busy tone.
487	Request Canceled	This response indicates that the initial request is terminated with a BYE or CANCEL request.
488	Not Acceptable	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
491	Request Pending	When acting as a UAS: the device sent a re-INVITE on an established session and is still in progress. If it receives a re-INVITE on the same dialog, it returns a 491 response to the received INVITE. When acting as a UAC: If the device receives a 491 response to a re-INVITE, it starts a timer. After the timer expires, the UAC tries to send the re-INVITE again.

7.2.5.5 5xx Response – Server Failure Responses

Table 7-9: Supported 5xx SIP Responses

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

7.2.5.6 6xx Response – Global Responses

Table 7-10: Supported 6xx SIP Responses

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

AudioCodes

Release Notes Ver. 6.6

www.audiocodes.com