Release Notes

AudioCodes Media Gateways, Session Border Controllers & MSBRs

Mediant™ Series Media Gateways, Session Border Controllers (SBC) & Multi-Service Business Routers (MSBR)

Version 6.8

audiocodes

Table of Contents

List of Tables

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: August-27-2019

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

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

Related Documentation

Document Name
Mediant 500 E-SBC Hardware Installation Manual
Mediant 500 E-SBC User's Manual
Mediant 500 MSBR Hardware Installation Manual
Mediant 500 MSBR User's Manual
Mediant 500L MSBR Hardware Installation Manual
Mediant 500L MSBR User's Manual
Mediant 800B Gateway and E-SBC Hardware Installation Manual

Document Name
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800B MSBR Hardware Installation Manual
Mediant 800B MSBR User's Manual
Mediant 1000B Gateway and E-SBC Hardware Installation Manual
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 3000 SIP Hardware Installation Manual
Mediant 3000 SIP User's Manual
Mediant 2600 E-SBC Hardware Installation Manual
Mediant 2600 E-SBC User's Manual
Mediant 4000 SBC Hardware Installation Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant 9000 SBC Hardware Installation Manual
Mediant SE SBC Installation Manual
Mediant VE SBC Installation Manual
Mediant Server & Virtual Editions SBC User's Manual
CLI Reference Guide

Document Revision Record

LTRT	Description
27389	G.722 changed to DSP Template #9 instead of #10 for Mediant 3000 capacity
27374	MSBR Patch Release 6.80A.375.004
27352	MSBR Patch Release 6.80A.371.003
27279	MSBR Patch Release 6.80A.369.004
27274	SBC/Gateway Patch Release 6.80A.368.001
27269	MSBR Patch Release 6.80M.597 (was 6.80M.596.003)
27266	MSBR Patch Release 6.80M.596.003 (was 6.80M.596)
27264	MSBR Patch Release 6.80M.596 (was 6.80M.595.002)
27263	MSBR Patch Release 6.80A.365.002 MSBR Patch Release 6.80M.595.002
27255	MSBR Patch Release 6.80A.358.003
27102	MSBR Patch Release 6.80A.352
27098	MSBR Patch Release 6.80M.591.004
27097	SBC/Gateway Patch Release 6.80A.346.005
27094	SBC/Gateway Patch Release 6.80A.338.003; MSBR Patch Release 6.80A.347.001
27086	Patch Release 6.80A.338.003; typo in Patch Release 6.80A.339.001 (Section 4.13)

LTRT	Description
27085	Patch Release 6.80A.339.001
27082	Patch Release 6.80M.589.007
27081	Patch Release 6.80A.335.005
26996	Patch Release 6.80A.333.004
26992	Patch Release 6.80M.588.002
26989	Patch Release 6.80A.328.004
26988	Patch Release 6.80A.330
26982	Patch Release 6.80A.323.002
26977	Patch Release 6.80AR.317.001
26975	Patch Release 6.80M.584.002
26974	Patch Release 6.80A.317.001
26973	Patch Release 6.80A.316.005
26967	Patch Release 6.80A.311.003
26965	Patch Release 6.80A.310.002
26960	Patch Release 6.80A.308.504
26959	Patch Release 6.80A.308.003
26954	Patch Release 6.80A.306.006 (Resolved Constraints)
26952	Patch Release 6.80A.303.006 (Resolved Constraints)
	Interworking BRI Call Forwarding Services to SIP
26949	Patch Release 6.80A.300.009 (Resolved Constraints)
26945	Patch Release 6.80A.298.004 (Resolved Constraints)
26941	Version 6.80A.295 release (Constraints and Resolved Constraints)
	Registered users capacity
	G.727 codec removed.
26939	Version 6.80A.292 release (Constraints and Resolved Constraints)
	Overlap Dialing using SIP INFO Messages
26937	Mediant SE Network Cards Support Modified
	Low-Capacity Mediant VE SBC and Hyper-V Support
	High-capacity Mediant VE SBC with 4 vCPUs Modified
	RFC 6035 Support by SBC Application
26934	Routing to Port Specified in Request-URI
	Media Realm with Multiple Port Ranges and Interfaces
	Lock/Unlock per Trunk Group
	New Out-of-Service Behavior
	CDR Field Customization for Syslog and Stored CDRs
	CDR Local Storage

LTRT	Description
	Enhanced Q.931 ISDN Traces
	Updated to write-and-backup Command
26232	Mediant 4000B SBC
	Allowed Video Coders (Software Feature Key removed)
	Capacity for Mediant 4000B SBC
26230	Capacity Tables
26929	CDR History Storage
26928	Full VRF Support
	Removing Quotations from Display Name using Message Manipulation
	Play User-defined Tone for Specific Q.931 Release Codes
	Auto Provisioning using USB
	SNMP Trap Binding to Source Address or VRF
26927	DHCP Server Functionality
	Enhanced NAT Configuration
	CLI Wizard Tool
	Fax Detection and Negotiation for SIP Entities (modified)
	Debug Capture on Physical VoIP Interfaces in CLI (modified)
26926	Mediant 500L MSBR
	Mediant 800B Platform
	Wi-Fi Button
	E1/T1 WAN Interfaces
	Secure LDAP Connection using TLS
	Disabling Analog Ports
	Re-Initialization with "Purified" Configuration
	Debug Captures to FTP Server
	New Data-Router Software Features
	Zero Configuration Certificate for Automatic Update
	TR-098 Data Model for TR-069
	Remote Trigger for TR-069 Connection Request using SIP NOTIFY
	Binding to All VRFs
	DHCP Option 43 for Obtaining URL of ACS
	Capacity for Mediant 9000 SBC & Mediant SE SBC (High Capacity)
	Mediant 800 Capacity for 1/2/3 x BRI assembly
26924	E1/T1 Support on Mediant 500 E-SBC
	Show VoIP ARP Table
	Show Ethernet Device Table in CLI

LTRT	Description
	Default SIP Port 5060 added to Outgoing Messages
	URI Type in Outgoing SIP Diversion Header
	UDP Port Spacing
	Access to CLI for All User Levels
	Configurable Trunk Name
	FXO Pulse Dial Generation
	Configurable Analog Port Name
	Automatic Archiving of Configuration File
	Debug Level according to CPU Usage
26923	Changed Name of CLI Command for UseDifferentRTPportAfterHold ini File Parameter
	Access to CLI for All User Levels
	E1/T1 Support on Mediant 500 E-SBC
26922	SIP-based Media Recording for SRTP Sessions
	LDAP-based Management User Login Authentication
	Timeout for ISDN Release Message before Releasing Channel
	Disabling SIP 503 Response when Device Overloaded
	Pre-Classification SIP Message Manipulation
	Collect Call Detection in Reverse Charging Indication IE of ISDN Setup
	Status Display of SBC User Registration per AOR in CLI
	Web Activity Notifications to Syslog in CLI
26921	New Mediant 9000 SBC
	Enhanced Server Support on Mediant SE
	Enhanced Hypervisor Support on Mediant VE
	Enhanced VM Support on Mediant VE
	Handling SBC Refresh Session Requests
	Stop Keep-Alive with Proxy when all Trunks of Trunk Group 1 Down
	Support for SRTP with SRS for SIPRec
	Play Music-on-Hold from PRT File for SBC Calls
	Three-Way Conferencing using Third-Party Conferencing Server
	Increase in SRD and SIP Interface Tables
	Rate Limiting User Registration Requests
	Random Change of Expiry Time of User Registration/Subscription
	Destination of In-dialog SUBSCRIBE Requests
	TLS Versions 1.1 and 1.2 Support
	Multiple TLS Certificates

LTRT	Description
	SIP-PSTN Mapping of CPC for MFC-R2 Variant Argentina
	HA Support for Mediant 500 E-SBC and Mediant 800 Gateway & E-SBC
	Reporting QoE to SEM/EMS in Geo-Redundancy Mode
	SNMP Trap Event per Proxy Server State
	PM MIBs for SIP Transactions per Second
	PM MIBs for HA
	PM MIBs for Attempted SBC Calls
	PM MIBs for Established SBC Calls
	PM MIB for All Busy Channels per Trunk Group
	Enhanced Debug Level and Reporting
	Test Call Enhancements
	Up/Down buttons in Configuration Tables
	Signaling-Media Sessions and User Registration (Mediant SW)
	Capacity for Mediant 8xx Series
26920	Hyper-V Support
	Port Assignment to Ethernet Groups
	Display of Number and Percentage of Active Channels per Coder
	Regex Support for ENUM Response
	Same Call-ID for Incoming and Outgoing Messages
	CRP Routing
	Generation of SRTP Key

Documentation Feedback

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

1 Introduction

This document describes the release of Version 6.8. This includes new products, new hardware features, new software features, supported call capacity and digital signal processing (DSP) templates, current constraints, and resolved constraints.

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.
- Open source software may have been added and/or amended. For further information, visit AudioCodes website at https://www.audiocodes.com/services-support/open-source/ 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 this release documentation. You can check for an updated version on AudioCodes website at https://www.audiocodes.com/library/technical-documents.

1.1 Products Supported in Version 6.8

The table below lists the products supported in Release 6.8.

Table 1-1: Products Supported in Release 6.8

Product	Telephony Interfaces					Ethernet Interfaces	Wi-Fi	WAN	USB	OSN Server
	FXS/FXO	BRI	E1/T1	T3	SDH/ SONET					
Incumbent Products										
Mediant 500 MSBR	4/1	2	1	-	-	4 GE	√	Multiple WAN: ▪ GbE ▪ Optical Fiber ▪ ADSL2+/VDSL 2 ▪ 3G Cellular (USB)	2	-
Mediant 800B MSBR	12/12	8	2	-	-	4 GE / 8 FE (PoE Optional)	√	Multiple WAN: ▪ GbE ▪ Optical Fiber ▪ 4 E1/T1 WAN ▪ ADSL2+/VDSL 2 ▪ SHDSL ▪ 3G Cellular (USB)	2	√
Mediant 800B Gateway & E-SBC	12/12	8	2	-	-	4 GE 8 FE			2	√
Mediant 1000B Gateway & E-SBC	24/24	20	6/8	-	-	6[1]			-	√

[1] These ports are provided by two on the CRMX module and four on the optional LAN Expansion module.

Product	Telephony Interfaces					Ethernet Interfaces	Wi-Fi	WAN	USB	OSN Server
	FXS/FXO	BRI	E1/T1	T3	SDH/ SONET					
Mediant 3000 Gateway & E-SBC	-	-	63/84	3	1+1	2 GE			-	-
Mediant 2600 E-SBC	-	-	-	-	-	8 GE			-	-
Mediant 4000 SBC	-	-	-	-	-	8 GE			-	-
Mediant SE SBC	-	-	-	-	-	12 GE			-	-
Mediant VE SBC	-	-	-	-	-	12 GE			-	-
New Products										
Mediant 500L MSBR	4/4	2				4 FE	√	Multiple WAN: ▪ GbE ▪ Optical Fiber ▪ ADSL2+/VDSL 2 ▪ SHDSL ▪ 3G Cellular (USB)	1	-
Mediant 500 E-SBC (see Section 2.2)	-	-	1/1	-	-	4 GE			2	-
Mediant 4000B SBC	-	-	-	-	-	8 GE	-	-	-	√
Mediant 9000 SBC (see Section 2.3)	-	-	-	-	-	12 GE			-	-

Notes:

- Product support and hardware configurations may change without notice for the GA release and also for subsequent 6.8 patch releases. Currently available hardware configurations are listed in AudioCodes Price Book. For further enquiries, please contact your AudioCodes sales representative.
- Figures listed in the table above are maximum values per interface. However, for available hardware configurations including combinations of the supported interfaces, contact your AudioCodes sales representative.
- A hardware revision upgrade has been made to the Mediant 800 platform, called *Mediant 800B*. For more information, see Section 2.5 on page 26.
- Mediant 850 MSBR has been replaced by Mediant 800B MSBR, offering the same functionality. Homologation is not affected; the Mediant 800B MSBR maintains the same homologation as Mediant 850 MSBR
- For Mediant SE SBC, software upgrade from Version 6.4 to 6.8 using the Web interface's Software Upgrade Wizard is currently not supported. Customers who require such a software upgrade should contact AudioCodes support for a detailed upgrade procedure.

1.2 Released Software Revision Record

This section lists the software versions released in Version 6.8.

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

1.2.1 SBC and Media Gateway Series

The following table lists the SBC and Media Gateway software versions released in Version 6.8.

Table 1-2: SBC and Media Gateway Software Revision Record

Software Version	Date
General Availability (GA)	February 2014
6.80A.292	November 2015
6.80A.295	December 2015
6.80A.298.004	January 2015
6.80A.300.009	February 2016
6.80A.303.006	March 2016
6.80A.306.006	April 2016
6.80A.316.005	August 2016
6.80A.323.002	October 2016
6.80A.328.004	December 2016
6.80A.333.004	February 2017
6.80A.338.003	April 2017
6.80A.346.005	July 2017
6.80A.368.001	July 2018

1.2.2 MSBR Series

The following table lists the MSBR software versions released in Version 6.8.

Table 1-3: MSBR Software Revision Record

Software Version	Date
General Availability (GA)	February 2014
6.80A.308.003	April 2016
6.80A.308.504	May 2016
6.80A.310.002	June 2016
6.80A.311.003	June 2016
6.80A.317.001	August 2016
6.80M.584.002	August 2016
6.80AR.317.001	September 2016
6.80A.323.002	October 2016
6.80A.330	December 2016
6.80M.588.002	January 2017
6.80A.335.005	March 2017
6.80M.589.007	March 2017
6.80A.339.001	April 2017
6.80A.347.001	July 2017
6.80M.591.004	July 2017
6.80A.352	October 2017
6.80A.365.002	April 2018
6.80M.597	June 2018
6.80A.369.004	August 2018
6.80A.371.003	December 2018
6.80A.375.004	May 2019

1.3 Product Naming Conventions in this Document

Throughout this document, the following terms, unless otherwise explicitly specified, are used to represent AudioCodes products:

- **Mediant 5xx:**
  - Mediant 500 E-SBC
  - Mediant 500 MSBR
  - Mediant 500L MSBR
- **Mediant 5xx MSBR:**
  - Mediant 500 MSBR
  - Mediant 500L MSBR
- **Mediant 8xx:**
  - Mediant 800B Gateway & E-SBC
  - Mediant 800 Gateway & E-SBC
  - Mediant 800B MSBR
  - Mediant 800 MSBR
- **Mediant 1000B:**
  - Mediant 1000B Gateway & E-SBC
- **Mediant Non-Hybrid SBC (i.e., no Gateway functionality; only SBC):**
  - Mediant 2600 E-SBC
  - Mediant 4000 SBC
  - Mediant 9000 SBC
  - Mediant Virtual Edition (VE) SBC
  - Mediant Server Edition (SE) SBC
- **Mediant SW:**
  - Mediant VE SBC
  - Mediant SE SBC
- **Mediant MSBR:**
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
  - Mediant 800 MSBR

This page is intentionally left blank.

2 New Products

This chapter lists new products introduced in Release 6.8.

2.1 Mediant 500L MSBR

AudioCodes' new Mediant 500L MSBR is a cost-optimized, multi-service business router (MSBR) and session border control (SBC) in one box, providing the following interfaces:

- Multiple WAN, depending on ordered configuration:
  - Single Gigabit Ethernet copper (10/100/1000Base-T) unshielded twisted pair (UTP) interface port
  - Dual-mode of 1.25 Gbps Optical Fiber Small Form-Factor Pluggable (SFP)
  - ADSL2+ / VDSL2
  - SHDSL
  - 3G Cellular WAN access (primary or backup), using a USB modem
- Four Fast Ethernet (10/100Base-T) LAN ports (RJ-45).
- One USB port for optional USB storage services and 3G cellular WAN modem.
- Optional PSTN telephony interfaces:
  - Up to four FXS port interfaces
  - Up to four FXO port interfaces
  - Two ISDN BRI port interfaces, supporting up to four voice channels as well as PSTN fallback
- (Optional) Wireless LAN 802.11n/b/g (Wi-Fi) access point, providing two integrated, multiple-input and multiple-output (MIMO) 2Tx/2Rx antennas that operate in the 2.4 GHz frequency range.
- Serial console port (RJ-45) for device management.

Notes:

- Available hardware configurations are listed in AudioCodes Price Book. For further enquiries, please contact your AudioCodes sales representative.
- Product support and hardware configurations may change without notice.

2.2 Mediant 500 E-SBC

AudioCodes Mediant 500 Enterprise Session Border Controller (E-SBC) is a compact, high performance VoIP connectivity solution for small enterprises and branch office locations. The Mediant 500 E-SBC provides the following interfaces:

- Four Gigabit Ethernet (10/100/1000Base-T) LAN ports (RJ-45)
- Single E1/T1 interface
- Two USB ports for optional USB storage services
- Serial console port (RJ-45) for device management

Note: Product support and hardware configurations may change without notice. Currently available hardware configurations are listed in AudioCodes Price Book. For further enquiries, please contact your AudioCodes sales representative.

2.3 Mediant 4000B SBC

This new product is an improved Mediant 4000, supporting a more advanced multicore CPU module as well as an increased number of Media Processing Modules (MPM) modules (DSP devices), providing greater capacity of media sessions and transcoding sessions.

The Mediant 4000B product is offered in three configurations:

- Mediant 4000B chassis without additional MPM modules (where little or no transcoding is required)
- Mediant 4000B chassis with up to three MPM modules for transcoding applications
- Mediant 4000B chassis with OSN4 server for third-party applications such as an IP PBX, and with up to two OSN hard drive modules (HDD or SSD)

2.4 Mediant 9000 SBC

The Mediant 9000 expands the Mediant SBC family and provides a solution for hosted services and large enterprise deployments requiring 2,000 to 16,000 voice sessions. Applying a 1:4 concentration ratio, means that Mediant 9000 can serve enterprises of up to 64,000 users, thus, making it suitable for the largest of the world's enterprises.

The Mediant 9000 can also fill the role of an Access SBC at the Service Provider's domain, providing interoperability, security and quality assurance that Service Providers need to connect to their enterprise and residential customers.

- 1U chassis
- 12 Gigabit Ethernet ports (can be grouped into pairs for active-standby port redundancy, providing up to 6 Ethernet groups)
- Power redundancy
- 1+1 High Availability (using two Mediant 9000 devices)

2.5 Mediant 800B Platform

AudioCodes has released a hardware revision upgrade to the Mediant 800 platform, referred to as *Mediant 800B*. The Mediant 800B platform is now used for the Mediant 800 Gateway & E-SBC and Mediant 800 MSBR.

The Mediant 800B provides the following enhancements:

- Enhanced performance, offering higher SBC capacity (supported from Software Version 6.8). For capacity figures, see Section 5.1 on page 235.
- The RS-232 port interface has been changed to a standard RJ-45 connector, replacing the PicoBlade™ connector type.
- (Mediant 800B MSBR Only) Multiple WAN interfaces support for WAN redundancy and load balancing. The number and type of WAN interfaces depend on the ordered model.
- (Mediant 800B MSBR Only) Additional USB port (two USB ports), allowing the use of both 3G-cellular WAN modem and USB storage services.
- (Mediant 800B MSBR Only) Data routing throughput has been increased from 120 to 200 KPPS.

Notes:

- Software functionality of the Mediant 800B (except for the above mentioned improvements) remains the same as the functionality supported on the Mediant 800.
- The Mediant 800 and Mediant 800B platforms use the same firmware file (cmp).

3 Gateway and SBC Series

This chapter describes new features, known constraints and resolved constraints relating to Gateway and SBC functionalities.

3.1 Version GA

This section describes new features, constraints and resolved constraints for the GA version.

3.1.1 New Features

This section describes new features.

3.1.1.1 E1/T1 Interface Support

This feature provides support for a single E1/T1 interface on the Mediant 500 E-SBC and Mediant 500 MSBR.

Applicable Products: Mediant 500 E-SBC; Mediant 500 MSBR.

3.1.1.2 Additional E1/T1 Interface Support

This feature provides support for additional E1 and T1 interfaces provided by the Mediant 1000B Gateway & E-SBC. The device now supports up to six E1 and eight T1 port interfaces. Up until this release, the device supported up to four E1/T1 interfaces. As a result of this increase in spans, the device now supports up to 192 voice channels.

Applicable Products: Mediant 1000B.

3.1.1.3 Additional MPM Module Support

This feature provides support for an additional Media Processing module (MPM) that can be housed in the Mediant 1000B Gateway & E-SBC chassis. Thus, the device can now be installed with up to four MPMs (instead of three), providing an increase in maximum DSP resources (to 192) for media processing.

Applicable Products: Mediant 1000B.

3.1.1.4 Wi-Fi Button

This feature provides support for a new Wi-Fi button that can be used to enable or disable the Wi-Fi functionality. This button is located on the front panel of the device.

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

3.1.1.5 E1/T1 WAN Interface Support

This feature provides support for up to four E1/T1 WAN interfaces. The device can use the E1/T1 WAN Data Service Unit/Channel Service Unit (DSU/CSU) port interface to transmit and receive data using IP over Point-to-Point Protocol (PPP) framing (up to two separate links), IP over High-Level Data Link Control (HDLC) framing (up to two separate links), or bundling both physical links into a single logical link using IP over Multilink Point-to-Point Protocol (ML-PPP) framing (RFC 1717).

Applicable Products: Mediant 800B MSBR.

3.1.1.6 Enhanced Server Support on Mediant SE SBC

This feature provides enhanced support of servers on which the Mediant SE SBC can be installed:

Resource	Server
Server	▪ Low-capacity servers: ✓ HP ProLiant DL120 G7 ✓ HP ProLiant DL320e G8 ▪ High-capacity server: HP ProLiant DL360p G8
CPU	▪ DL120: Intel Xeon E3-1220 (4 cores, 3.1 GHz, 8M Cache) ▪ DL320e: Intel Xeon E3-1220v2 (4 cores, 3.1 GHz, 8M Cache) ▪ DL360p: Intel Xeon E5-2690 (8 cores, 2.9 GHz, 20M Cache)
Memory	▪ DL120 / DL320e: 16 GB ▪ DL360p: 64 GB
Network Cards	One of the following add-on network cards may be used, providing up to 12 GE ports (including on-board ports): ▪ NC365T ▪
Disk	Mechanical hard drive, 40 GB or more, no RAID
Installation From	CD /DVD drive
Installation Interface	VGA Monitor and Keyboard

Applicable Products: Mediant SE SBC.

3.1.1.7 Single Preconfigured Virtual Network on Mediant VE

This feature provides support for allowing the Mediant VE SBC to be hosted in a virtual machine environment where only one virtual network is pre-configured. Up until this release, it required two preconfigured virtual networks.

Applicable Products: Mediant VE SBC.

3.1.1.8 Microsoft Hyper-V Support on Mediant VE SBC

A new profile supporting a single virtual CPU (vCPU) has been introduced and is referred to as the Low Capacity SBC. This feature also provides support for the Mediant VE Low Capacity SBC to be installed as a guest in a virtual machine environment that is hosted by Microsoft Hyper-V Server (Windows 2012 R2). Up until this release, the device could be installed only on VMware® vSphere Hypervisor (ESXi).

Applicable Products: Mediant VE SBC.

3.1.1.9 Enhanced VM Support on Mediant VE SBC

This feature provides support for enhanced support for the virtual machine on which the Mediant VE SBC runs:

- Virtual CPU:
  - Low-capacity SBC: 1 vCPU
  - High-capacity SBC: 4 vCPUs - when using 4 cores (as in the previous version), the number of supported sessions has been increased. This is supported only on VMware® vSphere Hypervisor (ESXi).
- Memory:
  - Low-capacity SBC: 2 GB

- High-capacity SBC: 4 GB

- Disk space: 10 GB

Applicable Products: Mediant VE SBC.

3.1.1.10 DHCP Server Functionality

This feature provides support for the device to act as a Dynamic Host Configuration Protocol (DHCP) server that assigns and manages IP addresses from a user-defined address pool for DHCP clients. The clients are typically IP phones (such as AudioCodes 400HD IP Phone family series) that are connected to the device's LAN port. When a client on the LAN requests an IP address, the DHCP server allocates one from the address pool. The DHCP server can also be configured to supply additional information (DHCP Options) to requesting clients such as IP addresses of the TFTP server, DNS server, NTP server, and default router (gateway). DHCP server functionality complies with IETF RFC 2131 and RFC 2132.

The DHCP server can service up to the following number of DHCP clients:

- 800 - Mediant 500 Gateway & E-SBC; Mediant 800 Gateway & E-SBC
- 600 - Mediant 1000B Gateway & E-SBC
- 10,000 - Mediant 2600 E-SBC; Mediant 4000 SBC
- 25,000 - Mediant 9000 SBC; Mediant SW

The main configuration of the DHCP server is done in the DHCP Servers table (DhcpServer). This table configures the DHCP address pool and "well known" DHCP Options (mentioned earlier), and assigns the DHCP server to an IP network interface (listed in the Interface table) on which it operates. The DHCP server can also be configured:

- To service only DHCP clients whose DHCPDiscover requests contain a specific value for DHCP Option 60 (Vendor Class Identification). For example, Option 60 can be configured with a unique type of IP Phone model (e.g., "440HD") to allow the DHCP server to differentiate it from other DHCP clients and to process their requests accordingly. This is configured in the DHCP Vendor Class table (DhcpVendorClass).
- With additional DHCP Options to send the DHCP client. The DHCP Options can be configured with a DHCP code (1 to 254), value and value format type (ASCII, IP address or hex). For example, the Cisco proprietary DHCP Option "150" for defining multiple TFTP server addresses can be configured, and with the value "192.168.10.5,192.168.10.10" and type "IP address". This is configured in the DHCP Option table (DhcpOption).
- To allocate static ("reserved") IP addresses to specific clients defined by MAC address. In other words, the DHCP server will always allocate the same IP address to the specified client. This is configured in the DHCP Static IP table (DhcpStaticIP).

DHCP clients currently serviced by the DHCP server are displayed in the DHCP Clients table. This table also lets users delete a DHCP client, terminating their lease over the IP address, allowing the DHCP server to allocate the IP address to another client.

The DHCP server temporarily blacklists an allocated IP address if it detects, using Address Resolution Protocol (ARP) that two different clients are using the same IP address (i.e., an unauthorized network device).

Applicable Products: Mediant 500 Gateway & E-SBC; Mediant 800 Gateway & E-SBC; Mediant 1000B Gateway & E-SBC; Mediant 2600 E-SBC; Mediant 4000 SBC; Mediant 9000 SBC; Mediant SW.

3.1.1.11 Enhanced IP Network Configuration

This feature introduces a new Ethernet Device table that defines VLANs used by the device and their association with underlying physical interfaces (Ethernet Port Group). The

Interface table references a relevant entry in the Ethernet Device table using the new 'Underlying Device' parameter. Multiple entries in the Interface table may reference the same Ethernet Device table entry, thus implementing “multi-homing” IP configuration - multiple IP addresses on the same interface/VLAN. The Ethernet Device table may also be referenced from the Static Routes table.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.11.1 Ethernet Device Table

The new Ethernet Device Table provides the following support:

- VLANs are now configured in a new, dedicated table - Ethernet Device table (Configuration tab > VoIP > Network > Ethernet Device Table).
- VLAN configuration includes associating it with an Ethernet Port Group (*underlying interface*). This is applicable only to Mediant 5xx, Mediant 8xx, Mediant 1000B, and Mediant Non-Hybrid SBC.
- The same VLAN ID cannot be configured for more than one Ethernet Port Group.
- The Ethernet Device Table provides the Ethernet Device Status Table button, which opens the Ethernet Device Status table, displaying the status of the Ethernet devices. This table can also be opened from the path, Status & Diagnostics tab > VoIP Status menu > Ethernet Device Status Table.

  Note that an Ethernet Device that has been assigned to an IP network interface cannot be deleted. Only once the Ethernet Device has been disassociated from the IP network interface (in the Interface table) can the Ethernet Device be deleted.

Ethernet Device Table CLI: config-voip > interface network-dev 0 [DeviceTable]	Defines an underlying device, which consists of a VLAN ID associated with an Ethernet Port Group (depending on product). [DeviceTable] FORMAT DeviceTable_Index = DeviceTable_VlanID, DeviceTable_UnderlyingInterface, DeviceTable_DeviceName; [\DeviceTable] ▪ VLAN ID = Defines a VLAN ID (default is 1). ▪ Underlying Interface = Associates an Ethernet Port Group with the VLAN (mandatory field). ▪ Name = Defines a name for the Underlying Device (i.e., VLAN). This name is used to associate the VLAN with an IP network interface in the Interface table's 'Underlying Device' field, and/or with a static route in the Static Route table's 'Device Name' field. By default, the device automatically assigns a name using the following syntax: "dev <table row index>" (e.g., "dev 3"). Note: For Ethernet Device Table entries to take effect, a device reset is required.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.11.2 Interface Table

The Interface table contains the definition of IP network interfaces. The following changes have been implemented in this release:

- Interfaces are associated with corresponding VLAN (Ethernet Device), using the new 'Underlying Device' parameter.
- Interfaces sharing the same VLAN (*Underlying Device*) may not have the same IP address.
- Interfaces sharing the same VLAN (*Underlying Device*) can be on different subnets.

Underlying Device [InterfaceTable_UnderlyingDevice]	Associates the IP interface with an Ethernet device (i.e., VLAN), configured in the Ethernet Device table. This value must be identical to the string value as configured in the Ethernet Device table.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.11.3 Static Route Table

The following changes were implemented in the Static Route table.

Device Name [StaticRouteTable_DeviceName]	Associates the static route with an Ethernet device (i.e., VLAN), configured in the Ethernet Device table. The static route is used for traffic received on this Ethernet device (e.g., VLAN 400). This value must be identical to the string value as configured in the Ethernet Device table.

The Static Route Status Table button has been added to the Web page of the Static Route table. This button opens the new IP Routing Status Table page, which displays all the static routes – active and inactive. This page can also be accessed using the path, Status & Diagnostics tab > VoIP Status menu > Static Route Status.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.11.4 Online Addition of IP Network Interfaces

This feature provides support for adding IP network interfaces in the Interface table without the need to reset the device. Up until this release, such configuration required a device reset for the new settings to take effect.

The following tables, which reference the Interface table, have also been modified to support online addition of row entries:

- Media Realm
- SIP Interface
- SRD

Note that edit and delete operations in the Interface table still require a device reset. Once such operations are performed, any further modifications to the Interface table require a device reset before the settings take effect.

Applicable Products: All.

3.1.1.12 Port Assignment to Ethernet Groups

This feature provides support for assigning any of the device's ports to an Ethernet Group. The Ethernet Group can be assigned 1, 2, or no ports. Up until this release, the two port members of the Ethernet Groups were factory set and could not be changed.

As a consequence to this feature, the maximum number of Ethernet Groups has also increased, which now reflects the number of physical ports provided on the device. In other words, if the device provides eight Ethernet ports, a maximum of eight Ethernet Groups are supported. The assignment of ports to Ethernet Groups is done in the existing Ethernet Group Settings table.

Note: For Mediant 2600 and Mediant 4000, ports 1 through 6 cannot be assigned to the same Ethernet Group as ports 6 through 12. For example, an Ethernet Group containing ports 2 and 7 is invalid.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.13 Native VLAN ID for OSN Access

This feature provides support for configuring a VLAN ID associated with any application type (Media, Control, or OAMP) to access the Open Solution Network (OSN) server through the device's internal port switch. Up until this release, access to the OSN could only be done from the device's OAMP interface VLAN (by default, VLAN ID 1).

This feature is useful, for example, for separating traffic within the device, between the CMX (i.e., voice traffic), OSN (i.e., application traffic), and RMX (i.e., data traffic).

Note that this feature applies when you connect to the OSN through one of its LAN ports (on the front panel of the device). If you are connecting to the OSN through a Gigabit Ethernet port (on the rear panel of the device), this feature is not relevant.

This feature also provides configuration for enabling or disabling the Ethernet port of the internal switch that interfaces with the OSN. The port status (Up or Down) can be viewed by running the following CLI command:

```
# show system interface osn
```

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

Web: OSN Native VLAN ID CLI: configure system > interface osn > native-vlan <id> [OSNAccessVlan]	Defines the OSN Native VLAN ID. The valid value is 0 to 4000. When set to 0 (default) the OSN uses the device's OAMP VLAN ID. When set to any other value, it specifies a VLAN ID configured in the Ethernet Device table and which is assigned to a Media and/or Control application in the Interface table.
Web: Block OSN Port CLI: configure system > interface osn > shutdown [OSNBlockPort]	Enables or disables the Ethernet port of the internal switch that interfaces with the OSN. ▪ [0] = (Default) Port enabled. ▪ [1] = Port disabled.

Applicable Products: Mediant 8xx; Mediant 1000B.

3.1.1.14 Authentication of NTP Message

This feature provides support for authentication of Network Time Protocol (NTP) messages. The device can be configured to authenticate and validate the messages received from the NTP server providing the date and time. Authentication is done using an authentication key with the MD5 cryptographic hash algorithm. When this feature is enabled, NTP messages received without authentication are ignored.

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

Web: NTP Authentication Key Identifier CLI: configure system > ntp > auth-key-id [NtpAuthKeyId]	Defines the NTP authentication key identifier. The identifier must match the value configured on the NTP server. The NTP server may have several keys configured for different clients; this number identifies which key is used. The valid value is 1 to 65535. The default is 0 (i.e., no authentication is done).
Web: NTP Authentication Secret Key CLI: configure system > ntp > auth-key-md5 [ntpAuthMd5Key]	Defines the secret authentication key shared between the device (client) and the NTP server. The valid value is a string of up to 32 characters. By default, no key is defined.

Applicable Products: All.

3.1.1.15 Display of Voice ARP Cache Table in CLI

This feature provides support for displaying the Address Resolution Protocol (ARP) cache table for the device's voice functionality. The feature displays the mapping of Ethernet/MAC addresses to IP addresses for the hosts which have previously ARP'ed the device.

To support this feature the following new CLI command has been added (from the basic command mode):

```
# show voip arp
```

For example:

```
IP Address  MAC Address     Interface       Type
10.8.2.19                    8c:89:a5:8f:9b:21   eth3.1    stale
10.8.2.225                   00:e0:81:ca:e9:cc   eth3.1    stale
10.8.0.1                     2c:21:72:a0:b9:81   eth3.1    reachable
End of arp table, 3 entries displayed.
```

Applicable Products: All.

3.1.1.16 Display of VoIP Interface Table in CLI

This feature provides support for displaying the VoIP Interface table in the CLI. To support this feature the following new command has been added (from the basic command mode):

```
# show voip interface network desc
```

Applicable Products: All.

3.1.1.17 Display of VoIP Ethernet Ports in CLI

This feature provides support for displaying the VoIP ports in the CLI. The information displayed includes the port number, port name, port MAC address, speed, duplex mode, native VLAN ID, and status of the Ethernet link ("UP" or "DOWN").

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

```
# show voip ports
```

For example:

```
Port Num  Port Name  MAC Address       Speed     Duplexity  Link Status Native VLAN
--------  ---------  ------------      ------    ---------  -----------  ----------
1          GE_1      00:90:8f:3b:46:29 100Mbps     Full       UP            1
2          GE_2      00:90:8f:3b:46:29 1Gbps       Full       DOWN          0
```

Applicable Products: Mediant 500 E-SBC; Mediant 800 E-SBC; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.18 Display of Ethernet Port Group Members in CLI

This feature provides support for displaying the configuration and status of the Ethernet port Group Members, in the CLI. For each Group Member, the name, mode of operation, status, number of ports whose link is up, and ports comprising the group are displayed.

To support this feature, the following new CLI command has been added (run from basic mode):

```
# show voip groups
```

For example:

```
G. Num    Group Name    Mode          State Uplinks    Group Members
 ------  --------------  -------------------  -----  -------  ----
 0      GROUP_1      REDUN_1RX_1TX/2    Up      1     GE_4_1 ,GE_4_2
 1      GROUP_2      REDUN_1RX_1TX/2   Down     0     GE_4_3 ,GE_4_4
```

Applicable Products: Mediant 800 E-SBC; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.19 Display of Ethernet Devices in CLI

This feature provides support for displaying the configured VoIP Ethernet Devices in the Ethernet Device table, using CLI. For each Ethernet Device, the device name, VLAN ID, and associated Ethernet port Group is displayed.

To support this feature, the following new CLI command has been added (run from basic mode):

```
# show voip devices
```

For example:

```
 D.Num   Device Name         VlanID     GroupName
 ------  ----------------  ---------  -------------
  0       vlan 1             1             GROUP_1
  1       vlan 20            20            GROUP_2
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.20 SIP Message Normalization

This feature provides support for SIP message normalization, whereby the device removes unknown SIP message elements before forwarding the message. SIP message normalization is achieved using SIP Message Manipulation rules that are tagged as "Normalize" as their Action Type in the existing Message Manipulations table. This feature is useful for SIP entities that are unable to handle SIP messages containing non-standard or unknown elements.

The device normalizes the following SIP elements:

- URLs:
  - User part is normalized, for example, the bolded area is removed:

    ```
    <sip:+1-800-229-229;phone-
    context=1@10.33.2.17;user=phone;UnknownUrlParam>
    ```

  - Unknown parameters are removed, for example, the bolded area is removed:

    ```
    <sip:+1-800-229-229;phone-
    context=1@10.33.2.17;user=phone;UnknownUrlParam>
    ```

  The resultant URL after above example normalization:

  ```
  <sip:+180022922910.33.2.17;user=phone>
  ```

- Headers:
  - Alert-Info: unknown header parameters are removed
  - P-Called-Party-ID: unknown header parameters are removed, URL is normalized
  - P-Charging-Vector: unknown header parameters are removed
  - P-Associated-URI: unknown header parameters are removed, URL is normalized
  - P-Preferred-Identity: URL is normalized
  - Diversion: unknown header parameters are removed, URL is normalized
  - P-Asserted-Identity: URL is normalized
  - Remote-Party-ID: unknown header parameters are removed, URL is normalized
  - Reason: unknown header parameters are removed
  - Max-Forwards: value is changed to 70
  - History-Info: unknown header parameters are removed, URL is normalized
  - From: unknown header parameters are removed, URL is normalized
  - To: unknown header parameters are removed, URL is normalized
  - Via: unknown header parameters are removed
  - Refer-To: unknown header parameters are removed, URL is normalized
  - Referred-By: unknown header parameters are removed, URL is normalized
  - Event: unknown header parameters are removed
  - Session-Expires: unknown header parameters are removed

- Min-SE: unknown header parameters are removed
- Min-Expires: unknown header parameters are removed
- Request-URI: URL is normalized
- Contact: unknown header parameters are removed
- Subscription-State: unknown header parameters are removed

For example:

- To header before normalization:

```
To: <sip:100;phone-context=1@10.33.2.17;user=phone;UnknownUrlParam>;UnknownHeaderlParam
```

- To header after SIP normalization (user parameter, unknown URL parameter, and unknown header parameter are removed):

```
To: <sip:100@10.33.2.17;user=phone>
```

- SDP Body: Removes unnecessary SDP fields (except v=, o=, s=, c=, t=, and r=) and unknown media with all its attributes. For example, the bolded text is removed before sending the message:

```
v=0
o=SMG 791285 795617 IN IP4 10.33.2.17
s=Phone-Call
i=A Seminar on the session description protocol
u=http://www.example.com/seminars/sdp.pdf
e=j.doe@example.com (Jane Doe)
c=IN IP4 10.33.2.26
t=0 0
m=unknown 6000 RTP/AVP 8
a=unknown
a=sendrecv
a=ptime:20
m=audio 6000 RTP/AVP 8
a=rtpmap:8 pcma/8000
a=sendrecv
a=unknown
a=ptime:20
```

- Message: Normalization of the entire message. Headers and bodies not listed below are removed while those listed are retained and normalized (if necessary and if listed as supported for normalization, as previously mentioned) :
  - Headers:
    - Request-URI
    - Via
    - Max-Forwards
    - From
    - To
    - Call-ID
    - Cseq
    - Contact
    - Record-Route
    - Route
    - Supported
    - Allow

- P-Preferred-Identity
- Diversion
- Rack
- Required
- RSeq
- Authorization
- Proxy-Authorization
- WWW-Authenticate
- Proxy-Authenticate
- Event
- Refer-To
- Referred-By
- Replaces
- User-Agent
- P-Asserted-ID
- History-Info
- Priority
- Resource-Priority
- Unsupported
- Expires
- Session-Expires
- Min-SE
- Min-Expires

- Bodies:
  - SDP
  - DTMF

To support this feature, the following optional value for SIP normalization has been added to the 'Action Type' parameter in the Message Manipulations table:

Action Type CLI: action-type [MessageManipulations_ActionType]	[7] Normalize

Applicable Products: All.

3.1.1.21 Message Manipulation Rules for IP Groups using Defined String

This feature provides support for manipulating SIP message headers where a special string value is used from an IP Group parameter, configured in the IP Group table. For example, a manipulation rule can be configured (in the Message Manipulations table) to add a SIP header to outgoing INVITE messages where the destination user of the header is taken from the IP Group.

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

- Two new fields have been added to the IP Group table for configuring up to two manipulation strings:
  - IPGroup_MsgManUserDef1
  - IPGroup_MsgManUserDef2

  Each string can include up to 30 characters. A manipulation rule can reference to only one of these parameters.
- The existing manipulation parameter for IP Groups -- *param.ipg.<src/dst>* -- has a new

sub-parameter, "user-defined.<0|1>" (param.ipg.<src/dst>.user-defined.<0-1>). This sub-parameter references to the parameters in the IP Group table where the manipulation strings are configured:

- *0* corresponds to the string configured in the IPGroup_MsgManUserDef1 field
- *1* corresponds to the string configured in the IPGroup_MsgManUserDef2 field

For example, to add the string "Joe" configured in the IPGroup_MsgManUserDef1 parameter to a new customized SIP header named "MyCustomHeader" in INVITE messages sent to this IP Group:

- IP Group table: Set the 'MsgManUserDef1' field to "Joe".
- Message Manipulations table:

Message Type	Condition	Action Subject	Action Type	Action Value
invite	-	header.MyCustomHeader	Add	param.ipg.dst.user-defined.0

In this example, the outgoing INVITE will have the following header:

```
MyCustomHeader: Joe
```

Applicable Products: All.

3.1.1.22 SIP Message Manipulation for Removing Quotation Marks from Display Name

This feature provides support for removing the quotation marks "…" enclosing a display name received in the SIP From header. For example, the quotation marks surrounding the display name in the following received From header,

```
From: "Joe" <sip:100@10.33.2.14;user=phone>;tag=1c1961797508
```

Can be removed as shown below:

```
From: Joe <sip:100@10.33.2.14;user=phone>;tag=1c1961797508
```

To support this feature, the new keyword, *quotecontrol* is used in the Action Subject field with the Action Value set to '0', in the Message Manipulations table:

Message Type	Condition	Action Subject	Action Type	Action Value
invite		header.from.quotecontrol	Remove	'0'

Applicable Products: All.

3.1.1.23 Regex Processing of ENUM Responses

This feature provides support for processing regular expression statements (regex) received in ENUM responses from ENUM (E.164 Number to URI Mapping) servers. Regex statements can also be used to manipulate the ENUM response in SIP messages, configured in the existing Message Manipulations table.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 3000; Mediant Non-Hybrid SBC.

3.1.1.24 Disabling SIP 408 Response upon Non-INVITE

This feature provides support for not sending a SIP 408 (Request Timeout) in response to non-INVITE requests, to comply with RFC 4320/4321. By default and in certain circumstances such as a timeout expiry, the device sends a SIP 408 Request Timeout in response to non-INVITE requests (e.g., REGISTER).

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

Enable non-INVITE 408	Enables the sending of SIP 408 responses upon receipt of non-

reply CLI: enbl-non-inv-408 [EnableNonInvite408Reply]	INVITE transactions. ▪ [0] Disable = SIP 408 response is not sent upon receipt of non-INVITE messages (to comply with RFC 4320). ▪ [1] Enable = (Default) SIP 408 response is sent upon receipt of non-INVITE messages, if necessary.

Applicable Products: All.

3.1.1.25 Disabling SIP 503 Response upon Device Overload

This feature provides support for disabling the sending of SIP 503 (Service Unavailable) responses upon receipt of new SIP dialog-initiating requests when the device's CPU is overloaded and thus, unable to accept and process new SIP messages. Up until this release, the device always sent this response when overloaded. Note that even if this feature is used (i.e., 503 is not sent), the device still discards the message when overloaded. This feature is applicable to SBC and Gateway calls.

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

Web: Send reject on overload CLI: configure voip/sip-definition advanced-settings/reject-on-ovrld [SendRejectOnOverload]	Disables the sending of a SIP 503 response upon receipt of a new SIP dialog-initiating request when the device is overloaded. ▪ [0] Disable ▪ [1] Enable (default)

Applicable Products: All.

3.1.1.26 Single Registration for Multiple Phone Numbers using GIN

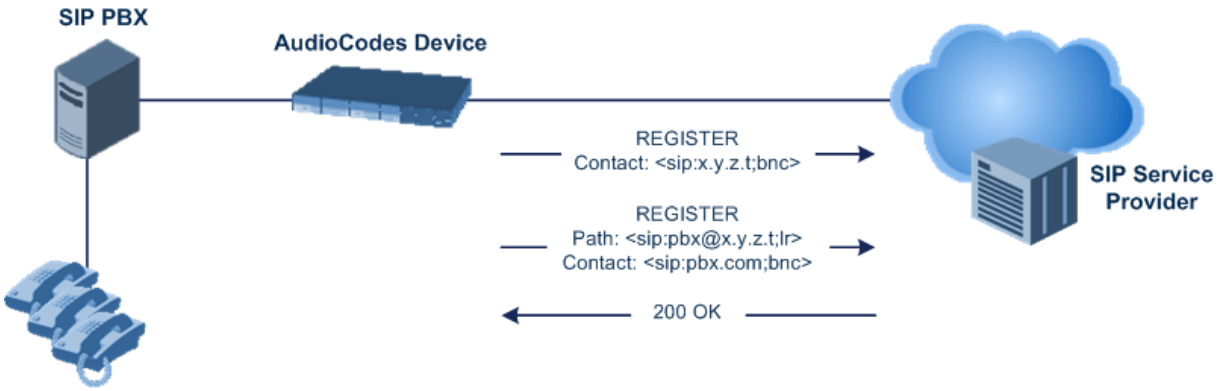
This feature provides support for the Global Identifiable Number (GIN) registration method, according to RFC 6140. The device can now perform GIN-based registration of users with a SIP registrar on behalf of a SIP PBX. In effect, the SIP PBX registers with the service provider, just as a directly hosted SIP endpoint would register. However, because a SIP PBX has multiple user agents, it needs to register a contact address on behalf of each of these. Rather than performing a separate registration procedure for each UA, GIN registration mode does multiple registrations using a single REGISTER transaction.

According to this mechanism, the SIP PBX delivers to the service provider in the Contact header field of a REGISTER request a template from which the service provider can construct contact URIs for each of the AORs assigned to the SIP PBX, and thus can register these contact URIs within its location service. These registered contact URIs can then be used to deliver to the SIP PBX inbound requests targeted at the AORs concerned. The mechanism can be used with AORs comprising SIP URIs based on global E.164 numbers and the service provider's domain name or sub-domain name.

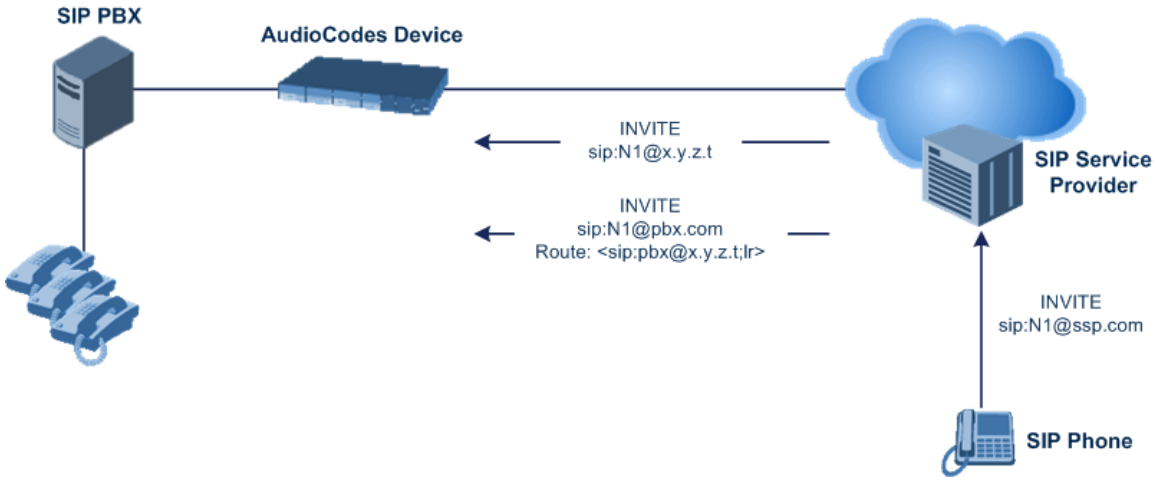
The SIP REGISTER request sent by the device for GIN registration with a SIP server provider contains the Require and Proxy-Require headers. These headers contain the token 'gin'. The Supported header contains the token 'path' and the URI in the Contact header contains the parameter 'bnc' and no user part.

```
Contact: <sip:198.51.100.3;bnc>;
```

The figure below illustrates the GIN registration process:



The figure below illustrates an incoming call using GIN:



The existing Account table represents the traditional PBX with E.164 numbers. To support this feature, the new option, GIN has been added to the 'Register' parameter in this table:

Register CLI: register [Account_Register]	Defines the registration type. ▪ [0] No ▪ [1] Regular = Regular registration. ▪ [2] GIN = Registration for legacy PBX, using Global Identification Number.

Note: This feature is applicable to both Gateway and SBC applications.

Applicable Products: All.

3.1.1.27 Default SIP Port (5060) added to Outgoing SIP Messages

This feature provides support for adding the default SIP port–5060 for TCP/UDP or 5061 for TLS–in outgoing messages for messages received without a port number. This condition also applies to manipulated messages where the resulting message has no port number. The device adds the port number to the following SIP headers: Request-Uri, To, From, P-Asserted-Identity, P-Preferred-Identity, and P-Called-Party-ID. If the message is received with a port number other than the default (i.e., 5060), for example, 5070, the port number is not changed.

An example of a SIP From header whose port was changed to 5060 is shown below:

```
From:
<sip:+4000@10.8.4.105:5060;user=phone>;tag=f25419a96a;epid=009FAB8
F3E
```

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

Display Default SIP Port	Enables adding the default SIP port 5060 to outgoing messages

CLI: display-default-sip-port [DisplayDefaultSIPPort]	that are received without a port. ▪ [0] Disable (default) ▪ [1] Enable

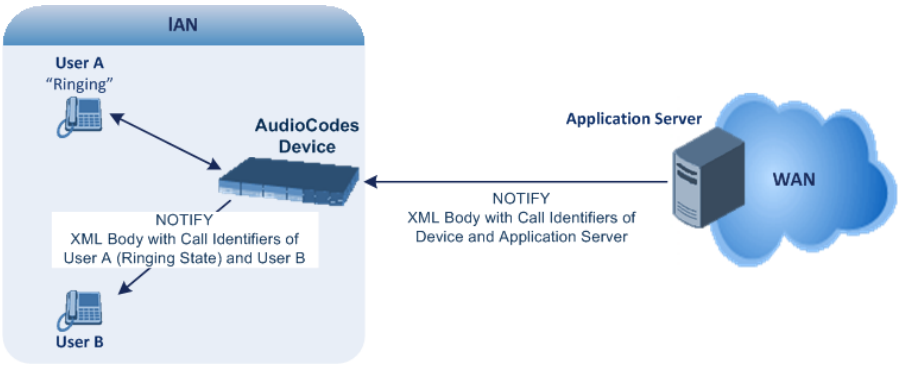
Applicable Products: All.

3.1.1.28 Interworking SBC Dialog Information in SIP NOTIFY Messages

This feature provides support for interworking dialog information (XML body) in SIP NOTIFY messages received from a remote (WAN) application server. The NOTIFY message is sent by an application server to notify a SIP client, subscribed to this service and located behind the device (LAN), of the status of another SIP client in the LAN.

For example, user B can subscribe to an application server for call pick-up service, whereby if user A's phone rings, the application server notifies user B. User B can then press a pre-configured key sequence to answer the call.

The NOTIFY message contains the XML body with call identifiers (call-id and tags). However, as the application server is located in the WAN and the SIP clients in the LAN (behind the device), the call dialog information sent by the application server reflects only the dialog between the device and itself; not that of the involved SIP clients. This is due to, for example, the device's topology hiding (e.g., IP address) of its LAN elements. This feature resolves this issue, by enabling the device to replace the call identifiers, received from the application server, with the correct call identifiers (e.g., user A and user B). Thus, users subscribed to the service (e.g., call pick-up) can receive relevant NOTIFY messages from the device and use the service. When this feature is disabled, the device forwards the NOTIFY message as is, without modifying its XML body.



Below is an example of an XML body where the call-id, tags, and URIs have been replaced by the device:

```
<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info"
version="10" state="partial"
entity="sip:alice@example.com">
<dialog id="zxcvbnm3" call-id="67402270@10.132.10.150"
local-tag="1c137249965"
remote-tag="CCDORRTDRKIKWFVBRWYM" direction="initiator">
<state event="replaced">terminated</state>
</dialog>
<dialog id="sfhjsjk12" call-id="67402270@10.132.10.150"
local-tag="1c137249965"
remote-tag="CCDORRTDRKIKWFVBRWYM" direction="receiver">
<state reason="replaced">confirmed</state>
<replaces
call-id="67402270@10.132.10.150"
local-tag="1c137249965"
remote-tag="CCDORRTDRKIKWFVBRWYM"/>
<referred-by>
sip:bob-is-not-here@vm.example.net
</referred-by>
```

```
<local>
<identity display="Jason Forster">
sip:jforsters@home.net
</identity>
<target uri="sip:alice@pc33.example.com">
<param pname="+sip.rendering" pval="yes"/>
</target>
</local>
<remote>
<identity display="Cathy Jones">
sip:cjones@example.net
</identity>
<target uri="sip:line3@host3.example.net">
<param pname="actor" pval="attendant"/>
<param pname="automaton" pval="false"/>
</target>
</remote>
</dialog>
</dialog-info>
```

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

SBC Dialog-Info Interworking CLI: sbc-dialog-info-interwork [EnableSBCDialogInfoInterworking]	Enables the parsing of call identifiers in the XML body of NOTIFY messages. ▪ [0] Disable (default) ▪ [1] Enable

Applicable Products: All.

3.1.1.29 SBC Interworking SIP Replaces Header

This feature provides support for interworking the SIP Replaces header in incoming INVITE messages. The Replaces header is used to replace an existing SIP dialog with a new dialog such as in call transfer or call pickup. For SIP entities that do not support the Replaces header, the device can now handle it locally for the SIP entity.

For example, assume that the device establishes a call between A and B. If B initiates a call transfer to C, the device receives an INVITE with the Replaces header from C. If A supports the Replaces header, the device simply forwards the INVITE as is to A; a new call is established between A and C and the call between A and B is disconnected. However, if A does not support the Replaces header, the device uses this feature to terminate the INVITE with Replaces header and handles the transfer for A. The device does this by connecting A to C, and disconnecting the call between A and B by sending a SIP BYE request to B. Note that if media transcoding is required, the device sends an INVITE to C on behalf of A with a new SDP offer.

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

Remote Replaces Behavior [IpProfile_SBCRemoteReplacesBehavior]	Enables the device to handle an incoming INVITE with Replaces header for the SIP entity that does not support this header. ▪ [0] Transparent = (Default) SIP entity supports Replaces header. The device forwards the received INVITE with Replaces header as is to the SIP entity. ▪ [1] Handle Locally = SIP entity does not support INVITE with Replaces header. The device terminates the received INVITE with Replaces header and establishes a new call between the SIP entity and the new call party. It then disconnects the call with the initial call party by sending it a SIP BYE request.

Applicable Products: All.

3.1.1.30 Session Refresh Requests Handled by SBC

This feature provides support for enabling the device to periodically refresh established SIP sessions (i.e., active calls). Up until this release, the remote user agent such as a proxy server (and when this feature is disabled) performed session refreshes.

The session refresh allows SIP user agents (UA) or proxies to determine the status of the SIP session. When a session expires, the session is considered terminated by the UAs, regardless of whether a SIP BYE was sent by one of the UAs.

The SIP Session-Expires header conveys the lifetime of the session, which is sent in re-INVITE or UPDATE requests (*session refresh requests*). The 'refresher=' parameter in the Session-Expires header (sent in the initial INVITE or subsequent 2xx response) indicates who sends the session refresh requests. If the parameter contains the value 'uac', the device performs the refreshes; if the parameter contains the value 'uas', the remote proxy performs the refreshes. An example of the Session-Expires header is shown below:

```
Session-Expires: 4000;refresher=uac
```

Thus, this feature is useful when the remote user agent does not support session refresh requests. In such a scenario, the device can be configured to perform the session refresh requests.

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

SBC Session Refreshing Policy CLI: configure voip/sbc general-setting/sbc-session-refresh-policy [SbcSessionRefreshingPolicy]	Defines the SIP user agent responsible for sending refresh requests. ▪ [0] Remote Refresher = (Default) The remote endpoint (proxy) is responsible for session refresh requests. The device indicates this to the endpoint by sending the SIP message with the 'refresher=' parameter in the Session-Expires header set to 'uas'. ▪ [1] SBC Refresher = The device is responsible for sending session refresh requests. The device indicates this to the endpoint by sending the SIP message with the 'refresher=' parameter in the Session-Expires header set to 'uac'. Note: The time values of the Session-Expires (session refresh interval) and Min-SE (minimum session refresh interval) headers can be configured using the SBCSessionExpires and SBCMinSE parameters, respectively.

Applicable Products: All.

3.1.1.31 SBC Ringback Tone Played to Transferred Party

This feature provides support for generating a ringback tone to the transferred party (transferee) during a blind call transfer. The ringback tone indicates to the transferee of the ringing of the transfer target (to where the transferee is being transferred). Thus, the device can play this ringback tone on behalf of SIP entities that do not support such a tone generation during call transfer.

Typically, the transferee hears a ringback tone only if the transfer target sends it early media. However, if the transferee was put on hold before being transferred, no ringback tone is heard.

When this feature is enabled, the device generates a ringback tone to the transferee during call transfer in the following scenarios:

- Transfer target sends a SIP 180 (Ringing) to the device.
- For non-blind transfer if the call is transferred while the transfer target is ringing and no early media occurs.
- The 'SBC Remote Early Media RTP' parameter (in the IP Profile table) is set to Delayed (used in the Lync environment), and transfer target sends a 183 Session progress with SDP offer. If early media from the transfer target has already been detected, the transferee receives RTP stream from the transfer target. If it has not been detected, the device generates a ringback tone to the transferee and stops the tone generation once RTP has been detected from the transfer target.

For any of these scenarios, if the transferee is placed on-hold by the transferor, the device retrieves the transferee from hold, sending a re-INVITE if necessary, and then plays the ringback tone.

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

SBC Play RBT To Transferee CLI: sbc-play-rbt-to-xferee [IpProfile_SBCPlayRBTTo Transferee]	Enables the device to play a ringback tone to the transferred party for call transfer. This is for the SIP entity associated with this IP Profile. ▪ [0] No (Default) ▪ [1] Yes

Applicable Products: All.

3.1.1.32 Disabling 100 Trying SIP Responses for SBC

This feature provides support for disabling the sending of 100 Trying SIP responses. Up until this release, the device always sent 100 Trying messages in response to the receipt of SUBSCRIBE or NOTIFY messages.

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

Web: SBC Enable Subscribe Trying CLI: configure voip > sbc general-setting > set sbc-subs-try [SBCSendTryingToSubscribe]	Enables the sending of 100 Trying in response to SUBSCRIBE or NOTIFY messages. ▪ [0] Disable (Default) ▪ [1] Enable

Applicable Products: All.

3.1.1.33 Match Calling Name for SBC IP-to-IP Outbound Manipulation Rules

This feature provides support for using the SIP calling name (caller ID) as a matching characteristic for determining the outbound manipulation rule in the IP-to-IP Outbound Manipulation table. The calling name appears in the SIP From header.

To support this feature, a new parameter has been added to the IP-to-IP Outbound Manipulation table:

Calling Name Prefix [IPOutboundManipulation_ CallingNamePrefix]	Defines the prefix of the calling name. The valid value is a string of up to 37 characters. By default, no prefix is defined.

Applicable Products: All.

3.1.1.34 Match Message Conditions for SBC Outbound Manipulation Rules

This feature provides support for using Condition rules as matching characteristics for determining outbound manipulation rules in the IP-to-IP Outbound Manipulation table. Condition rules, supported in previous releases, are configured in the Message Condition Table and define a required SIP message format. For example, a rule could define SIP messages whose To header contains the string "audiocodes" as its host part.

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

Message Condition [IPOutboundManipulation_ MessageCondition]	Associates a Condition rule as a matching characteristic for the outbound manipulation rule.

Applicable Products: All.

3.1.1.35 Calling Name Manipulation for SBC IP Outbound Manipulation

This feature provides support for manipulating the calling name in SIP messages for outbound manipulation, configured in the IP-to-IP Outbound Manipulation table. Up until this release, only manipulation of the SIP Request-URI user part (source and destination) for outbound SIP dialog requests was supported.

To support this feature, the 'Manipulated URI' parameter has been replaced by the new 'Manipulated Item' parameter, and the Calling Name option has been added to it:

Manipulated Item [IPOutboundManipulation_ ManipulatedURI]	Defines the item in the SIP message that you want manipulated. ▪ [0] Source URI (Default) ▪ [1] Destination URI ▪ [2] Calling Name Note: If the Source URI or Destination URI option is selected, the 'Prefix to Add' and 'Suffix to Add' parameters can be defined with up to 49 characters. If the Calling Name option is selected, the 'Prefix to Add' and 'Suffix to Add' parameters can be defined with up to 36 characters.

Applicable Products: All.

3.1.1.36 URI Type in SIP Diversion Headers for SBC

This feature provides support for specifying the Uniform Resource Identifier (URI) type–"sip", "tel", or transparent–that is to be used in the SIP Diversion header. If a different URI type appears in the header, the device overwrites it with the configured URI type. For example:

- Original Diversion header:

```
Diversion:<sip:+1447865432@uas1.isp.com>;reason=do-not-
disturb;;privacy=off
```

- New diversion header:

```
Diversion: <tel:+1447865432>;counter=1;reason=do-not-
disturb;privacy=off
```

The existing parameters, SBCDiversionMode and SBCHistoryInfoMode determine the call redirection (diversion) SIP header to use - History-Info or Diversion. If the Diversion header is used, this new feature then determines the URI type to use in the header.

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

Web: SBC Diversion URI Type CLI: sbc-diversion-uri-type (configure voip > sbc general-setting) [SBCDiversionUriType]	Defines the URI type to use in the SIP Diversion header. ▪ [0] Transparent (Default) = The device does not change the URI and leaves it as is. ▪ [1] Sip = The "sip" URI is used. ▪ [2] Tel = The "tel" URI is used.

Applicable Products: All.

3.1.1.37 Response Codes for Proxy Keep-Alive using SIP OPTIONS

The device can now be configured with a list of SIP responses that if received indicates a failure in the proxy server keep-alive mechanism using SIP OPTIONS messages. Up until this release, if any SIP response was received for the proxy keep-alive, the device assumed the proxy to be "alive". With this feature, only if a configured SIP response (for example, 407) is received, does the device consider the proxy as "down". If no responses are configured or responses received are not those configured, the proxy is considered "alive".

To support this feature, the following parameter has been added to the Proxy Sets table:

KeepAlive Failure responses [ProxySet_KeepAliveFailure	Defines SIP response codes that if received in response to a keep-alive using SIP OPTIONS, the proxy is assumed down.

Resp]	The default value is the exact code number (e.g., 407). Up to three response codes can be configured, where each code is separated by a comma. By default, no responses are defined (i.e., proxy assumed alive upon receipt of any response). Note: The 200 response cannot be used.

Applicable Products: All.

3.1.1.38 DNS Request Type per Proxy Set

This feature provides support for the configuration of a specific domain name system (DNS) request type per Proxy Set in order to resolve host names into IP addresses. Up until this release, the DNS request type could only be configured globally (i.e., for all Proxy Sets), using the Proxy DNS Query Type parameter.

To support this feature, the following parameter has been added to the Proxy Set table:

DNS Resolve Method [ProxySet_DNSResolveMethod]	Defines the DNS query record type for resolving the proxy server's host name to an IP address. ▪ [-1] = DNS resolving is done according to the settings of the global parameter, Proxy DNS Query Type. ▪ [0] A-Record = (Default) A-record DNS query. ▪ [1] SRV = If the Proxy address is configured with a domain name without a port (e.g., domain.com), an SRV query is done. The SRV query can return up to four Proxy host names and their weights. The device then performs DNS A-record queries for each Proxy host name (according to the received weights). Each host name can be resolved into up to 15 IP addresses. ▪ [2] NAPTR = NAPTR query is done. If successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is done according to the configured transport type. If the configured Proxy address contains a domain name with a port (e.g., domain.com:5080), the device performs a regular DNS A-record query. If the transport type is configured for the Proxy address, a NAPTR query is not performed. Note: The device supports up to 30 DNS resolved IP addresses. If the DNS resolution provides more than this number, the device uses only the first 30 received IP addresses and ignores the rest.

Applicable Products: All.

3.1.1.39 Increased Maximum Proxy Server Address Entries in Proxy Set Table

This feature provides support for an increase to 10 in the maximum number of proxy server address entries (IP addresses and/or FQDNs) that can be configured in the Proxy Set table. Up until this release, each Proxy Set could be configured with up to 5 entries only. (Note that the device supports up to 30 DNS-resolved IP addresses.)

Applicable Products: All.

3.1.1.40 Dual LDAP Servers and New LDAP Configuration Table

This feature provides support for using two Lightweight Directory Access Protocol (LDAP) compliant servers (e.g., Microsoft Active Directory). LDAP can be used for routing decisions based on retrieved LDAP queried information such as calling name and destination address. Up until this release, only one LDAP server was supported.

When two LDAP servers are implemented, the device runs an LDAP query to search distinguished name (DN) object records on both LDAP servers. The method of how the

device queries the DN object record between the two LDAP servers can be configured to one of the following:

- Parallel: The device queries the LDAP servers at the same time (simultaneously).
- Sequential: The device first queries one of the LDAP servers, and if the DN object is not found, it queries the second LDAP server.

The method for searching DN objects within each LDAP server can also be configured:

- Parallel: The query is done in all DN objects simultaneously. For example, a search for the DN object record "JohnD" is done simultaneously in the "Marketing", "Sales" and "Administration" DN objects.
- Sequential: The query is done in each DN object, one by one, until a result is returned. For example, a search for the DN object record "JohnD" is first run in DN object "Marketing" and if a result is not found, it searches in "Sales", and if not found, it then searches in "Administration", and so on.

The device can query up to three DN objects per LDAP server.

The LDAP servers and related parameters are now configured in the new LDAP Configuration table, described below. This table replaces the following LDAP parameters from previous releases (now obsolete): LDAPServerDomainName, LDAPServerPort, LDAPSearchDn, LDAPPassword, LDAPBindDn, LDAPInterfaceType, and LDAPServerMaxRespondTime.

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

LDAP Configuration Table [LdapConfiguration]	Defines the LDAP servers. To configure DNs per LDAP server, use the subset table, Ldap Servers Search Dns Table. [LdapConfiguration] FORMAT LdapConfiguration_Index = LdapConfiguration_LdapConfServerIp, LdapConfiguration_LdapConfServerPort, LdapConfiguration_LdapConfServerMaxRespondTime, LdapConfiguration_LdapConfServerDomainName, LdapConfiguration_LdapConfPassword, LdapConfiguration_LdapConfBindDn, LdapConfiguration_LdapConfInterfaceType, LdapConfiguration_Type, LdapConfiguration_MngmAuthAtt, LdapConfiguration_ConnectionStatus; [\LdapConfiguration] The read-only field, Connection Status, displays the connection status with the LDAP server.
Ldap Servers Search Dns Table [LdapServersSearchDNs]	This is a subset table of the LDAP Configuration Table. It defines the full path (i.e., distinguished name / DN) to the objects in the Active Directory where the query is done. Up to three DNs can be configured per LDAP server. An example of a base DN path is OU=NY,DC=OCSR2,DC=local. [LdapServersSearchDNs] FORMAT LdapServersSearchDNs_Index = LdapServersSearchDNs_Base_Path, LdapServersSearchDNs_LdapConfigurationIndex, LdapServersSearchDNs_SearchDnInternalIndex; [\LdapServersSearchDNs]
Web: LDAP Search Server Method CLI: ldap-search-server-method [LDAPSearchServerMethod]	Defines the method of how the device queries between the two LDAP severs. ▪ [0] Sequential = The query is done on the first LDAP server, and only if the DN object is not found, it searches on the second LDAP server. ▪ [1] Parallel = (Default) The query is done simultaneously on both LDAP servers.
[LdapSearchDnsInParallel]	Defines the method of how the device queries the DN within each LDAP server.

	▪ [0] Sequential (Default) = The query searches each DN object sequentially, one after the other, until a result is found. ▪ [1] Parallel = The query searches for a specific object record in multiple DN objects, simultaneously.

Applicable Products: All.

3.1.1.41 Customized Call Setup Rules for LDAP and Routing Logic

This feature provides support for configuring call setup rules, which are run upon the receipt of an incoming call (dialog) before the call is routed to its destination. These rules can be used for Lightweight Directory Access Protocol (LDAP) based routing as well as other advanced routing logic requirements including manipulation:

- LDAP query rules: LDAP is used by the device to query Microsoft's Active Directory (AD) server for specific user details such as the office extension number, mobile number, private number, OCS (Lync) address, and display name. Up until this release, the LDAP feature was relatively rigid, using the called (destination) number for AD lookup of user details and then routing the call using hard-coded routing rules. This new feature enhances the LDAP feature, providing full flexibility in AD lookup configuration to suite just about any customer deployment requirement:
  - Routing based on query results.
  - Queries based on any AD attribute.
  - Queries based on any attribute value (alphanumeric), including the use of the asterisk (*) wildcard as well as the source number, destination number, redirect number, and SIP message (SBC only). For example, the following queries the attribute "proxyAddresses" for the record whose value is "WOW:" followed by source number: "proxyAddresses=WOW:12345*"
  - Conditional LDAP queries, for example, where the query is based on two attributes (&(telephoneNumber=4064)(company=AudioCodes).
  - Employs conditions for checking the LDAP query results.
  - Manipulation of call parameters (such as source number, destination number, and redirect number) and the SIP message (SBC only), while using the LDAP query results.
  - Allows more than one LDAP query, if necessary.
- Manipulation (similar to the Message Manipulations table) of call parameters (such as source number, destination number, and redirect number) and SIP SBC messages.
- Conditions for routing, for example, if the source number equals a specific value, then use the call routing rule.

Call Setup rules are defined with a Set ID (similar to the Message Manipulations table), where multiple rules can be associated with the same Set ID. This allows the device to perform multiple Call Setup rules, if necessary, on the same call setup dialog. Set IDs are associated with routing rules in the routing tables. If an incoming call matches the input characteristics of a routing rule, the device first runs the associated call setup rules of the Set ID. The Set ID can result in any of the following:

- Rule's condition is met: The device performs the rule's action and then runs the next rules in the Set ID until the last rule or until a rule with an Exit Action Type. If the Exit rule is defined with a "True" Action Value, the device uses the current routing rule. If the Exit rule is defined with a "False" Action Value, the device uses the next routing rule and runs its associated Set ID.
- Rule's condition is not met: The device runs the next rule in the Set ID (regardless of whether an "Exit" Action Type is configured). When all the rules have been run and no condition has been met, the device uses the current routing rule to route the call (i.e., ends rules with Exit and True).

Note: If the source or destination numbers were manipulated, they revert to their original values when attempting the next routing rule.

Below are two examples of how this feature can be used:

- Routing according to source number existence in AD server for Tel-to-IP calls. In this example, the device queries the AD server for an attribute record "telephoneNumber" whose value equals the received source number (e.g., telephoneNumber=4064"). If it exists, the device sends the call to the Lync server; if the query fails, the device sends the call to the incumbent PBX.
  - Call Setup Rules table configuration:

Rules Set ID	Attributes to Query	Attributes to Get	Row Role	Condition	Action Subject	Action Type	Action Value
1	'telephoneNumber =' + param.call.src.user	telephoneNumber	Use Current Condition	ldap.found !exists	-	Exit	false

    - If the record is found (i.e., the condition is not met), Call Setup rule ends with a default exit result of true and uses the first routing rule (Lync).
    - If the record does not exist (i.e., the condition is met), the Call Setup rule exits with a false result and uses the second routing rule (PBX).
  - Routing table configuration includes two routing rules associated with the same Call Setup Rule Set ID:
    - Routing rule 1: Destination is set to IP Group 1 (Lync)
    - Routing rule 2: Destination is set to IP Group 2 (incumbent PBX)
- Calling Number Manipulation: In this example, the device queries the AD server for the attribute record "telephoneNumber" whose value is equal to the source number (e.g., "telephoneNumber =4064"). If found, it retrieves the number of the alternateNumber attribute and uses this number as the source number.
  - Call Setup Rules table configuration:

Rules Set ID	Attributes to Query	Attributes to Get	Row Role	Condition	Action Subject	Action Type	Action Value
1	'telephoneNumber =' + param.call.src.user	alternateNumber	Use Current Condition	ldap.attr. alternateNumber exists	param.call.src.user	Modify	ldap.attr. alternateNumber

  - Routing table includes a single rule that is associated with the Call Setup Rule Set ID.

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

Call Setup Rules Table [CallSetupRules]	Defines Call Setup rules and manipulation. [CallSetupRules] FORMAT CallSetupRules_Index = CallSetupRules_RulesSetID, CallSetupRules_AttributesToQuery, CallSetupRules_AttributesToGet, CallSetupRules_RowRole, CallSetupRules_Condition, CallSetupRules_ActionSubject, CallSetupRules_ActionType, CallSetupRules_ActionValue; [\CallSetupRules] ▪ Index = Unique index row of rule. Up to 40 rules can be defined. ▪ Rules Set ID = Defines the group of rules to which the rule belongs. Up to 10 Set IDs can be defined, where each Set ID can have up to 10 rules. ✓ Each rule can query the LDAP server and/or perform manipulations and/or run another rule set and/or exit with a true or false result. ✓ If Exit Action Type is not used and the rule set has reached its

	end, default return value of the rules set is true. ▪ Attributes To Query = Defines the query string (max. characters is 100) sent to the LDAP server. ✓ Combined strings and values can be done in a similar way to the Message Manipulations table (without regex), using the '+' operator. Single quotes (') can be used for specifying a constant string, e.g., '12345'. ✓ If conditional LDAP query is required, it is done in the MS LDAP language (similar to Lisp - '&' or '|' and then the phrases in parenthesis). Examples: 'telephoneNumber=EUM:' + param.call.redirect + '*' '&(telephoneNumber=' + param.call.src.user + ')(company=' + param.call.src.host + ')' '|(&(telephoneNumber=' + param.call.src.user + ')(attribute1=*))(mobile=' + param.call.dst.user + ')' ▪ Attributes To Get = Defines the attributes (max. characters is 100) of the found LDAP record that must be regarded. Up to five attributes can be defined, separated by a comma, e.g., msRTCSIP-PrivateLine,msRTCSIP-Line,mobile. The retrieved attributes' values are kept available for use in other rules until the next LDAP query or until the call is connected. Thus, re-queries of the same attributes are avoided. ▪ Row Role: Use Current Condition / Use Previous Condition. Similar to the Message Manipulations table. It is used for performing more than one action when a specific condition occurs. ▪ Condition: Similar to the Message Manipulations table (max. characters is 200). Regular Expression can also be used (regex command). Examples: ✓ ldap.attr.attribute1 exists ✓ param.call.dst.user == ldap.attr.msRTCSIP-PrivateLine ✓ ldap.found !exists (record was not found) ✓ ldap.err exists (if LDAP error) ▪ Action Subject: Similar to the Message Manipulations table (max. characters is 100). Examples: ✓ param.call.dst.user (called number) ✓ param.call.src.user (calling number) ✓ param.call.src.name (calling name) ✓ param.call.redirect (redirect number) ✓ param.call.src.host (source host) ✓ param.call.dst.host (destination host) ▪ Action Type: Add / Remove / Modify / Add Prefix / Add Suffix / Remove Suffix / Remove Prefix / Exit / Run Rules Set. ✓ Exit: stops the rule set and returns a result (true or false). ✓ Run Rules Set: performs another rule set. ▪ Action Value = (max. characters is 300) Examples: ✓ '+9723976'+ldap.attr.alternateNumber ✓ '9764000' ✓ ldap.attr.displayName ✓ true ✓ false
Routing tables	New column added to associate routing rule with Call Setup Rule Set: CallSetupRulesSetID.

Note: For backward compatibility, the LDAP configuration method from the previous release is still supported in this release.

Applicable Products: All.

3.1.1.42 Release-Cause Reasons for Alternative Routing Tables Enhancements

This feature provides an enhancement to the tables used for configuring call release reasons for alternative routing. This enhancement facilitates configuration and improves user experience:

- Up until this release, the Tel-to-IP and IP-to-Tel release-cause reasons for alternative routing were configured in the same table (Reasons for Alternative Routing table). In this release, they appear in separate tables and on separate pages:
  - Reasons for Tel-to-IP Alternative Routing table (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **Alternative Reasons** > **Reasons for Tel-to-IP**).
  - Reasons for IP-to-Tel Alternative Routing table (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **Alternative Reasons** > **Reasons for IP-to-Tel**).
- The SBC Alternative Routing Reasons table has been re-designed to allow the user to add table rows, where each row represents a release-cause reason for alternative routing.
- For IP release-cause reasons, the wildcards 4xx, 5xx, and 6xx have been added as possible options.
- The number of table entries that can be configured has been increased from 5 to 10.
- Up until this release, the configured alternative release-cause reasons were displayed in the Web GUI and CLI as number codes only (e.g., "486"). In this release, descriptions are now displayed alongside these number codes (e.g., "486 Busy").

Applicable Products: All.

3.1.1.43 Resolving NAT Traversal by Sending SIP Messages to Source IP

This feature provides support for configuring the device to always send SIP requests and responses, within a SIP dialog, to the source IP address of the previously received SIP message. This feature is especially useful in scenarios where the SIP endpoint is located behind a NAT firewall (and the device is unable to identify this using its regular NAT mechanism).

By default (and according to the SIP standard), the device sends SIP requests using the address in the Contact header and SIP responses using the address in the Via header of the previously received message.

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

Web: Always Use Source Address CLI: always-use-source-addr [IPGroup_AlwaysUseSourceAddr]	Enables the device to always send SIP requests and responses to the source IP address received in the previous SIP message. ▪ [0] No (default). ▪ [1] Yes = Sends SIP requests and responses, within a dialog, to the source IP address received in the previous SIP message.

Applicable Products: All.

3.1.1.44 SIP Response upon INVITE from Endpoints behind NAT

This feature provides support for disabling the device's Automatic NAT Detection feature. Up until this release, the device by default handled NAT issues by comparing the incoming packet's source IP address with the SIP Contact header's IP address. If the Contact header had a local IP address and the source IP address a public one, the device considered the endpoint as located behind NAT and thus, sent the SIP message using the public IP address. If both had local addresses, the device used the IP address in the Contact header.

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

SIP NAT Detection CLI: sip-nat-detect [SIPNatDetection]	Enables the device to detect whether the incoming INVITE message is sent from an endpoint located behind a NAT. ▪ [0] Disable = Incoming SIP message is processed as

	received from an endpoint that is not located behind NAT and the response to the INVITE is sent to the IP address in the SIP Contact header. ▪ [1] Enable (default) = Incoming SIP message is processed as received from an endpoint that is located behind NAT and the response to the INVITE is sent to the packet's source IP address.

Applicable Products: All.

3.1.1.45 Stop Keep-Alive with Proxy if all Trunks of Trunk Group #1 are Down

This feature provides support for configuring the device to not send keep-alive messages to the associated proxy server when all trunks in Trunk Group ID 1 are down. Together with this behavior, the device can also be configured to not respond to SIP OPTIONS messages received form the proxy in such a scenario.

This feature may be useful, for example, in deployments where the proxy server (e.g., IP PBX) determines connectivity status with the device by its receipt of keep-alive messages (e.g., SIP OPTIONS) from the device. If the proxy stops receiving keep-alive messages, it would consider all the trunks as down and consequently, re-route calls to an alternative gateway. To support this feature, options [2] and [3] have been added to the following existing parameter:

CLI: trunk-status-reporting [TrunkStatusReportingMode]	Enables the device to not respond to received SIP OPTIONS messages from, and/or send keep-alive messages to, a proxy server associated with Trunk Group ID 1 if all its member trunks are down. ▪ [0] = Disable (default) ▪ [1] = The device does not respond to SIP OPTIONS received from the proxy associated with Trunk Group 1. ▪ [2] = The device does not send keep-alive messages to the proxy associated with Trunk Group 1. ▪ [3] = Both options [1] and [2]. Notes: ▪ When this parameter is set to not respond to SIP OPTIONS received from the proxy, it is applicable only if the OPTIONS message does not include a user part in the Request-URI. ▪ The proxy server is determined by the Proxy Set that is associated with the Serving IP Group defined for the Trunk Group in the Trunk Group Settings table.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.46 SBC Pre-Classification SIP Message Manipulation

This feature provides support for performing message manipulation on new incoming SIP initiating-dialog request messages (not in-dialog) prior to the Classification process. This is achieved by assigning a Message Manipulation Set ID, configured in the existing Message Manipulations table, to the appropriate SIP Interface on which the message will be received. This feature may be useful, for example, to apply message manipulation to calls that otherwise would be rejected by the device for whatever reason.

Notes:

- The Message Manipulation Set assigned to a SIP Interface that is associated with an outbound leg, is ignored. Only the Message Manipulation Set assigned to the IP Group is applied to the outgoing call.
- If both the SIP Interface and IP Group associated with the incoming call are assigned a Message Manipulation Set, the one assigned to the SIP Interface is performed first.

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

Web: Pre Classification ManSet CLI: configure voip/voip-network sip-interface/preclassification-manset [SIPInterface_PreClassificationManipulationSet]	Assigns a Message Manipulation Set ID to the SIP Interface. By default, no Message Manipulation Set ID is defined. Note: This parameter is applicable only to SBC calls.

Applicable Products: All.

3.1.1.47 SBC Dial Plan Prefix Tags for Increasing Routing Rule Capacity

This feature provides support for using special, user-defined number prefix tags (character strings) in the Dial Plan file for IP-to-IP routing rules. This character tag can be used to represent the source or destination prefix number in the IP-to-IP Routing table, as matching input characteristics. When the device locates a matching rule, it removes the tag and then routes the call to the actual destination.

This feature is extremely useful for scenarios in which a significant number of routing rules are required. In such cases, the IP-to-IP Routing table may not be large enough to accommodate all the required rules. For example, this feature is useful in deployments that need to handle hundreds of call routing scenarios such as for a large geographical area (a state in the US). Such an area could consist of hundreds of local area codes as well as codes for international calls. The local calls and international calls would need to be routed to different SIP trunks. Thus, instead of configuring many routing rules for each call destination type, you can simply configure two routing rules, one with a unique prefix tag representing the different local area codes and the other with a tag representing international calls.

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

- Dial Plan file defined with prefix number tags:

  ```
  <prefix number>,0,<prefix tag>
  ```

  where:

  - *prefix number* is the number prefix (ranges can be defined in brackets)
  - *prefix tag* is the user-defined prefix tag (text) representing the prefix number

  For example, the Dial Plan 1 below defines the prefix tags "LOCL" and "INTL" for the listed prefix numbers:

  ```
  [ PLAN1 ]
  11,0,INTL
  42520[3-5],0,LOCL
  425207,0,LOCL
  425207,0,LOCL
  253,0,LOCL
  …
  ```

- The IP-to-IP Inbound Manipulation table supports the keyword string, *$DialPlan<x>*, where *x* is the Dial Plan index (0 to 7). This string is used in the 'Prefix to Add' (or 'Suffix to Add') fields to indicate the Dial Plan index from where the prefix tag must be taken. For example, if the number 4252000555 is received, it is manipulated to LOCL4252000555. The manipulation rule can be associated with, for example, a specific IP Group.
- The IP-to-IP Routing table supports the use of the user-defined prefix tag in the 'Source / Destination Username Prefix' fields (for example, LOCL).
- The IP-to-IP Outbound Manipulation table is used to remove the tag before sending the call to its destination.

Applicable Products: All.

3.1.1.48 Enhanced Alternative Routing to PSTN upon Failed SBC Calls

This feature provides support to facilitate configuration for routing a call to the PSTN as an alternative route upon a failed IP destination (e.g., receipt of SIP 4xx response). The device automatically, and without any special configuration, re-routes the SBC call to its' Gateway interface. It does the routing logic by appending a user-defined prefix destination URI user part (by default, "acgateway-", for example, acgateway-200) to identify call redirection from the SBC to Gateway interface. The device removes this prefix before sending it to the Gateway interface.

To support this feature, the alternative routing rule in the IP-to-IP Routing table is configured with the 'Destination Type' parameter set to the new optional value, Gateway (see new feature in Section 3.1.1.49). In addition, to specify the destination Trunk Group, an IP-to-Tel routing rule must be configured in the Inbound IP Routing table, using the destination number prefix (e.g., 200) as the matching rule characteristics.

Up until this release, it was necessary to configure an IP Group and SIP interface for the Gateway interface.

To change the default prefix destination URI user part, the following new parameter has been added:

Gateway Direct Route Prefix CLI: gw-direct-route-prefix [GWDirectRoutePrefix]	Defines the prefix destination URI user part that is appended to the original user part for alternative IP-to-IP call routing from SBC to Gateway interfaces. The valid value is a string of up to 16 characters. The default is 'acgateway-". For example, "acgateway-200".

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.49 Hybrid SBC SIP Interface for SBC and Gateway Call Routing

This feature provides support for routing gateway calls directly from the SBC SIP Interface (in addition to SBC calls). In other words, IP calls received on the SBC SIP Interface can be routed using the Gateway (IP-to-Tel) routing rules, directly to the PSTN, and PSTN calls received on this interface can be routed directly to the IP.

Up until this release, routing of gateway calls involved a two-stage process, where the call was first routed from the SBC SIP Interface to a Gateway SIP Interface, and then from this interface to the PSTN. This process utilized two call session resources.

This feature now eliminates the need to configure a dedicated Gateway SIP Interface and also offers efficient session resource utilization.

To support this feature, an additional optional value has been added to the 'Destination Type' parameter in the IP-to-IP Routing table:

Destination Type [IP2IPRouting_DestType]	▪ [8] Gateway

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.50 Call Forking using SBC IP-to-IP Routing Rules

This feature provides support for configuring call-forking routing rules for sending an incoming IP call to multiple destinations. These rules are configured in the IP-to-IP Routing table. The incoming call can be routed to multiple destinations of any type such as an IP Group or IP address. The device forks the call by sending simultaneous INVITE messages to all the specified destinations. It handles the multiple SIP dialogs until one of the calls is answered, at which stage it terminates the other SIP dialogs.

This feature is configured by creating a forking group in the IP-to-IP Routing table. A forking group consists of a main routing rule ('Alternative Route Options' set to Route Row) whose 'Group Policy' is set to Forking, and one or more associated routing rules ('Alternative Route Options' set to Group Member Ignore Inputs or Group Member Consider Inputs).

These group members must be configured in contiguous table rows to the main routing rule. If an incoming call matches the input characteristics of the main routing rule, the device routes the call to its destination and all those of the group members.

An alternative routing rule can also be configured for the forking group. The alternative route is used if the call fails for the forking group (i.e., main route and all its group members fail). The alternative routing rule must be configured in the table row immediately below the last group member of the forking group, and its 'Group Policy' must be set to Forking. The alternative route can also be configured with its group members. These group members must be configured in the rows immediately below the alternative routing rule. If the device uses the alternative route, the call is also sent to its group members.

The Least Cost Routing (LCR) feature can also be employed with call forking. For LCR, The device calculates a maximum call cost for each forking group and routes the call to the forking group with the lowest cost. The prerequisite for this functionality is that the incoming call must successfully match the input characteristics of the main routing rule. Thus, even if the call can successfully be routed to the main routing rule, a different routing rule can be chosen (even an alternative route, if configured) based on LCR. If routing to one forking group fails, the device attempts to route the call to the forking group with the next lowest cost (main or alternative route), and so on.

To support this feature, the following new parameter and options have been added to the IP-to-IP Routing table.

Group Policy CLI: group-policy [IP2IPRouting_GroupPolicy]	Defines whether the routing rule includes call forking. ▪ [0] None (default) = Call uses only this route (even if forking group members are configured in the rows below it). ▪ [1] Forking = Call uses this route and the routes of group members, if configured (in the rows below it).
Alternative Route Options [IP2IPRouting_AltRouteOptions]	Additional optional values for associating routing rules as forking members (group members) of the main forking rule. ▪ [3] Group Member Ignore Inputs = This routing rule is a member of the "forking" routing rule. The incoming call is also forked to the destination of this routing rule. The matching input characteristics of the routing rule are ignored. ▪ [4] Group Member Consider Inputs = This routing rule is a member of the "forking" routing rule. The incoming call is also forked to the destination of this routing rule only if the incoming call matches this rule's input characteristics. Note: The group members must be configured in a table row that is immediately below the main forking routing rule, or below an alternative routing rule for the main rule, if configured.

Note: Call forking is not applicable to LDAP IP-to-IP routing rules.

Applicable Products: All.

3.1.1.51 Same Call-ID for SBC End-to-End Calls

This feature provides support for enabling the device to use the same call identification value as received in the incoming message (e.g., INVITE) for the outgoing message (e.g., INVITE). The call identification value is contained in the SIP Call-ID header. When this feature is disabled, the device creates a new Call-ID header value for the outgoing message (as done in previous releases).

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

CLI: sbc-keep-call-id [SBCKeepOriginalCallId]	Enables the device to use the same call identification received in incoming messages for the outgoing messages. The call identification value is contained in the SIP Call-ID header. ▪ [0] = (Default) Disable - outgoing messages are sent with a different Call-ID value. ▪ [1] = Enable Note: When the device sends an INVITE as a result of a REFER/3xx termination, it always creates a new Call-ID value

	and ignores this parameter's settings.

Applicable Products: All.

3.1.1.52 SBC Routing to Port Specified in Request-URI

This feature provides support for enabling the device to use the port indicated in the Request-URI of the incoming message as the destination port when routing to an IP Group that uses a Proxy Set to define its address. By default (and in previous releases), the <device> uses the port configured for the Proxy Set associated with the IP Group. The IP address configured for the Proxy Set is still used as the destination.

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

Route Using Request URI Port use-requri-port [IPGroup_SBCRouteUsingRequestURIPort]	Enables the <device> to use the port indicated in the Request-URI of the incoming message as the destination port when routing the message to the IP Group. The <device> uses the IP address configured for the Proxy Set that is associated with the IP Group. The parameter thus allows the <device> to route calls to the same server (IP Group), but different port. ▪ [0] Disable = (Default) The port configured for the associated Proxy Set is used as the destination port. ▪ [1] Enable = The port indicated in the Request-URI of the incoming message is used as the destination port.

Applicable Products: All.

3.1.1.53 Gateway Dial Plan File Source Prefix Tags for Increasing Routing Rule Capacity

This feature provides support for Dial Plan prefix tags to denote the source number in IP-to-Tel call routing (PRI and BRI). Up until this release, the device supported prefix tags only for the destination number.

The prefix tags are user-defined character strings defined in the Dial Plan file per prefix number (source or destination). This tag can then be used to represent the source or destination prefix number (instead of the original prefix) in the Inbound IP Routing table, as the matching input characteristics. When the device locates a matching rule, it removes the tag by number manipulation, and then routes the call to its destination. The source prefix tag is removed using a manipulation rule defined in the Source Phone Number Manipulation Table for IP-to-Tel Calls Manipulation table; the destination prefix tag is removed using a manipulation rule defined in the Destination Phone Number Manipulation Table for IP-to-Tel Calls Manipulation table.

The prefix tags in the Dial Plan file are defined using the following syntax:

```
<calling prefix number>,0,<calling prefix tag>
```

For example:

```
[ PLAN1 ]
42520[3-5],0,PBX-1
425207,0,PBX-1
42529,0,PBX-1
```

This feature resolves the limitation of entries in the Inbound IP Routing Table for deployments requiring many routing rules. Instead of configuring many routing rules to represent the many possible routing scenarios, a single routing rule can be configured, with a source and/or destination prefix tag to represent a group of call scenarios whose destination is the same (e.g., a specific PBX).

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

Web: IP to Tel Tagging Source Dial Plan Index	Determines the Dial Plan index in the Dial Plan file used for source prefix tags in incoming IP-to-Tel calls. The tag is added

CLI: ip-to-tel-tagging-src [IP2TelTaggingSourceDialPlanIndex]	as a prefix to the calling party number, and the Inbound IP Routing table uses this tag instead of the original prefix. Manipulation is done in the Manipulation table to remove the tag before sending the call to the destination. The valid values are 0 to 7, where 0 denotes PLAN1, 1 denotes PLAN2, and so on. The default is -1 (i.e., no dial plan file used). The prefix tag can be up to nine (text) characters. Note: Configure these routing rules so that routing is done before manipulation.

Note: Source and destination prefix tags can be used together - in the same routing rule or different routing rules.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.54 Gateway Call Redirection for SIP 3xx Responses with Multiple Contacts

This feature provides support for configuring how the device handles received SIP 3xx responses that contain multiple alternative contacts. The 3xx response indicates that the original destination is not available (e.g., 301 Moved Permanently – user cannot be found) and that the call can be redirected to alternative destinations specified in the SIP Contact headers.

This feature allows the device to handle 3xx responses as follows:

- Upon receipt of a 3xx response, the device tries each contact sequentially, listed in the Contact headers, until a successful destination is found. However, if a contact responds with a SIP 486 or 600, the device does not try to redirect the call to the next contact, and drops the call.
- Upon receipt of a 3xx response, the device tries each contact sequentially, listed in the Contact headers. However, if a SIP 6xx Global Failure response is received during this process (e.g., 600 Busy Everywhere) the device does not try to redirect the call to the next contact, and drops the call.
- Upon receipt of a 3xx response, the device redirects the call to the first contact listed in the Contact header. If the contact responds with a SIP response that is defined in the Reasons for Tel-to-IP Alternative Routing table, the device tries to redirect the call to the next contact, and so on. If a contact responds with a response that is not configured in the table, the device does not try to redirect the call to the next contact, and drops the call.

Note: If a 401 or 407 response is received from a contact, the device does not try to redirect the call to the next contact, regardless of the settings of this parameter. Instead, the device continues with the regular authentication process, as indicated by these response types.

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

Web: 3xx Use Alt Route Reasons CLI: 3xx-use-alt-route [UseAltRouteReasonsFor3xx]	Determines the handling of received SIP 3xx responses regarding call redirection to listed contacts in the Contact header. ▪ [0] No = (Default) Upon receipt of a 3xx response, the device tries each contact, one by one, listed in the Contact headers, until a successful destination is found. However, if a contact responds with a 486 or 600, the device does not try to redirect the call to next contact, and drops the call. ▪ [1] No if 6xx = Upon receipt of a 3xx response, the device tries each contact, one by one, listed in the Contact headers. However, if a 6xx Global Failure response is received during this process (e.g., 600 Busy Everywhere) the device does not try to redirect the call to the next contact, and drops the call. ▪ [2] Yes = Upon receipt of a 3xx response, the device redirects the call to the first contact listed in the Contact

	header. If the contact responds with a SIP response that is defined in the Reasons for Tel-to-IP Alternative Routing table, the device tries to redirect the call to the next contact, and so on. If a contact responds with a response that is not configured in the table, the device does not try to redirect the call to the next contact, and drops the call.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.55 Delay Outgoing INVITE Messages for Tel-to-IP Call Forking

This feature provides support for delaying the sending of INVITE messages in Tel-to-IP call forking. The delay does not apply to the first routing member of the forking group, where the INVITE is sent immediately (as in normal operation). The delay applies only to the other routing members of the forking group, where once a user-defined timeout expires, INVITEs are sent simultaneously to all these other members.

If the device receives a SIP 4xx or 5xx in response to the first INVITE, the device immediately sends INVITEs to all the other forking group members. This occurs even if the timeout has not yet expired.

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

CLI: forking-delay-time-invite [ForkingDelayTimeForInvite]	Defines the interval (in seconds) to wait before sending INVITE messages to the other members of the forking group. The INVITE is immediately sent to the first member. The valid value range is 0 to 40. The default is 0 (i.e., send immediately).

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.56 Alternative Routing upon ISDN Disconnect

This feature provides support configuring the device's call disconnection behavior when an IP-to-Tel call cannot be established (e.g., busy on Tel side). This feature determines when the device sends the call to an alternative route in such a scenario.

By default, if an ISDN Q.931 Disconnect message with a Progress Indicator (PI) IE is received from the Tel side, the device does not disconnect the call immediately. Instead, it waits for any subsequent media from the Tel (e.g., "this number is currently busy") and forwards it to the IP side (SIP 183 for early media). Only when the Q.931 Release message is received does the device disconnect the call (sends SIP BYE message to the IP side). If an alternative route has been configured, the device sends the IP call to the alternative route.

Alternatively, upon receipt of a Disconnect message, the device can be configured to immediately send the IP call to an alternative route, if exists. If no alternative route has been configured and the Disconnect message is received with PI, the device forwards the subsequent early media to the IP side. The device disconnects the IP call only upon receipt of the subsequent Release message.

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

[DisconnectCallwithPIifAlt]	Enables the device to wait for subsequent media from Tel side upon receipt of a Disconnect message. ▪ [0] (Default) = Upon receipt of Disconnect, the device forwards early media to the IP side if Disconnect includes PI, and disconnects the call when a Release is received. Only after the call is disconnected does the device send the call to an alternative route, if exists. ▪ [1] = Upon receipt of Disconnect, the device immediately sends call to alternative route, if exists.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.57 CRP Routing for SIP Proxy to PSTN

This feature provides support for enabling the routing of calls from the SIP Proxy to the PSTN. This applies to calls for which the device is unable to locate matching users in its Users Registration database. Thus, this allows, for example, emergency calls (911) or any other PSTN calls received from the SIP Proxy to be routed to the PSTN. This routing feature is applicable when the CRP is in Normal or Auto-Answer Registrations mode.

When enabled, the device adds another routing rule (Index 7) to the IP-to-IP Routing table, for routing calls from IP Group 2 (i.e., SIP Proxy) to IP Group 3 (Gateway).

Notes:

- This routing feature does not serve as an alternative route. In other words, if the device locates a matching user but the user is busy, it does not re-route the call to the PSTN using this routing feature.
- Enabling this feature may expose the device to security threats, by allowing calls from the WAN to be routed to the PSTN Gateway. Thus, this feature should be used only if necessary and appropriate security measures should be taken by the customer's network administrator.

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

CLI: crp-gw-fallback [CRPGatewayFallback]	Enables fallback routing from the proxy server to the Gateway (PSTN). ▪ [0] = Disable (default) ▪ [1] = Enable

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 4000.

3.1.1.58 SIP-based Media Recording

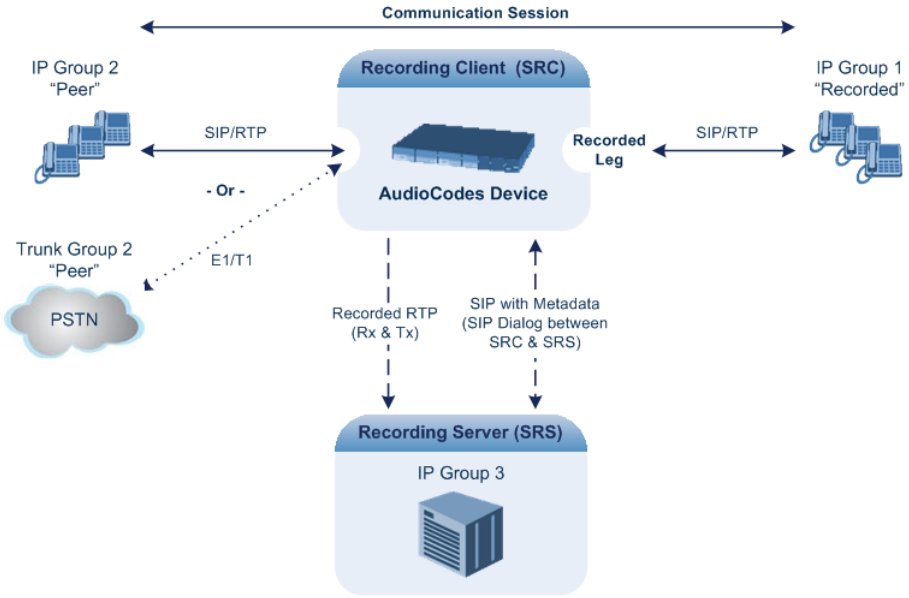
This feature provides support for SIP-based media recording of call sessions. This feature is applicable to all the device's main applications (SBC, and Gateway/IP-to-IP applications).

Note: Recording of Gateway calls is applicable only to Mediant 3000. For all other products that support SIP-based media recording, this feature is applicable only to SBC calls (even though some of them may support Gateway call functionality).

This feature is in accordance with the Session Recording Protocol (siprec), which describes architectures for deploying session recording solutions and specifies requirements for extensions to SIP that will manage delivery of RTP media to a recording device. The siprec protocol is based on RFC 6341 (Use Cases and Requirements for SIP-Based Media Recording), Session Recording Protocol (draft-ietf-siprec-protocol-02), and Architecture (draft-ietf-siprec-architecture-03).

Session recording is a critical requirement in many business communications environments such as call centers and financial trading floors. In some of these environments, all calls must be recorded for regulatory and compliance reasons. In others, calls may be recorded for quality control or business analytics. Recording is typically performed by sending a copy of the session media to the recording devices.

The siprec protocol support by the AudioCodes device is referred to as SIP-based Media Recording. The siprec protocol specifies the use of SIP, SDP, and RTP to establish a Recording Session (RS) from the Session Recording Client (SRC), which is on the path of the Communication Session (CS), to a Session Recording Server (SRS) at the recording device. AudioCodes device functions as the SRC, sending recording sessions to a third-party SRS, as shown in the figure below.



The device can record calls between two IP Groups, or between an IP Group and a Trunk Group (for Gateway calls). The type of calls to record can be specified by source and/or destination prefix number or SIP Request-URI, as well as by call initiator. The side ("leg") on which the recording is done must be specified. This recording leg must be one that is interfacing with one of the IP Groups. Specifying the leg is important as it determines the various call media attributes of the recorded RTP (or SRTP) such as coder type.

The device initiates a recording session by sending an INVITE message to the SRS when the recorded call is connected. The SIP From header contains the identity of the SRC and the To header contains the identity of the SRS.

The SDP in the INVITE contains:

- Two 'm=' lines that represent the two RTP/SRTP streams (Rx and Tx).
- Two 'a=label:' lines that identify the streams.
- XML body (also referred to as *metadata*) that provides information on the participants of the call session:
  - <group id>: Logging Session ID (displayed as [SID:nnnnn] in Syslog), converted from decimal to hex. This number remains the same even if the call is forwarded or transferred. This is important for recorded calls.
  - <session id>: Originally recorded Call-ID, converted from decimal to hex.
  - <group-ref>: same as <group id>.
  - <participant id>: SIP From / To user.
  - <nameID aor>: From/To user@host.
  - <send> and <recv>: ID's for the RTP streams in hex - bits 0-31 are the same as group, bits 32-47 are the RTP port.
  - <stream id>: Same as <send> for each participant.
  - <label>: 1 and 2 (same as in the SDP's 'a=label:' line).

The SRS can respond with 'a=recvonly' for immediate recording or 'a=inactive' if recording is not yet needed, and send re-INVITE at any later time with the desired RTP/SRTP mode change. If a re-INVITE is received in the original call (e.g. when a call is on hold), the device sends another re-INVITE with two 'm=' lines (but without metadata) to the SRS with the updated RTP/SRTP data.

Below is an example of an INVITE sent by the device to an SRS:

```
INVITE sip:VSRP@1.9.64.253 SIP/2.0
Via: SIP/2.0/UDP 192.168.241.44:5060;branch=z9hG4bKac505782914
Max-Forwards: 10
```

```
From: <sip:192.168.241.44>;tag=1c505764207
To: <sip:VSRP@1.9.64.253>
Call-ID: 50576309724120101115 7@192.168.241.44
CSeq: 1 INVITE
Contact: <sip:192.168.241.44:5060>;src
Supported: replaces,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Require: siprec
User-Agent: TrunkPack 8410/v.6.70A.014
Content-Type: multipart/mixed;boundary=boundary_ac1fffff85b
Content-Length: 1832

--boundary_ac1fffff85b
Content-Type: application/sdp
v=0
o=AudiocodesGW 921244928 921244893 IN IP4 10.33.8.70
s=SBC-Call
c=IN IP4 10.33.8.70
t=0 0
m=audio 6020 RTP/AVP 8 96
c=IN IP4 10.33.8.70
a=ptime:20
a=sendonly
a=label:1
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
m=audio 6030 RTP/AVP 8 96
c=IN IP4 10.33.8.70
a=ptime:20
a=sendonly
a=label:2
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15

--boundary_ac1fffff85b
Content-Type: application/rs-metadata
Content-Disposition: recording-session

<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns='urn:ietf:params:xml:ns:recording'>
  <datamode>complete</datamode>
  <group id="00000000-0000-0000-0000-00003a36c4e3">
    <associate-time>2010-01-24T01:11:57Z</associate-time>
  </group>
  <session id="0000-0000-0000-0000-00000000d0d71a52">
    <group-ref>00000000-0000-0000-0000-00003a36c4e3</group-ref>
    <start-time>2010-01-24T01:11:57Z</start-time>
     <ac:AvayaUCID
xmlns="urn:ietf:params:xml:ns:Avaya">FA080030C4E34B5B9E59</ac:AvayaUCID>
  </session>
  <participant id="1056" session="0000-0000-0000-0000-00000000d0d71a52">
    <nameID aor="1056@192.168.241.20"></nameID>
    <associate-time>2010-01-24T01:11:57Z</associate-time>
    <send>00000000-0000-0000-0000-1CF23A36C4E3</send>
    <recv>00000000-0000-0000-0000-BF583A36C4E3</recv>
  </participant>
     <participant id="182052092" session="0000-0000-0000-0000-00000000d0d71a52">
    <nameID aor="182052092@voicelab.local"></nameID>
    <associate-time>2010-01-24T01:11:57Z</associate-time>
    <recv>00000000-0000-0000-0000-1CF23A36C4E3</recv>
```

```
    <send>00000000-0000-0000-0000-BF583A36C4E3</send>
  </participant>
  <stream id="00000000-0000-0000-0000-1CF23A36C4E3" session="0000-0000-0000-0000-
00000000d0d71a52">
    <label>1</label>
  </stream>
  <stream id="00000000-0000-0000-0000-BF583A36C4E3" session="0000-0000-0000-0000-
00000000d0d71a52">
    <label>2</label>
  </stream>
</recording>
--boundary_ac1fffff85b—
```

If the recorded leg uses SRTP, the device can also send the media streams to the SRS as SRTP.

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

Web: SIP Recording Application CLI: enable-sip-rec [EnableSIPRec]	Enables the SIP-based Media Recording feature: ▪ [0] Disable (default) ▪ [1] Enable Note: For this parameter to take effect, a device reset is required.
Web: Recording Server (SRS) Destination Username CLI: siprec-server-dest-username [SIPRecServerDestUsername]	Defines the SIP user part for the recording server. This user part is added in the SIP To header of the INVITE message that the device sends to the recording server. The valid value is a string of up to 50 characters. By default, no user part is defined.
Web: SIP Recording Routing table CLI: sip-rec-routing [SIPRecRouting]	Defines the calls to record. [SIPRecRouting] FORMAT SIPRecRouting_Index = SIPRecRouting_RecordedIPGroupID, SIPRecRouting_RecordedSourcePrefix, SIPRecRouting_RecordedDestinationPrefix, SIPRecRouting_PeerIPGroupID, SIPRecRouting_PeerTrunkGroupID, SIPRecRouting_Caller, SIPRecRouting_SRSIPGroupID; [\SIPRecRouting]; ▪ Recorded IP Group ID = Defines the IP Group participating in the call and the recording is done on the leg interfacing with this IP Group. ▪ Recorded Source Prefix = Defines calls to record based on source number / URI. ▪ Recorded Destination Prefix = Defines calls to record based on destination number / URI. ▪ Peer IP Group ID = Defines the peer IP Group that is participating in the call. ▪ Peer Trunk Group ID = Defines the peer Trunk Group that is participating in the call (applicable only to Gateway calls). ▪ Caller = Defines which calls to record according to which party is the caller: ✓ [0] Both (default) = Caller can be peer or recorded side ✓ [1] Recorded Party (in Gateway, IP-to-Tel call) ✓ [2] Peer Party (in Gateway, Tel-to-IP call) ▪ Recording Server (SRS) IP Group ID = Defines the IP Group of the recording server (SRS). Note: The SIP Interface used for communicating with the SRS is according to the SRD associated with the SRS IP Group in the IP Group table. If two SIP Interfaces are associated with the SRD - one for "SBC" and one for "GW &IP2IP" – the device uses the SIP Interface set for SBC. If no SBC SIP interface type is

	defined, the device uses the “GW & IP2IP” interface.

Notes:

- The SIP-based Media Recording feature is enabled by the Feature Key, "SIP-REC" that needs to be included in the Software License Key installed on the device. This Feature Key also specifies the maximum number of supported SIP recording sessions. To order this Feature Key, contact your AudioCodes sales representative.
- For maximum concurrent call recording sessions, contact your AudioCodes sales representative.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 3000; Mediant Non-Hybrid SBC.

3.1.1.59 SIP-based Media Recording of SRTP Sessions

This feature provides an enhancement to the SIP-based media recording feature (SIPRec), discussed in Section 3.1.1.58. The device can now record SRTP calls and send it to the Session Recording Server (SRS) in SRTP. This applies to both Gateway and SBC calls and involves scenarios where SRTP is used in the IP leg for Gateway calls, or in one of the IP legs for SBC calls.

For an SBC RTP-SRTP session, the recorded IP Group in the SIP Recording Routing table must be the RTP leg if recording is required to be RTP, or the SRTP leg if recording is required to be SRTP.

This feature also allows the SBC device to be located between an SRS and a Session Recording Client (SRC) and act as an RTP-SRTP translator. In such a setup, the device receives SIP recording sessions (as a server) from the SRC and translates SRTP media to RTP, or vice versa, and then forwards the recording to the SRS in the translated media format.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 3000; Mediant Non-Hybrid SBC.

3.1.1.60 SIP-based Media Recording for Interoperating with Genesys

This feature provides support for interworking the device's new SIP-based media recording feature with Genesys equipment. If the device receives a SIP message with Genesys proprietary SIP header, *X-Genesys-CallUUID* (which is used to identify the session), it adds the header's information to an AudioCodes proprietary tag in the XML metadata of the SIP INVITE sent to the recording server, as shown below:

```
<ac:GenesysUUID
xmlns="urn:ietf:params:xml:ns:Genesys">4BOKLLA3VH66JF112M1CC9VHKS1
4F0KP</ac:GenesysUUID>
```

Genesys sends the *X-Genesys-CallUUID* header in the first SIP message, typically in the INVITE and the first 18x response.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 3000; Mediant Non-Hybrid SBC.

3.1.1.61 SIP-based Media Recording for Interoperating with Avaya UCID

This feature provides support for interworking the device's new SIP-based media recording feature with Avaya equipment. The Universal Call Identifier (UCID) is an Avaya-proprietary call identifier that is used to help correlate call records between different systems and identifies sessions. Avaya generates this in outgoing calls. If the device receives a SIP INVITE from Avaya, it adds the UCID value received in the User-to-User SIP header, to an AudioCodes proprietary tag in the XML metadata of the SIP INVITE that is sent to the recording server.

For example, if the received SIP header is:

```
User-to-User: 00FA080019001038F725B3;encoding=hex
```

the device includes the following in the XML metadata:

```
xml metadata:
<ac:AvayaUCID xmlns="urn:ietf:params:xml:ns:Avaya">
FA080019001038F725B3</ac:AvayaUCID>
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 3000; Mediant Non-Hybrid SBC.

3.1.1.62 SBC Play of Tones from PRT File and DSP Resources

This feature provides enhanced support regarding DSP utilization and play of tones from a Prerecorded Tone (PRT) file that is installed on the device. This applies to SBC calls and involves the currently supported tones, ringback and hold.

- Mediant 1000B: Up until this release, the device required DSPs for playing tones from a PRT file or for generating them locally; now, PRT functionality no longer requires DSPs (tone generation does require DSPs).
- Mediant 3000: No change - PRT file and local tone generation are supported and DSPs are required for both.
- Mediant 5xx, Mediant 8xx, Mediant 2600, Mediant 4000: Up until this release, the device required DSPs for generating local tones and PRT functionality was not supported. Now, PRT is supported and does not require DSPs (DSPs are still required for local tone generation). If DSPs are being used for a call (for whatever reason), only local tone generation is supported.
- Mediant 9000, Mediant SW: Up until this release, PRT functionality was not supported. Now, PRT is supported as this does not require DSPs (local tone generation is not supported as DSPs are required).

For PRT functionality, the tones can be created with standard third-party, recording utilities such as Adobe Audition (formerly Cool Edit Pro) and combined into a single PRT file, using AudioCodes existing DConvert utility.

Note: This feature applies only to calls using the G.711 coder.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant Non-Hybrid SBC.

3.1.1.63 Enhanced Gateway Advice-of-Charge for Pre-billing

This feature provides enhanced support for the Advice of Charge (AOC) feature for Tel-to-IP calls. This feature is applicable only to the Gateway/IP-to-IP application.

AOC is a pre-billing feature that tasks the rating engine with calculating the cost of using a service and relaying that information to the customer thus, allowing users to obtain charging information for all calls at communication set-up time (AOC-S), periodically during the call (AOC-D), or at the end of the call (AOC-E). The AOC-S, AOC-D, and AOC-E messages are sent in the EURO ISDN Facility Information Element (IE) message. The device interworks these ISDN and SIP messages by converting the AOC messages into SIP INFO (during call) and BYE messages (end of call) in AudioCodes proprietary SIP AOC header.

This new feature provides two additional methods for sending the call charge information (AOC messages) in the Euro ISDN Facility IE:

- Proprietary method of Teles: The device calculates the charge units based on 6 Euro-cents per unit. Calculation is based on seconds. The formula is 0,06ct / (factor * scale). The device parses the proprietary format to calculate the time interval (in seconds, in steps of 0.5). If little tariff data is provided before the call is connected, the interval is calculated based on the last tariff data. The device ignores all tariffs sent after the call is established.
- Proprietary method of Cirpack: The device supports two AOC-E calculation methods:

- Summation method: The AOC-D message in the payload is an increment. The device generates the AOC-E. Parsing every AOC-D received, and summing the values is required to obtain the total sum (to be placed in the AOC-E). This method is performed if the 'Generate Metering Tones' parameter is set to SIP RAW Data Provided.
- Incremental method: The received AOC-D messages contain a subtotal. The device generates the AOC-E, parsing the last AOC-D is sufficient to obtain the value required to be placed in AOC-E. This method is performed if the 'Generate Metering Tones' parameter is set to SIP RAW Data Incremental Provided.

The AOC feature is enabled using the existing EnableAOC parameter.

To support this enhancement, new optional values have been added to the following existing parameter:

Web: Generate Metering Tones CLI: gen-mtr-tones [PayPhoneMeteringMode]	Determines the method used to configure the metering tones that are generated to the Tel side. ▪ [0] Disable = (Default) Metering tones aren't generated. ▪ [1] Internal Table = Metering tones are generated according to the device's Charge Code table. ▪ [2] SIP Interval Provided = (Proprietary method of TELES Communications Corporation) Periodic generation of AOC-D and AOC-E toward PSTN. The time interval is calculated according to the scale and tariff provided in the proprietary formatted file included in SIP INFO messages, which is always sent before 200 0K. ▪ [3] SIP RAW Data Provided = (Proprietary method of Cirpack) When receiving AOC-D in raw format, provided in the header of SIP INFO messages, the device parses AOC-D raw data in order to obtain the number of units. This number is sent in the Facility message with AOC-D. The device generates the AOC-E. Parsing every AOC-D received, and summing the values is required to obtain the total sum (to be placed in the AOC-E). ▪ [4] SIP RAW Data Incremental Provided = (Proprietary method of Cirpack) When receiving AOC-D in raw format, provided in the header of SIP INFO messages, the device parses AOC-D raw data in order to obtain the number of units. This number is sent in the Facility message with AOC-D. In addition, the device stores the latest number of units in order to send them in AOC-E IE when the call is disconnected.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.64 Gateway Three-Way Conferencing by Third-Party Conferencing Server

This feature provides support for an additional mode of operation when using an external, third-party Conferencing server (Media server) for managing three-way conferencing for FXS interfaces. The mode of operation is similar to the existing method used when conferencing is managed by a third-party server. The difference being that instead of sending the SIP REFER message to the remote participants, the device sends the REFER message to the Conferencing server. The Conferencing server then sends INVITE messages with Replaces header to the remote participants.

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

Web: Three Way Conference Mode CLI: 3w-conf-mode [3WayConferenceMode]	New Option – [3]: Defines the mode of operation for three-way conferencing. ▪ [3] Huawei Media Server = The conference is managed by an external, third-party Conferencing (media) server. The conference-initiating INVITE sent by the device uses only the ConferenceID as the Request-URI. The Conferencing server sets the Contact header of the 200 OK response to the

	actual unique identifier (Conference URI) to be used by the participants. The Conference URI is included in the URI of the REFER with Replaces header sent by the device to the Conferencing server. The Conferencing server sends an INVITE with Replaces header to the remote participants.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B.

3.1.1.65 Gateway Overlap Dialing using SIP INFO Messages

This feature provides support for configuring the device to use SIP INFO messages for sending subsequent phone number digits in overlap dialing. Up until this release, the device sent the remaining digits in re-INVITE messages. The feature is applicable to Tel-to-IP and IP-to-Tel calls.

To support the feature, an additional optional value has been added to the following existing parameters:

ISDN Overlap IP-to-Tel Dialing [ISDNTxOverlap]	New optional value [2] and modified [1] value. ▪ [0] Disable (default) ▪ [1] Through SIP = Sends subsequent phone number digits in SIP re-INVITE messages. ▪ [2] Through SIP INFO =Sends subsequent phone number digits in SIP INFO messages.
Select type of Overlap Receiving [ISDNRxOverlap]	New optional value [3] and modified value [2]. ▪ [0] None = (Default) Disabled. ▪ [1] Local receiving = ISDN Overlap Dialing - the complete number is sent in the INVITE Request-URI user part. The <device> receives ISDN called number that is sent in the 'Overlap' mode. The ISDN Setup message is sent to IP only after the number (including the Sending Complete IE) is fully received (via Setup and/or subsequent Info Q.931 messages). In other words, the <device> waits until it has received all the ISDN signaling messages containing parts of the called number, and only then it sends a SIP INVITE with the entire called number in the Request-URI. ▪ [2] Through SIP INVITE = Interworking of ISDN Overlap Dialing to SIP, based on RFC 3578. The <device> interworks ISDN to SIP by sending digits each time they are received (from Setup and subsequent Info Q.931 messages) to the IP, using subsequent SIP INVITE messages. ▪ [3] Through SIP INFO =Sends subsequent phone number digits in SIP INFO messages.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.66 Increased SBC Capacity of Signaling, Media and Registered Users

This feature provides support for an increase in the maximum number of supported signaling sessions, media sessions, and registered SIP users. For capacity figures, see Table 5-1 in Section 5.1 on page 235.

Applicable Products: Mediant 8xx; Mediant Non-Hybrid SBC.

3.1.1.67 Guaranteed SBC Call Sessions per SIP Entity

This feature provides support for configuring guaranteed (*reserved*) call capacity per SIP entity. Reserved call capacity can be applied per IP Group and/or SRD, for any call direction (incoming, outgoing, or both), and per SIP message type (INVITE or SUBSCRIBE).

Up until this release, only a maximum (*limit*) call capacity could be configured. However, maximum capacity does not guarantee capacity when the device is deployed to operate

with multiple SIP entities such as in a contact center environment handling multiple customers. For example, if the total call capacity of the device is 200, a scenario may arise where one SIP entity may reach the maximum configured call capacity of 200 and thus, leave no available call resources for the other SIP entities. This new feature guarantees a minimum capacity for each SIP entity.

If the reserved call capacity of a SIP entity is threatened by a new call for a different SIP entity, the device rejects the call to safeguard the reserved capacity.

Reserved call capacity can be configured for both an SRD and each of its associated IP Groups. In such a setup, the SRD's reserved call capacity must be greater or equal to the summation of the reserved call capacity of all these IP Groups. In other words, the SRD serves as the "parent" reserved call capacity. If the SRD's reserved call capacity is greater, the extra call capacity can be used as a shared pool between its IP Groups for unreserved calls when they exceed their reserved capacity. For example, assume the following configured reserved capacities for an SRD and its associated IP Groups:

- SRD reserved call capacity is 40
- IP Group 1 reserved call capacity is 10
- IP Group 2 reserved call capacity is 20

In this setup, the SRD offers a shared pool for unreserved call capacity of 10 (40 – [10 + 20]). If IP Group 1 needs to handle 15 calls, it is guaranteed 10 calls and the remaining 5 is provided from the SRD's shared pool. If the SDR's shared pool is currently empty and resources for new calls are required, the quota is taken from the device's total capacity, if available. For example, if IP Group 1 needs to handle 21 calls, it's guaranteed 10, the SRD's shared pool provides another 10 (now used up), and the last call is provided from the device's total call capacity support (e.g., of 200).

To support this feature, the following new parameter has been added to the existing Admission Control table:

Reservation CLI: sbc-admission-control [SBCAdmissionControl_Reservation]	Defines the guaranteed, minimum call capacity. Notes: ▪ An IP Group ID or SRD ID must be specified when this parameter is configured and for its functionality to work. The IP Group or SRD cannot be all (-1). ▪ Reserved call capacity is applicable only to INVITE and SUBSCRIBE messages. ▪ Reserved call capacity must be less than the maximum capacity (limit) configured for the CAC rule. ▪ The total reserved call capacity configured for all the CAC rules cannot exceed the device's total call capacity support.

Applicable Products: All.

3.1.1.68 Configurable Maximum SIP SUBSCRIBE Sessions for SBC

This feature provides support for configuring the maximum number of concurrent SIP SUBSCRIBE sessions permitted on the device.

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

[NumOfSubscribes]	Defines the maximum number of concurrent SIP SUBSCRIBE sessions. The valid value is any value between 0 and the maximum supported SUBSCRIBE sessions. When set to -1, the device uses the default value. For more information, contact your AudioCodes sales representative. Note: For this parameter to take effect, a device reset is required.

Note: The maximum number of SUBSCRIBE sessions can be increased by reducing the maximum number of SBC channels in the Software License Key. For every reduced SBC session, the device gains two SUBSCRIBE sessions.

Applicable Products: All.

3.1.1.69 Increased Maximum Number of SBC Configuration Table Rows

This feature provides support for an increase in the maximum number of rows (indices) that can be configured in the following tables:

Table	Mediant 8xx/500	Mediant 1000B/3000	Mediant 4000/2600/SW
SRD Table	-	-	500 (from 31)
SIP Interface	-	-	500 (from 32)
IP Group	50 (from 32)	100 (from 32)	200 (from 32)
Proxy Sets	50 (from 32)	100 (from 32)	200 (from 32)
Account Table	50 (from 32)	100 (from 32)	200 (from 32)
Message Policy	20	20	20
Message Manipulations	-	-	200 (from 100)
IP Profile Settings	20 (from 9)	40 (from 9)	40 (from 9)
Admission Control	-	-	200 (from 100)
Classification	-	-	200 (from 100)
Condition	20	20	40
IP to IP Routing	500 (from 200)	500 (from 200)	-
Alternative Routing Reasons	20 (from 5)	20 (from 5)	20 (from 5)
IP to IP Inbound Manipulation	-	-	200 (from 100)
IP to IP Outbound Manipulation	-	-	200 (from 100)

Applicable Products: All.

3.1.1.70 Rate Limiting of User Registration Requests with Proxy

This feature provides support for limiting the number of registration requests that the device sends per second, to a proxy (registrar) server. The benefit of this feature is that it can be used to prevent an overload on the device's CPU, which may be caused by the sending of many (for example, 1,000) registration requests to a proxy server at any given time.

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

Max Generated Register Rate CLI: configure voip/sip-definition proxy-and-registration/max-gen-reg-rate [MaxGeneratedRegistersRate]	Defines the maximum number of user register requests that the device can send to a proxy (registrar) server per second. The valid value is 30 to 300 register requests per second. The default is 100.

Applicable Products: All.

3.1.1.71 SBC Device Authentication of SIP Servers

This feature provides support for authenticating remote SIP servers, as an Authentication server. This provides protection from rogue SIP servers, preventing unauthorized usage of device resources and functionality.

Up until this release, the device could be configured as an Authentication server to authenticate SIP clients only. This prevented unauthorized usage of the device resources by rogue SIP clients. The usernames and passwords of the SIP clients for authentication were stored in the SBC User Info file.

To authenticate remote servers, the device challenges the server with a user-defined username and password which is shared with the remote server. When the device receives an INVITE request from the remote server, it challenges the server by replying with a SIP 401 Unauthorized response containing the WWW-Authenticate header. The remote server then re-sends the INVITE containing an Authorization header with authentication information based on this username-password combination to confirm its identity. The device uses the username and password to authenticate the message prior to processing it.

This feature is configured per Server-type IP Group, which represents the remote server. The IP Group needs to be configured with the following:

- 'Authentication Mode' (existing parameter) set to SBC as Server.
- Specify SIP requests (for example, INVITE) that must be challenged by the device, using the 'Authentication Method List' parameter (existing).
- Shared username and password for authenticating the IP Group. This is configured by the following new IP Group parameters:

Username [IPGroup_Username]	Defines the username for authentication. The valid value is a string of up to 51 characters. By default, no username is defined. Note: This parameter is applicable only when Authentication Mode is set to SBC as Server (i.e., authentication of servers).
Password IPGroup_Password]	Defines the password for authentication. The valid value is a string of up to 51 characters. By default, no password is defined. Note: This parameter is applicable only when Authentication Mode is set to SBC as Server (i.e., authentication of servers).

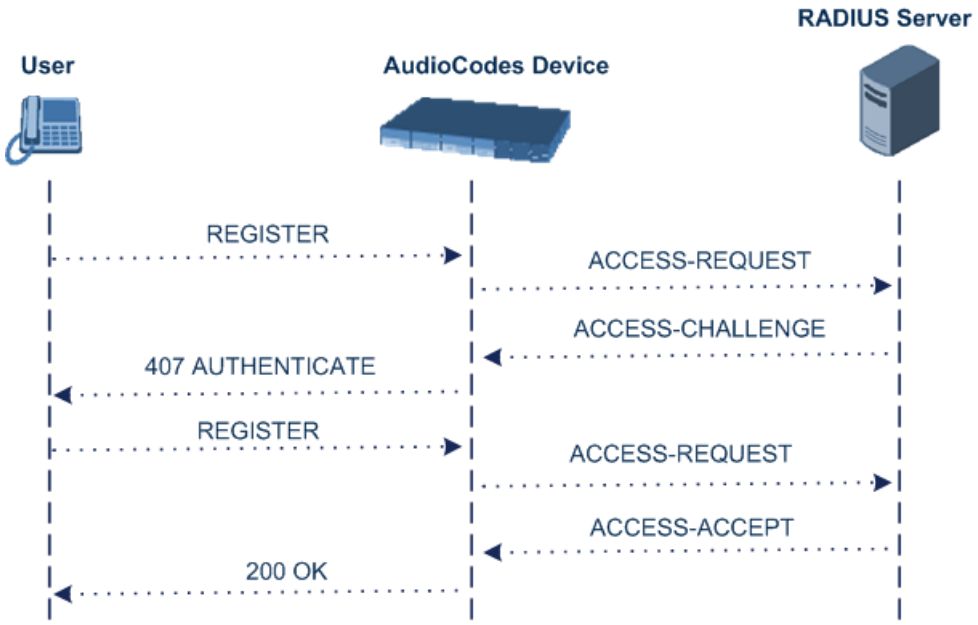
Applicable Products: All.

3.1.1.72 RADIUS Digest Authentication (RFC 5090) for SBC

This feature provides support for digest authentication of SIP users by a RADIUS server, according to RFC 5090. This feature allows the device to offload the MD5 calculation (validation) to an external server (RADIUS server), where the device is classed as a RADIUS client. Up until this release, the device supported RFC 2865 and RFC 2866. Authorizing of calls was done locally, whereby the device challenged the method and validated the response.

RFC 5090 implements digest authentication without being provided a user password attribute. RFC 5090 defines new attributes that allows a remote server to perform remote authentication. Nonces required by the digest algorithm are generated by the RADIUS server.

The figure below illustrates a successful authentication by a RADIUS server:



1. SIP client sends the device an HTTP/SIP request without an authorization header.
2. Device sends this request (Access-Request packet) to the RADIUS server.
3. RADIUS server sends an Access-Challenge to the device with a generated nonce.
4. Device constructs and sends a Proxy-Authorization header (based on the digest attributes from the RADIUS server) to the SIP client (Authenticate 407).
5. SIP client sends credentials to the device.
6. Device forwards the user credentials to the RADIUS server.
7. RADIUS server verifies the credentials and either sends an Access-Accept or Access-Reject to the device.
8. Device processes the SIP client's request (sends 200 OK) or rejects it (sends again 'Proxy Authorization required' to the SIP user (Authenticate 407).

This feature is configured by the existing RADIUS server parameters (RADIUS Authentication Server IP Address; RADIUS Authentication Server Port; RADIUS Shared Secret) as well as by the following new parameter:

Web: SBC Server Auth Mode CLI: sbc-server-auth-mode [SBCServerAuthMode]	Defines whether authentication of the SIP client is done locally (by the device) or by the RADIUS server. ▪ [0] (default) = Authenticate locally. ▪ [1] = Authentication is done by the RFC 5090 compliant RADIUS server

Applicable Products: All.

3.1.1.73 SBC Client Authentication based on RADIUS draft-sterman-aaa-sip-01

This feature provides support for the RADIUS extension for digest authentication of SIP clients, according to draft-sterman-aaa-sip-01. Based on this standard, the device generates the nonce (in contrast to RFC 5090 where it is done by the RADIUS server).

RADIUS based on draft-sterman-aaa-sip-01 operates as follows:

1. SIP client sends the device a SIP request without an Authorization header.
2. Device generates nonce and sends it to the client in a SIP 407 (Proxy Authentication Required) response.
3. SIP client sends the SIP request with the Authorization header to the device.
4. Device sends an Access-Request to the RADIUS server.

5. RADIUS server verifies the credentials and sends an Access-Accept (or Access-Reject) to the device.
6. Device processes the SIP client's request (sends 200 OK or forwards the authenticated request) or rejects it (sends another SIP 407 to the SIP client).

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

Web: SBC Server Auth Mode CLI: sbc-server-auth-mode [SBCServerAuthMode]	Defines whether authentication of the SIP client is done locally (by the device) or by the RADIUS server. ▪ [0] (default) = Authenticate locally. ▪ [1] = Authentication is done by the RFC 5090 compliant RADIUS server ▪ [2] = Authentication is done according to the Draft Sterman-aaa-sip-01 method.

Applicable Products: All.

3.1.1.74 SBC Expiry Time Extension for Registered Users

This feature provides support for adding extra time (graceful time) to the expiration timer of registered users in the device's Users Registration database. Typically, when a user's registration timer expires, the device removes the user from the database. However, this new feature keeps the user in the database (does not send an unregister to the registrar server), allowing the user to send a "late" re-registration to the device. Only when this additional time expires does the device remove the user from the database.

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

Web: User Registration Grace Time CLI: sbc-usr-reg-grace-time [SBCUserRegistrationGraceTime]	Defines additional time (in seconds) to add to the registration expiry time. The valid value is 0 to 300 (i.e., 5 minutes). The default is 0.

Applicable Products: All.

3.1.1.75 SBC Registered Users Retained even if Proxy not Responding

This feature provides support for keeping registered users in the device's Users Registration database even if connectivity with the SIP proxy server is lost. The device removes the users only when their registration expiry time is reached (with the additional "graceful" registration time, if configured). Up until this release, the device removed users from the database when the proxy did not respond to their registration refresh requests.

Applicable Products: All.

3.1.1.76 SBC Random Assignment of Expiry Time Value

This feature provides support for assigning a random expiry time for registration and subscription requests from users. The expiry time value appears in the Expires header in REGISTER and SUBSCRIBE SIP messages. When the device receives such a request from a user, it forwards it to the proxy or registrar server. Upon a successful registration or subscription, the server sends a SIP 200 OK response. If the expiry time was unchanged by the server, the device applies this feature and changes the expiry time in the SIP 200 OK response before forwarding it to the user; otherwise, the device does not change the expiry time.

This feature is useful in scenarios where multiple users may refresh their registration or subscription simultaneously, thereby causing the device to handle many such sessions at a given time. This may result in an overload of the device (reaching maximum session capacity), thereby preventing the establishment of new calls or preventing the handling of some user registration or subscription requests.

When this feature is enabled, the device assigns a random expiry time to each user registration or subscription. Thus, this ensures that future user registration and subscription requests are more distributed over time (i.e., do not all occur simultaneously).

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

Web: Randomize Expires Time CLI: config-voip>sbc general-setting sbc-rand-expire [SBCRandomizeExpires]	Defines a value (in seconds) used to calculate a new value for the expiry time in the Expires header of SIP 200 OK responses for user registration and subscription requests sent to users. The device takes any random number between 0 and this configured value, and then subtracts this number from the original expiry time value. For example, assume that the original expiry time is 120 and this parameter is set to 10. If the device randomly chooses the number 5 (i.e., between 0 and 10), the resultant expiry time will be 115 (120-5). The valid value is 0 to 20. The default is 10. If set to 0, the device does not change the expiry time. Notes: ▪ The lowest expiry time that the device sends in the 200 OK, regardless of the resultant calculation, is 10 seconds. For example, if the original expiry time is 12 seconds and this parameter is set to 5, theoretically, the new expiry time can be less than 10 (e.g., 12 – 4 = 8). However, the expiry time will be set to 10. ▪ The expiry time received from the user can be changed by the device before forwarding it to the proxy. This is configured by the SBCUserRegistrationTime parameter.

Applicable Products: All.

3.1.1.77 SBC Routing In-dialog Refresh SUBSCRIBE Requests

This feature provides support for routing refresh SUBSCRIBE requests within an ongoing subscribe dialog to the "working" (connected) proxy server. The "working" proxy (address) is determined by the device's keep-alive mechanism for the Proxy Set that was used to route the initial SUBSCRIBE. Up until this release, the device routed in-dialog refresh SUBSCRIBES according to the proxy address in the Contact header of the SIP 200 OK received from the proxy to which the initial SUBSCRIBE was sent (as per SIP standard).

Note that this feature is not applicable (disabled) when proxy load-balancing is enabled.

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

CLI: configure voip/sbc general-setting/sbc-dialog-subsc-route-mode [SBCInDialogSubscribeRouteMode]	Enables the device to route in-dialog refresh SUBSCRIBE requests to the "working" proxy. ▪ [0] = (Default) Disable – Device sends in-dialog refresh SUBSCRIBES according to address in Contact header of 200 OK received from proxy to which initial SUBSCRIBE was sent. ▪ [1] = Enable – Device routes in-dialog refresh SUBSCRIBES to "working" proxy (regardless of Contact header). Note: For this feature to be functional, ensure the following: ▪ Keep-alive mechanism is enabled for the Proxy Set ('Enable Proxy Keep Alive' parameter is set to any value other than Disable). ▪ Load-balancing between proxies is disabled ('Proxy Load Balancing Method' parameter is set to Disable).

Applicable Products: All.

3.1.1.78 UDP Port Spacing and Maximum Port

This feature provides support for configuring the "distance" or spacing between consecutively assigned ports for RTP, RTCP, and T.38 media streams. The spacing

between ports can now be configured to 5 (default) or 10. Up until this release, the spacing between ports was fixed to 10, for example, 6150, 6160, 6170 and so on. This feature applies only to Mediant 2600, Mediant 4000, Mediant 9000 and Mediant SW. For all other products, the port spacing is fixed to 10. Note that the device allocates ports randomly within the configured port range (using the existing BaseUDPPort parameter).

This feature also increases the maximum port to 65535, regardless of the number of supported channels (sessions), as was the case in the previous release. This feature applies to Mediant 5xx, Mediant 8xx, Mediant 2600, Mediant 4000, Mediant 9000 and Mediant SW. The port range is calculated as follows:

```
BaseUDPPort to 65,535
```

For all other products, the port range is calculated as follows:

```
BaseUDPPort to (BaseUDPPort + number of channels*10)
```

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

[UdpPortSpacing]	Defines the UDP port spacing. ▪ [5] (default) ▪ [10] Note: A device reset is required for this parameter to take effect.

Applicable Products: Mediant Non-Hybrid SBC.

3.1.1.79 Enhanced Media Latching

This feature provides support for an enhancement to the device's media (RTP, RTCP, SRTP, SRTCP, and T.38) latching feature. This enhancement assists in protecting the device against malicious attacks (i.e., Denial of Service) from multiple sources of traffic. Thus, this can prevent an established call been stolen by a malicious attacker on the media stream.

The device's channel latches on to the first stream of the first received packet. All packets (any media type) received from the same IP address and SSRC are accepted. For T.38 packets, the device considers only the IP address. If the channel receives subsequent packets from a non-latched source, the channel latches onto this new media stream if the following conditions exist:

- A minimum number (user-defined) of continuous packets (per media type) have been received from the new stream - configured by the new parameter, 'No packets have been received within a user-defined period from the current media stream - configured by the new parameter, 'TimeoutToRelatch<media type>Msec'.
- For SRTP streams, the call media latches onto the new stream only if it also successfully passes the SRTP decipher process.

Latching of a new T.38 stream is now reported in CDR using the following new CDR fields:

- LatchedT38Ip – new IP address
- LatchedT38Port – new port

In addition, the SIP PUBLISH message updates the latched RTP SSRC, for example:

```
RemoteAddr: IP=10.33.2.55 Port=4000 SSRC=0x66d510ec
```

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

Inbound Media Latch Mode CLI: inbound-media-latch-mode [InboundMediaLatchMode]	Applicable only to Mediant 5xx, Mediant 8xx, Mediant 2600, Mediant 4000, Mediant 9000, and Mediant SW. New optional values [2] and [3]. Enables the Media Latching feature. ▪ [0] Strict = Device latches onto the first original stream (IP address:port). It does not latch onto any other stream during the session. ▪ [1] Dynamic = (Default) Device latches onto the first stream. If it receives at least a minimum number of consecutive packets (configured by New<media type>StreamPackets) from a different

	source(s) and the device has not received packets from the current stream for a user-defined period (TimeoutToRelatch<media type>Msec), it latches onto the next packet received from any other stream. If other packets of a different media type are received from the new stream, based on IP address and SSRC for RTCP/RTP and based on IP address only for T.38, the packet is accepted immediately. Note: If a packet from the original (first latched onto) IP address:port is received at any time, the device latches onto this stream. ▪ [2] Dynamic-Strict = Device latches onto the first stream. If it receives at least a minimum number of consecutive packets (configured by New<media type>StreamPackets) all from the same source which is different to the first stream and the device has not received packets from the current stream for a user-defined period (TimeoutToRelatch<media type>Msec), it latches onto the next packet received from any other stream. If other packets of different media type are received from the new stream based on IP address and SSRC for RTCP and based on IP address only for T.38, the packet is accepted immediately. Note: If a packet from the original (first latched onto) IP address:port is received at any time, the device latches onto this stream. ▪ [3] Strict-On-First = Typically used for NAT, where the correct IP address:port is initially unknown. The device latches onto the stream received in the first packet. The device does not change this stream unless a packet is later received from the original source.
New RTP Stream Packets [NewRtpStreamPackets]	Defines the minimum number of continuous RTP packets received by the device's channel to allow latching onto the new incoming stream. The valid range is 0 to 20. The default is 3. If set to 0, the device is left exposed to attacks against multiple packet streams.
New RTCP Stream Packets [NewRtcpStreamPackets]	Defines the minimum number of continuous RTCP packets received by the device's channel to allow latching onto the new incoming stream. The valid range is 0 to 20. The default is 3. If set to 0, the device is left exposed to attacks against multiple packet streams.
New SRTP Stream Packets [NewSRTPStreamPackets]	Defines the minimum number of continuous SRTP packets received by the device's channel to allow latching onto the new incoming stream. The valid range is 0 to 20. The default is 3. If set to 0, the device is left exposed to attacks against multiple packet streams.
New SRTCP Stream Packets [NewSRTCPStreamPackets]	Defines the minimum number of continuous SRTCP packets received by the device's channel to allow latching onto the new incoming stream. The valid range is 0 to 20. The default is 3. If set to 0, the device is left exposed to attacks against multiple packet streams.
Timeout To Relatch RTP (msec) [TimeoutToRelatchRTPMsec]	Defines a period (msec) during which if no packets are received from the current RTP session, the channel can re-latch onto another stream. The valid range is any value from 0. The default is 200.
Timeout To Relatch SRTP [TimeoutToRelatchSRTPMsec]	Defines a period (msec) during which if no packets are received from the current SRTP session, the channel can re-latch onto another stream. The valid range is any value from 0. The default is 200.
Timeout To Relatch Silence [TimeoutToRelatchSilenceMsec]	Defines a period (msec) during which if no packets are received from the current RTP/SRTP session and the channel is in silence mode, the channel can re-latch onto another stream. The valid range is any value from 0. The default is 200.
Timeout To Relatch RTCP	Defines a period (msec) during which if no packets are received from

[TimeoutToRelatchRTCP Msec]	the current RTCP session, the channel can re-latch onto another RTCP stream. The valid range is any value from 0. The default is 10,000.
Fax Relay Rx/Tx Timeout [FaxRelayTimeoutSec]	Defines a period (sec) during which if no T.38 packets are received or sent from the current T.38 fax relay session, the channel can re-latch onto another stream. The valid range is 0 to 255. The default is 10.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant Non-Hybrid SBC.

3.1.1.80 Enhanced NAT Configuration for Media

This feature provides enhanced support for NAT configuration for media on the device. This concerns NAT scenarios in which the far-end (remote) endpoint is located behind a NAT server. In such cases, although the remote endpoint sends its private IP address:port in the SIP message (INVITE), the device receives the media packets (RTP, RTCP, and T.38) with a source address of a public IP address:port (i.e., allocated by the NAT server). Therefore, to ensure that the media reaches the endpoint (via the NAT address), the device should send it to the public address.

The device identifies whether the endpoint is located behind NAT, by comparing the source IP address of the first received media packet, with the IP address and UDP port of the first received SIP message (INVITE) when the SIP session was started.

This new feature enables the following NAT modes:

- NAT is disabled: The device always sends the media packets to the remote endpoint using the IP address:port obtained from the first received SIP message.
- NAT is used only if necessary: If the endpoint is identified as being located behind NAT, the device sends the media packets to the public IP address:port obtained from the source address of the first media packet received from the endpoint. Otherwise, the packets are sent using the IP address:port obtained from the address in the first received SIP message.
- NAT is always used: The device always sends the media packets to the remote endpoint using the source address obtained from the first media packet received from the endpoint.

To support this feature, the following parameter has been modified (parameter name and options):

Web/EMS: NAT Mode CLI: disable-NAT-traversal [NATMode]	Enables the NAT feature for media when the device communicates with endpoints located behind NAT. ▪ [0] Auto-Detect = NAT is performed if necessary. If the endpoint is identified as being located behind NAT, the device sends the media packets to the public IP address:port obtained from the source address of the first media packet received from the endpoint. Otherwise, the packets are sent using the IP address:port obtained from the address in the first received SIP message. ▪ [1] NAT Is Not Used = (Default) NAT feature is disabled. The device always sends the media packets to the remote endpoint using the IP address:port obtained from the first received SIP message. ▪ [2] NAT Is Used = NAT is always performed. The device always sends the media packets to the remote endpoint using the source address obtained from the first media packet from the endpoint.

Applicable Products: All.

3.1.1.81 ICMP Destination Unreachable Message

This feature provides support for enabling or disabling the sending of an Internet Control Message Protocol (ICMP) Destination Unreachable message. The device sends this message in response to a packet that cannot be delivered to its destination for reasons other than congestion. ICMP is used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is unavailable. A Destination Unreachable message can be sent upon any of the following:

- Address unreachable
- Port unreachable

This feature is applicable to IPv4 and IPv6 addressing schemes.

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

Web: Send ICMP Unreachable Messages [DisableICMPUnreachable]	Enables sending of ICMP Unreachable messages. ▪ [0] Enable = (Default) Device sends these messages. ▪ [1] Disable = Does not send ICMP messages.

Applicable Products: Mediant 500 E-SBC; Mediant 800B Gateway & E-SBC; Mediant 1000B; Mediant 3000; Mediant Non-Hybrid SBC.

3.1.1.82 Efficient SRTP-to-SRTP with Transcoding

This feature provides support for efficient SRTP-to-SRTP with transcoding (encryption/decryption) capabilities between SIP entities, by utilizing only a single DSP. For SRTP-to-SRTP calls, transcoding capabilities, for example, coder transrating only require one DSP. Thus, this feature frees up DSP resources for additional call sessions or other transcoding functionalities.

Applicable Products: Mediant 3000.

3.1.1.83 Generation of SRTP Key

This feature provides support for generating a new SRTP key when the device receives a SIP re-INVITE message. This feature is configured per SIP entity (IP Group) using IP Profiles.

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

Generate SRTP keys mode CLI: generate-srtp-keys [IpProfile_GenerateSRTPKeys]	Enables the device to generate a new SRTP key upon receipt of a re-INVITE for the SIP entity. ▪ [0] Only If Required= (Default) The device generates an SRTP key only when necessary. ▪ [1] Always = The device always generates a new SRTP key.

Applicable Products: All.

3.1.1.84 iLBC Coder Support

This feature provides support for the Internet Low Bitrate Codec (iLBC) speech coder. The iLBC is suitable for robust voice communication over IP. The codec is designed for narrowband speech and results in a payload bit rate of 13.33 Kbit/s with an encoding frame length of 30 msec and 15.20 kbps with an encoding length of 20 msec. The iLBC codec enables graceful speech quality degradation in the case of lost frames, which occurs in connection with lost or delayed IP packets.

To support this feature, the iLBC coder has been added to the list of optional coders in the Allowed Coders Group table, Coders table, and Coder Group Settings table.

- iLBC [iLBC]
- Packetization Time: 20; 40; 60; 80; 100; 120 msec

- Rate (Kbps): 13; 15
- Payload Type: 65
- Silence Suppression: enable/disable

Note: This coder is already supported on other products from previous releases.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000.

3.1.1.85 Media Realm with Multiple Port Ranges and Interfaces

This feature provides support for configuring the device with a Media Realm that has multiple port range to interface settings. Up until this release, a Media realm could only be configured (in the Media Realm table) with one port range and for one specific network interface. Now, the Media Realm can be configured with multiple port range-interface settings, using the new "child" table of the Media Realm table, called Media Realm Extensions table. Thus, the Media Realm can now be distributed across multiple interfaces. Media Realm Extensions can be useful, for example, where limitations (constraints) exist for bandwidth or number of media ports per interface. As a Media Realm is associated with an IP Group, media streams pertaining to the IP Group can now distributed across the network media interfaces.

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

Media Realm Extension [SubRealm]	Defines Media Realm Extensions. The format of the ini file table parameter is as follows: [MediaRealmExtension] FORMAT MediaRealmExtension_Index = MediaRealmExtension_MediaRealmIndex, MediaRealmExtension_ExtensionIndex, MediaRealmExtension_IPv4IF, MediaRealmExtension_IPv6IF, MediaRealmExtension_PortRangeStart, MediaRealmExtension_PortRangeEnd, MediaRealmExtension_MediaSessionLeg; [\MediaRealmExtension]

Applicable Products: All.

3.1.1.86 SBC Non-Standard or Unknown Audio Coders Allowed List

This feature provides support for voice (audio) coders that are non-standard or unknown. This is configured by typing any string value in the Allowed Coders Group table (existing) to represent the non-standard or unknown coder (e.g., "JohnCoder"). The device uses this voice coder for the specified SIP entity if this coder name also appears in the SDP offer ('a=rtpmap' field) from the SIP entity. The coder is associated with the SIP entity, by assigning its Allowed Coders Group ID to the SIP entity's IP Profile. Note that the coder name is not case-sensitive. Thus, the Allowed Coders Group table can include pre-defined coders and user-defined coders.

Applicable Products: All.

3.1.1.87 SBC Media Types Allowed List

This feature provides support for configuring a list of media types that are permitted for a specific SIP entity. The media type appears in the SDP 'm=' line (e.g., 'm=audio'). The device uses only the media types that appear in both the SDP offer and the configured media types lists. If not configured, the device permits all media types. If no common media types exist between the SDP offer and the configured media types list, the device drops the call.

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

Allowed Media Types	Defines media types permitted for the SIP entity associated with this

CLI: sbc-allowed-media-types [IPProfile_SBCAllowedMediaTypes]	IP Profile. The valid value is a string of up to 64 characters. To configure multiple media types, separate the strings with a comma, e.g., "media, audio" (but without the quotes). By default, no media types are configured (i.e., all media types are permitted).

Note that other non-related features may be employed to modify the SDP, including media types.

Applicable Products: All.

3.1.1.88 SBC Video Coders Allowed List

This feature provides support for configuring a list of permitted video coders when forwarding video streams to a specific SIP entity. The list applies to media of the type "video" in the SDP (i.e., 'm=video' line). The list includes default video coders as well as optional, user-defined (string) video coders for non-standard or unknown coders. The video coders are configured in the new Allowed Video Coders Group table and associated with the SIP entity by assigning the relevant Allowed Video Coders Group ID to the SIP entity's IP Profile. For the SIP entity, the device uses only the video coders that appear in both the SDP offer and the Allowed Video Coders Group ID.

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

IP Profile table Allowed Video Coders Group ID [IPProfile_SBCAllowedVideoCodersGroupID]	Assigns an Allowed Video Coders Group ID to the IP Profile. The default value is 0. If not defined, all video coders are allowed. The coders are configured in the Allowed Video Coders Group table.
Allowed Video Coders Group CLI: sbc allowed-video-coders-group [AllowedVideoCodersGroup0/1/2/3/4]	Defines groups of video coders for enforcing coder use for a SIP entity. Each group can be configured with up to 20 coders. Each group can be defined with pre-configured coders as well as user-defined coders. The valid value for user-defined coders is a string of up to 25 characters. For example, "WOW.789" (but without quotes). Up to four groups can be defined. [AllowedVideoCodersGroup0] FORMAT AllowedVideoCodersGroup_Index = AllowedVideoCodersGroup_Name; [\AllowedVideoCodersGroup] Name = Name of the user-defined coder

Note that the SBC Allowed Coders Mode parameter, which specifies various modes of operation for Allowed Coders, is also applicable to this feature.

Applicable Products: All.

3.1.1.89 SBC Handling of RTCP during Call Sessions

This feature provides support for various handling methods for RTP Control Protocol (RTCP) packets during call sessions. This handling can include one of the following:

- Forwards the received RTCP as is (unless transcoding is done, in which case the device generates RTCP on both legs).
- Generates RTCP packets during active and inactive (i.e., during call hold) RTP periods.
- Generates RTCP during active RTP periods only. In other words, the device does not generate RTCP when there is no RTP traffic (such as in call on-hold).

This feature is useful for interworking RTCP between SIP entities. For example, this may be necessary when incoming RTCP is not compatible with the destination SIP entity's RTCP support. In such scenarios, the device can generate the RTCP and send it to the SIP entity.

Note: The device can generate RTCP only if transcoding is not employed.

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

IP Profile table: RTCP Mode [IPProfile_SBCRTCPMode]	Defines how the device handles RTCP per IP Profile. ▪ [0] Transparent (default) = RTCP is forwarded as is. ▪ [1] Generate Always = Generates RTCP during active and inactive (e.g., call on-hold) RTP periods (i.e., media is 'a=recvonly' or 'a=inactive' in the INVITE SDP). ▪ [2] Generate only if RTP Active = Generates RTCP only during active RTP periods.
SBC RTCP Mode CLI: sbc-rtcp-mode [SBCRTCPMode]	Defines how the device handles RTCP (global parameter). ▪ [0] Transparent (default) ▪ [1] Generate Always ▪ [2] Generate only if RTP Active

Applicable Products: All.

3.1.1.90 SBC Transcoding of RTP Ptime, Silence Suppression and DTMF

This feature provides support for enhanced transcoding between SIP entities. The following new transcoding capabilities are supported:

- Packetization time (ptime) of the coder (transrating). Note that DSPs are not required for this functionality (except for Mediant 3000).
- Silence suppression
- DTMF payload type

These transcoding features are applied by using IP Profiles for each SIP entity. To support this feature, the following new parameters have been added to the IP Profile table:

Web: SDP Ptime Answer CLI: sbc-sdp-ptime-ans [IpProfile_SBCSDPPtimeAnswer]	Defines the ptime value for RTP packets. ▪ [0] Remote Answer (Default) = Use ptime according to SDP answer. ▪ [1] Original Offer = Use ptime according to SDP offer. ▪ [2] Preferred Value= Use preferred ptime for negotiation (if defined)
Web: Preferred Ptime CLI: sbc-preferred-ptime [IpProfile_SBCPreferredPTime]	Defines the ptime value (in msec) for this SIP entity if the 'SBC SDP Ptime Answer' parameter is set to Preferred Value. The valid range is 0 to 200. The default is 0 (i.e., preferred ptime is not used).
Web: Use Silence Suppression CLI: sbc-use-silence-supp [IpProfile_SBCUseSilenceSupp]	Defines silence suppression support for the SIP entity. ▪ [0] Transparent (default) = Forward as is. ▪ [1] Add = Enable silence suppression for each relevant coder listed in the SDP. ▪ [2] Remove = Disable silence suppression for each relevant coder listed in the SDP.
Web: SBC RFC2833 DTMF Payload Type CLI: sbc-2833dtmf-payload [IpProfile_SBC2833DTMFPayloadType]	Defines the payload type of DTMF digits in the RTP stream according to RFC 2833, for this SIP entity. The valid range is 0 to 200. The default is 0.

Applicable Products: All.

3.1.1.91 SBC Interworking RFC 2833 Payload Type without DSPs

This feature provides support for interworking the RFC 2833 payload type between SIP entities (e.g., payload type 97 to payload type 101), without the need for DSP resources. Up until this release, the device required two DSPs for this functionality.

Applicable Products: All.

3.1.1.92 On-Demand Jitter Buffer for SBC Calls

This feature provides support for an on-demand jitter buffer for SBC calls per SIP entity. This jitter buffer can be used (when other functionality such as voice transcoding are not employed, for Mediant 3000, Mediant 5xx, Mediant 8xx, Mediant 2600, Mediant 4000). Up until this release, jitter buffering for SBC calls could only be implemented together with voice transcoding.

The jitter buffer is assigned per SIP entity using IP Profiles. The jitter buffer is useful when incoming packets are received at inconsistent intervals (i.e., packet delay variation). The jitter buffer stores the packets and sends them out at a constant rate (according to the coder's settings).

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

Jitter Compensation CLI: sbc-jitter-compensation [IpProfile_SBCJitterCompensation]	Enables the on-demand jitter buffer. ▪ [0] Disable (default) ▪ [1] Enable

Notes:

- The existing jitter buffer parameters, 'Dynamic Jitter Buffer Minimum Delay' (DJBufMinDelay) and 'Dynamic Jitter Buffer Optimization Factor' (DJBufOptFactor) can be used to configure minimum packet delay only when transcoding is employed.
- DSP resources may be required for this functionality for Mediant 5xx, Mediant 8xx, Mediant 2600, and Mediant 4000).

Applicable Products: All.

3.1.1.93 SBC Fax Detection and Negotiation for SIP Entities

This feature provides support for handling fax detection and negotiation for remote SIP entities that do not support this functionality. This feature applies to faxes sent immediately upon establishment of a voice channel (i.e., after 200 OK). The device attempts to detect the fax within a user-defined interval upon establishment of the voice call.

The device can detect the fax signal (CNG tone) from the originating SIP entity and handle the subsequent fax negotiation by sending re-INVITE messages to both SIP entities. The device also performs fax-coder negotiation between the two SIP entities. The negotiated coders are according to the list of fax coders assigned to each SIP entity, using the IP Profile parameter 'Fax Coders Group ID'.

Notes:

- This feature is applicable only when both SIP entities do not support fax detection (receive or send) and negotiation.
- This feature is supported only when at least one of the SIP entities use G.711.
- This feature utilizes DSP resources. If there are insufficient resources, the fax transaction fails.

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

IP Profile table: Remote Renegotiate on Fax Detection [IPProfile_SBCRemoteRenegotiateOnFaxDetection]	Enables local handling of fax detection and negotiation. ▪ [0] Don't Care = (Default) Device does not interfere in the fax transaction and assumes that the SIP entity fully supports fax renegotiation upon fax detection. ▪ [1] Only on Answer Side = The SIP entity supports fax renegotiation upon fax detection only if it is the terminating (answering) fax, and does not support renegotiation if it is the originating fax. ▪ [2] No = The SIP entity does not support fax re-negotiation upon

	fax detection when it is the originating or terminating fax. Note: This feature is applicable only when both SIP entities do not fully support fax detection (receive or send) and negotiation: one SIP entity must be assigned an IP Profile where this parameter is set to [1] or [2], while the peer SIP entity must be assigned an IP Profile where this parameter is set to [2].
Web: SBC Fax Detection Timeout [sec] CLI: sbc-fax-detection-timeout [SBCFaxDetectionTimeout]	Defines the duration (in seconds) for which the device tries to detect fax. This duration starts at the establishment of the voice call. The valid value is 1 to any integer. The default is 10.

Applicable Products: Mediant 500 MSBR; Mediant 8xx; Mediant 1000B Series; Mediant 3000; Mediant 4000.

3.1.1.94 Gateway Fax over IP using T.38 Transmission over RTP

This feature provides support for Fax over IP (FoIP) transmissions using T.38 over RTP, whereby the T.38 payload is encapsulated in the RTP packet. Up until this release, the device sent T.38 as dedicated T.38 packets (out-of-band).

T.38 is the ITU standard for real-time facsimile (fax) over the IP network. To indicate T.38 over RTP, the SDP body uses "udptl" (Facsimile UDP Transport Layer) in the 'a=ftmp' line. AudioCodes supports T.38 over RTP according to this standard or according to AudioCodes proprietary method, as follows:

- Call parties belong to AudioCodes devices: AudioCodes proprietary T.38-over-RTP method is used, whereby the device encapsulates the entire T.38 packet – payload with all its headers - in the sent RTP. AudioCodes devices use the proprietary identifier for T.38 over RTP -- "AcUdptl" -- in the 'a=ftmp' line of the SDP, for example:

```
v=0
o=AudiocodesGW 1357424688 1357424660 IN IP4 10.8.6.68
s=Phone-Call
c=IN IP4 10.8.6.68
t=0 0
m=audio 6080 RTP/AVP 18 100 96
a=ptime:20
a=sendrecv
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:100 t38/8000
a=fmtp:100 T38FaxVersion=0
a=fmtp:100 T38MaxBitRate=0
a=fmtp:100 T38FaxMaxBuffer=3000
a=fmtp:100 T38FaxMaxDatagram=122
a=fmtp:100 T38FaxRateManagement=transferredTCF
a=fmtp:100 T38FaxUdpEC=t38UDPRedundancy
a=fmtp:100 AcUdptl
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
```

- AudioCodes call party with non-AudioCodes party: The device uses the standard T.38-over-RTP method, which encapsulates only the T.38 payload without its headers (i.e., includes only fax data) in the sent RTP packet (RFC 4612).

The T.38-over-RTP method also depends on call initiator:

- Device initiates a call: The device always sends the SDP offer where the 'fmtp' attribute includes the proprietary token "AcUdpTl". If the SDP answer includes the same token, the device employs AudioCodes proprietary T.38-over-RTP mode;

otherwise, the standard mode is used.

- Device answers a call: If the SDP offer from the remote party contains the 'fmtp' attribute with "AcUdpTI", the device answers with the same attribute and employs AudioCodes proprietary T.38-over-RTP mode; otherwise, the standard mode is used.

To support this feature, the following new coder has been added to the Coders table and Coder Group Settings table:

Coder name	Packetization Time	Rate	Payload Type	Silence Suppression
T.38 Over RTP [t38OverRTP]	N/A	N/A	Dynamic (90 - 127; default 106)	N/A

Note: If both T.38 (regular) and T.38 over RTP coders are negotiated between the call parties, T.38 over RTP is used.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.95 Gateway CED Tone Transfer Enhancement for V.150.1 Fax/Modem Relay

This feature provides support for additional options for transferring the fax/modem CED (answering) tone. The CED tone is sent by the terminating fax machine when it answers the call. The additional options include the following:

- CED tone is sent only in the RTP packet payload, according to RFC 2833
- CED tone is sent simultaneously in the RTP packet payload, according to RFC 2833, and voice-band data (VBD) packet bypass.

This feature also provides support for combined V.150.1 modem relay and fax relay. This is configured by setting the CEDTransferMode parameter to 3.

To support this feature, the following optional values have been added to the existing parameter:

[CEDTransferMode]	Determines the fax CED (answering) tone transfer mode. ▪ [0] Fax Relay or VBD = (Default) Device transfers the CED tone in relay mode and starts the fax session immediately. ▪ [1] Voice Mode or VBD = Device transfers the CED tone in either voice or bypass mode and starts the fax session on V21 preamble. ▪ [2] RFC 4733 Blocking RTP VBD = Device transfers the CED tone in RFC 2833. Applicable only to V.150.1 modem relay and fax bypass. ▪ [3] RFC 4733 Along with RTP VBD = Device transfers the CED tone in RFC 2833 and bypass, in parallel. For combined V.150.1 modem relay and fax relay, use this option.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 3000.

3.1.1.96 Dynamic Blacklisting of Malicious Attackers

This feature provides an enhancement to the Intrusion Detection System (IDS) feature, by supporting dynamic blacklisting of remote hosts (IP addresses / ports) considered by the device as malicious. Up until this release, the IDS feature supported only the notification of malicious activity, by sending SNMP alarms.

A host is considered as malicious if it has reached or exceeded a user-defined threshold of malicious attacks (counter). The device automatically blacklists the malicious source for a user-defined period, after which it is removed from the blacklist. When an attacker is added to or removed from the blacklist, the device sends the following new SNMP trap:

Event	acIDSBlacklistNotification
OID	1.3.6.1.4.1.5003.9.10.1.21.2.0.101
Event Type	securityServiceOrMechanismViolation
Probable Cause	thresholdCrossed
Alarm Text	Added IP * to blacklist; Removed IP * from blacklist

This feature also provides the following new IDS-related CLI commands:

- Displays the blacklist:

```
# show voip security ids blacklist active
```

For example:

```
Active blacklist entries:
  10.33.5.110(NI:0) remaining 00h:00m:10s in blacklist
```

Where *SI* is the SIP Interface, and *NI* is the Network interface.

- Displays all active IDS alarms:

```
# show voip security ids active-alarm all
```

For example:

```
IDSMatch#0/IDSRule#1: minor alarm active.
```

- Displays details regarding an active IDS alarm of the specified match and rule IDs:

```
# show voip security ids active-alarm match <Match Rule ID>
rule <IDS Rule ID>
```

For example:

```
# show voip security ids active-alarm match 0 rule 1
IDSMatch#0/IDSRule#1: minor alarm active.
- Scope values crossed while this alarm is active:
    10.33.5.110(SI0)
```

To support this feature, the following two fields have been added to the IDS Rule Table:

Deny Threshold [IDSRule_DenyThreshold]	Defines the threshold that if crossed, the remote host (attacker) is blocked (blacklisted). The default is -1 (i.e., not configured). Note: This parameter is applicable only if the 'Threshold Scope' parameter is set to **IP** or **IP+Port**.
Deny Period [IDSRule_DenyPeriod]	Defines the duration (in sec) to keep the attacker on the blacklist. The valid range is 0 to 1,000,000. The default is -1 (i.e., not configured).

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.97 TLS Versions 1.1 and 1.2 Support

This feature provides support for Version 1.1 and Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides client/server communications security over the Internet. Up until this release, the device supported only TLS Version 1.0.

By default, all TLS versions are allowed. However the TLS version can be restricted using the following existing parameter:

Web/EMS: TLS Version CLI: version [TLSVersion]	Defines the supported versions of Transport Layer Security (TLS) / SSL (Secure Socket Layer). ▪ [0] All SSL and TLS Versions = (Default) SSL 3.0 and all TLS versions (1.0, 1.1, and 1.2) are supported. SSL/TLS handshakes always start with an SSL 2.0-compatible handshake and then switches to the highest TLS version supported by both peers.

	▪ [1] TLS 1.0 Only = only TLS 1.0 is used. Clients attempting to contact the device using any other version are rejected. Notes: ▪ For this parameter to take effect, a device reset is required. ▪ SSL 2.0 is not supported (only supported for handshakes).

Applicable Products: All.

3.1.1.98 Multiple TLS Certificates

This feature provides support for using different TLS certificates for each IP Group (SIP user agent), referred to as a *TLS Context*. Up until this release, the device supported the use of only a single TLS certificate, which served all IP Groups. This feature is applicable to gateway and SBC calls.

Each TLS Context can be configured with the following:

- Context ID and name
- TLS version (SSL3.0, TLS1.0, TLS1.1, TLS1.2)
- Encryption ciphers for server and client (AES, RC4)
- Online Certificate Status Protocol (OCSP) server addresses and ports - device checks whether a peer's certificate has been revoked by this OCSP server
- Private key (uploaded to device)
- Certificate (self-signed certificates or signed as a result of a certificate signing request / CSR)
- Trusted root certificate authority (CA) store (for validating certificates)

The device is shipped with a default TLS Context (ID 0 and string name "default"), which includes a self-generated private key and a self-signed certificate (as in previous releases).This default TLS Context cannot be deleted.

User-defined TLS Contexts are used only for SIP over TLS (SIPS). The default TLS Context (ID 0) can be used for SIPS and all the other supported applications, for example, Web server (HTTPS), Telnet server, and SSH server.

The TLS Context can be assigned to a Proxy Set and/or SIP Interface. When the device establishes a TLS connection (handshake) with a SIP user agent (UA), the TLS Context used by the device is determined as follows:

- Incoming call: If the IP address of the called (source) party is also defined for a Proxy Set (i.e., the UA is successfully classified to Proxy Set / IP Group), the device uses the TLS Context configured for this Proxy Set. If the Proxy Set is not configured with a TLS Context or classification to a Proxy Set fails, the device checks the SIP Interface used for the call. If the SIP Interface is configured with a TLS Context, the device uses it. If the SIP Interface is not configured with a TLS Context or no SIP Interface is used, the default TLS Context (ID 0 and string "default") is used.
- Outgoing calls: The TLS Context is determined by the destination IP Group (i.e., associated Proxy Set). If the Proxy Set is not configured with a TLS Context, the TLS Context is determined according to the SIP Interface used for the call and employs the same logic as used for incoming calls (see above).

TLS Context certification also enables employing different levels of security strength (key size) per certificate. This feature also enables the display of the list of all trusted certificates currently installed on the device. For each certificate, detailed information such as issuer and expiration date is shown. Certificates can be deleted or added from/to the Trusted Root Certificate Store.

If the TLS Context used for an existing TLS connection is changed during the call by the user agent, the device ends the connection.

TLS certificate expiry check (existing feature from previous releases) is configured globally for all TLS Contexts. However, the existing SNMP trap event,

acCertificateExpiryNotification which is sent to indicate that a certificate is soon to expire, has been enhanced to indicate the TLS Context to which the certificate belongs.

The maximum number of TLS Contexts that can be configured based on product:

- Mediant 5xx, Mediant 8xx: 12
- Mediant 1000B: 15
- Mediant 3000: 20
- Mediant 2600/4000: 400
- Mediant 9000, Mediant SW: 1,000

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

Web: TLS Contexts [TLSContexts]	[TLSContexts] FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion, TLSContexts_ServerCipherString, TLSContexts_ClientCipherString, TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary, TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort, TLSContexts_OcspDefaultResponse; [\TLSContexts]
Proxy Set Table	New field added: TLS Context Name [ProxySet_TLSContext] = Assigns a TLS Context to the specific proxy Set. By default, no TLS Context is assigned and the TLS Context is determined by the SIP Interface to which the call belongs.
SIP Interface Table	New field added: TLS Context Name [SIPInterface_TLSContext] = Assigns a TLS Context to the specific SIP Interface. By default, no TLS Context is assigned. .
CLI: configure system > tls #	Configures the TLS Contexts table. The following command deletes the TLS Context entry from the table: `Configure system > no tls #`

CLI: show system tls contexts	Displays configured TLS Contexts.
	`# show system tls contexts`
	`Context #  Name`
	`--------  --------------------------`
	`0  default`
	`2  itsp-a`
	`Total 2 active contexts.`
	`Total certificate file size: 4208 bytes`

CLI: configure system > tls # > certificate status	Displays the status of the certificate belonging to the specified TLS Context.
	`(tls-2)# certificate status`
	`Security context #2 - user2`
	`Certificate subject: /CN=jon/O=AudioCodes/L=Lod/C=ZA`
	`Certificate issuer : /CN=jon/O=AudioCodes/L=Lod/C=ZA`
	`Time to expiration : 7299 days`
	`Key size: 512 bits`
	`Active sockets: 0`
	`The currently-loaded private key matches this certificate.`

CLI: configure system > tls # > certificate detail	Displays details of the certificate belonging to the specified TLS Context.
	`(tls-2)# certificate detail`
	`Certificate:`
	`Data:`
	`Version: 1 (0x0)`

	Serial Number: 0 (0x0) Signature Algorithm: sha1WithRSAEncryption Issuer: CN=jon, O=AudioCodes, L=Lod, C=ZA Validity Not Before: Aug 26 09:01:36 2013 GMT Not After : Aug 21 12:01:36 2033 GMT Subject: CN=jon, O=AudioCodes, L=Lod, C=Za ...
CLI: configure system > tls # > certificate import | export	▪ import: Imports a new certificate for the specified TLS Context, which replaces the previous certificate. ▪ export: Saves a certificate
CLI: configure system > tls # > private-key generate 512	Generates a new private key.
CLI: configure system > tls # > trusted-root summary	Displays a summary of all certificates available in the Trusted Root Store belonging to the specific TLS Context. tls-2)# trusted-root summary 63 trusted certificates. Num Subject Issuer Expires --- 1 Xcert EZ by DST Xcert EZ by DST 7/11/2009 2 wireless wireless 6/06/2010 3 VeriSign, Inc. VeriSign, Inc. 5/18/2018 …
CLI: configure system > tls # > trusted-root detail #	Displays details of the trusted root certificate belonging to the specified TLS Context. (tls-2)# trusted-root detail 1 Certificate: Data: Version: 3 (0x2) Serial Number: d0:1e:40:90:00:00:27:4b:00:00:00:01:00:00:00:04 Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, ST=Utah, L=Salt Lake City, O=Xcert EZ by DST, CN=Xcert EZ by DST/emailAddress=ca@digsigtrust.com Validity Not Before: Jul 14 16:14:18 1999 GMT Not After : Jul 11 16:14:18 2009 GMT Subject: C=US, ST=Utah, L=Salt Lake City, O=Xcert EZ by DST, CN=Xcert EZ by DST/emailAddress=ca@digsigtrust.com Subject Public Key Info: ...
CLI: configure system > tls # > private-key import	Imports a new private key for the specified TLS Context, which replaces the previous private key.
CLI: configure system > tls # > trusted-root import | export | delete #	▪ import: Imports a certificate from the Trusted Store ▪ export: Exports a certificate from the Trusted Store ▪ delete: Removes a certificate from the Trusted Store

Applicable Products: All.

3.1.1.99 Secure LDAP Connection using TLS

This feature provides secure device communication with an LDAP server, using TLS. Up until this release, connectivity with the Active Directory (AD) server using LDAP could only be over TCP. This is relevant for LDAP-based login management (username-password) and LDAP-based SIP routing.

By default, the device sends the username and password in plaintext when establishing a connection with the LDAP server. This new feature enables the use of TLS (recommended) for securing the connection and encrypting the username and password.

To support this feature, the following new parameter has been added to the LDAP Configuration table:

LDAP Configuration Table	New field: ▪ [LdapConfiguration_useTLS] Use SSL: Encrypts username and password using TLS when sent to LDAP server. ✓ [0] No (Default) ✓ [1] Yes

Applicable Products: All.

3.1.1.100 LDAP-based Management User Login Authentication

This feature provides support for authentication and authorization of the device's management users (Web and CLI) through an LDAP-compliant server such as Microsoft Active Directory (AD). When a user attempts to log in to one of the management platforms, the device verifies the login username and password with AD. The device can also determine the user's management access level (privileges) based on the user's profile in the AD. The device can process up to 15 concurrent users for LDAP-based login authentication.

To enable LDAP-based user login authentication and authorization, a new stand-alone parameter has been added–Use LDAP for Web/Telnet (LoginMgmtLDAPLogin).

The LDAP server is configured using the new LDAP Configuration table which is also used for AD-based SIP routing and manipulation (see Section 3.1.1.40 on page 45). To support LDAP-based login authentication, a new parameter–Type–has been added to the table to determine whether the LDAP server is for SIP-related queries or management login authentication-related queries.

When the device connects to the LDAP server (i.e., an LDAP session is created), the LDAP BIND operation establishes the authentication of the user based on username and password, which is sent in plaintext or encrypted using TLS, configured by the new parameter, Use SSL in the LDAP Configuration table. The server typically checks the password against the userPassword attribute in the named entry. A successful BIND operation indicates that the username-password combination is correct. The established LDAP session may be used for further LDAP queries such as determining the user's access level (also known as authorization). A failed BIND operation indicates that the username-password combination is incorrect.

The configuration of the existing LDAP Bind DN (login username) and LDAP Password (login password) fields are based on a template using the $ (dollar) wildcard. This allows the device to automatically replace the $ sign with the username and password values entered by the user when logging in.

Once the LDAP session is established (in the authentication stage above), the device performs an LDAP search configured to match the specific LDAP server data structure:

- baseObject - configured by the existing LDAP Server Search Base DN table
- filter - configured by the new LDAP Authentication Filter parameter. This is used for the login username and is also based on the $-sign template, whereby the entered username is automatically filled in, e.g., "(sAMAcountName=$)"
- attributes - configured by the new Management Attribute parameter in the LDAP Configuration table

For example:

```
baseObject = "ou=ABC,dc=corp,dc=abc,dc=com"
filter = "(&(objectClass=person)(sAMAccountName=alexa))"
attributes = "memberOf"
```

The LDAP response includes all the groups to which the specific user is a member, for example:

```
CN=\# Support Dept,OU=R&D
Groups,OU=Groups,OU=APC,OU=Japan,OU=ABC,DC=corp,DC=abc,DC=com
```

```
CN=\#AllCellular,OU=Groups,OU=APC,OU=Japan,OU=ABC,DC=corp,DC=abc,D
C=com
```

The device searches the AD for specified group names in order to determine the user's access level (Operator, Admin, and Security Admin). The group names and their corresponding access levels are configured in a new table–Management LDAP Groups Table–which is a "child" of the LDAP Configuration table. Each access level can be configured with multiple group names, separated by a semicolon (;). If the device finds a group name, it assigns the user the corresponding access level and permits login; otherwise, login is denied. Once the LDAP response has been received (success or failure), the LDAP session terminates. Note that when the same LDAP server is used for both management user authentication and SIP applications, different LDAP sessions need to be established for each application.

The device can also be configured to authenticate users based on its local user database, using the new parameter, MgmtLocalDatabaseBehavior. Depending on the parameter's settings, the device can either use the database when an LDAP server is not configured (or as fallback if the server is inaccessible), or to use the database first, and only if the user is not found, to authenticate using the LDAP server.

The following existing features for RADIUS-based login now also apply to LDAP-based login authentication:

- If the LDAP server's responses does not contain the access level attribute, a default access level can be configured which is applied to all authenticated users (Default Access Level).
- If connection with the LDAP server fails due to a timeout, the device can be configured to either deny access or verify the user's credentials (username/password) locally in the device's user database (Behavior upon Authentication Server Timeout).

As a result of this new feature, the RADIUS Settings page has been renamed "Authentication Settings" and includes parameters for LDAP-based user authentication, RADIUS-based user authentication, and those shared between the two.

Web: Use LDAP for Web/Telnet Login CLI: configure voip > ldap > enable-mgmt-login [LoginMgmtLDAPLogin]	Enables LDAP-based management user login authentication and authorization. ▪ [0] Disable (default) ▪ [1] Enable Note: For this parameter to take effect, a device reset is required.
LDAP Configuration Table Type	New fields: ▪ Type [LdapConfiguration_Type]: Defines whether the LDAP server is used for SIP-related queries or management login authentication-related queries. ✓ [0] Control (Default) ✓ [1] Management ▪ Management Attribute [LdapConfiguration_MngmAuthAtt]: Defines the attribute to search in the AD. ▪ Use SSL: Enables encrypting username and password using TLS when sent to LDAP server. ✓ [0] No (Default) ✓ [1] Yes
Web: LDAP Authentication Filter CLI: configure voip > ldap > auth-filter [LDAPAuthFilter]	Defines the LDAP search filter attribute for searching the login username for user authentication. You can use the dollar ($) sign to represent the username. For example, if this parameter is set to (sAMAcountName=$) and the user enters "SueM" as the username, the LDAP search is done on sAMAcountName=SueM.
Web: Use Local Users Database CLI: configure system >	Defines when the device uses its local user database for LDAP- or RADIUS-based login authentication. ▪ [0] When No Auth Server Defined = (Default) When no

mgmt-auth > use-local-users-db [MgmtLocalDatabaseBehavior]	LDAP/RADIUS server is configured (or as fallback if the server is inaccessible). ▪ [1] Always = Always verify user's credentials using local user database first, and only if not found, search LDAP/RADIUS server. In other words, the local database has precedence over the server.
Web: Behavior upon Authentication Server Timeout CLI: configure system > mgmt-auth > timeout-behavior [MgmtBehaviorOnTimeout]	Defines the mode of operation regarding user login authentication if connection with the LDAP server fails (due to a timeout, temporary network malfunction or AD server problem). ▪ [0] Deny Access ▪ [1] Verify Access Locally = (Default) Device verifies the user's credentials (username/password) locally in its user database and grants access if correct; otherwise, it denies access. Note: This parameter replaces the BehaviorUponRadiusTimeout parameter.
Web: Management LDAP Groups Table [MgmntLDAPGroups]	Defines the users group in the AD and corresponding management access level. [MgmntLDAPGroups] FORMAT MgmntLDAPGroups_Index = MgmntLDAPGroups_LdapConfigurationIndex, MgmntLDAPGroups_GroupIndex, MgmntLDAPGroups_Level, MgmntLDAPGroups_Group; [\MgmntLDAPGroups] Where MgmntLDAPGroups_Level: ▪ [0] Monitor ▪ [1] Security Administrator ▪ [2] Administrator

Applicable Products: All.

3.1.1.101 FXO Pulse Dialing Generation

This feature provides support for generating pulse (rotary) dialing from analog FXO equipment (e.g., legacy PBX) connected to the device's FXO port interfaces. The feature can be required, for example, for Business to Government (B2G) environments in which the primary signaling method to the central office (CO) is pulse dialing rather than DTMF (touch-tone) using push-button telephones.

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

[EnablePulseDialGeneration]	Enables pulse dialing generation to the analog side when dialing is received from the FXO side. ▪ [0] Disable = (Default) Device generates DTMF signals. ▪ [1] Enable = Generates pulse dialing. Note: For this parameter to take effect, a device reset is required.
[PulseDialGenerationBreakTime]	Defines the duration of the Break connection (off-hook) for FXO pulse dial generation. The valid value range is 20 to 120 (in msec). The default is 60. Note: For this parameter to take effect, a device reset is required.
[PulseDialGenerationMakeTime]	Defines the duration of the Make connection (on-hook) for FXO pulse dial generation. The valid value range is 20 to 120 (in msec). The default is 40. Note: For this parameter to take effect, a device reset is required.
[PulseDialGenerationInterDig	Defines the inter-digit duration (time between consecutively

itTime]	dialed digits) for FXO pulse dial generation. The valid value range is 300 to 1500 (in msec). The default is 700. Note: For this parameter to take effect, a device reset is required.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B.

3.1.1.102 FXS Pulse Dialing Detection

This feature provides support for detecting pulse (rotary) dialing from analog equipment (e.g., telephones) connected to the device's FXS port interfaces.

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

[EnablePulseDialDetection]	Enables pulse dialing detection. ▪ [0] Disable (default) ▪ [1] Enable Note: For this parameter to take effect, a device reset is required.

Applicable Products: Mediant 1000B.

3.1.1.103 Multiple Line Extensions per FXS Interface

This feature provides support for multi-line configuration of FXS ports. Multiple line extension numbers can be configured per FXS interface (port/module). For each line extension, a username and password for registration and authentication can be configured, as well as caller ID.

To support this feature, the former ISDN Supplementary Services table used for BRI interfaces has been enhanced to also support FXS interfaces. The name of this table has been changed to Supplementary Services table.

This table can also be used for routing IP-to-Tel calls to specific FXS channels (or BRI channels) based on the called line-extension number. To enable this functionality, the 'Channel Select Mode' in the Trunk Group Settings table must be set to Select Trunk by Supplementary Services Table for the Trunk Group ID to which the FXS port belongs.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B.

3.1.1.104 INVITE upon Constant Ringing on FXO Interfaces

This feature provides support for configuring a delay time before the FXO initiates a call to the IP side upon detection of a RING_START event from the Tel side. This occurs instead of waiting for a RING_END event. Until this release, the FXO interface would only send an INVITE upon receipt of the RING_END event.

This feature is useful for telephony services that employ constant ringing (i.e., no RING_END is sent). For example, Ringdown circuit is a service that sends a constant ringing current over the line, instead of cadence-based 2 second on, 4 second off. For example, when a telephone goes off-hook, a phone at the other end instantly rings.

If a RING_END event is received before the timeout expires, the device does not initiate a call and ignores the detected ring. Any RING_END event detected after the timeout expires is ignored by the device.

This feature can be applied per port, using Tel Profiles.

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

FXO Ring Timeout CLI: fxo-ring-timeout [FXORingTimeout]	Defines the delay for generating a SIP INVITE to the IP side upon detection of a RING_START from the Tel (FXO) side. The valid value range is 0 to 50 (msec), in steps of 100-msec. For example, a value of 50 represents 5 sec. The default value

	is 0 (i.e., standard ring operation).
Tel profile table: FXO Ring Timeout [TelProfile_FXORingTimeout]	Same as global parameter above, but per Tel Profile (per port) Note: If this parameter is configured for a specific FXO port, Caller ID detection does not occur, and the RingBeforeCallerID and FXONumberOfRings parameters do not affect the outgoing INVITE for that FXO port.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B.

3.1.1.105 Double Wink-Start Signaling for FXO Interfaces

This feature provides support for double wink-start signaling for FXO interfaces for IP-to-Tel calls. Up until this release, double wink-start signaling was supported only for FXS interfaces. Wink-start signaling is used for Direct Inward Dialing (DID), typically for signaling between an E-911 switch and the PSAP.

The FXO double wink-start signaling process is as follows:

1. Upon incoming INVITE message, the FXO interface goes off-hook (seizes the line).
2. Upon detection of a Wink signal from the Tel side (instead of a dial tone), the FXO interface dials the digits, "KP911ST" (denotes *911#).
3. The FXO interface waits for polarity reversal change from normal to reverse for an interval of 2,000 msec.
4. Upon detection of a polarity reversal change, the FXO interface dials the DTMF (or MF) digits of the calling party (number that dialed 911) in the format "KP<ANI>ST" (*ANI#), where ANI is the calling number from the INVITE. If no polarity reversal, the FXO goes idle.

For example: (Wink) KP911ST (Polarity Change) KP02963700ST

To enable this feature, the following existing parameters must be configured:

- Enable911PSAP must be set to 1.
- DID Wink (EnableDIDWink) must be set to Wink & Polarity [3].

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B.

3.1.1.106 Ground-Start or Loop-Start Signaling per FXS/FXO Port

This feature provides support for configuring ground-start or loop-start signaling per analog (FXS and FXO) port. Up until this release, ground-start or loop-start signaling could only be applied per device (i.e., all analog modules), using the GroundKeyDetection parameter.

To support this feature, the following new table has been added (VoIP > Media > Port Ground Start Table):

Web: Port Ground Start [GroundKeyDetection_x]	Enables ground-key detection (ground-start signaling) per analog (FXS or FXO) port. When disabled, the device uses loop-start signaling. ▪ [0] Disable = (Default) Port uses loop-start signaling. ▪ [1] Enable = Port uses ground-start signaling. Notes: ▪ For this parameter to take effect, a device reset is required. ▪ For the ini file parameter, the x denotes the port number, where 0 represents Port I. ▪ For ground-start signaling, ensure that the FXO G module is installed (and not the regular FXO module) in the device's chassis. ▪ To support FXO ground-start signaling, set the following: EnableCurrentDisconnect parameter to 1 and the FXOBetweenRingTime parameter to 300. ▪ FXS ground-start interface does not generate a ringing voltage. The FXS interface initiates the signaling by

	grounding the TIP lead.

Applicable Products: Mediant 1000B.

3.1.1.107 Configurable Analog Port Name in ini File

This feature provides support for configuring an arbitrary name for each analog (FXS/FXO) port on the device, in the ini file. Up until this release, a port name could only be configured in the Web interface (on the Home page).

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

[AnalogPortInfo_x]	Defines an arbitrary name to easily identify the analog port. The valid value is a string of up to 40 characters. By default, the value is undefined. Note: For the ini file parameter, the *x* denotes the port number.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B.

3.1.1.108 Disabling Analog Ports

This feature provides support for disabling an analog port (FXS or FXO). When disabled, the port cannot be used and no signaling is transmitted through the port. By default, all the analog ports are enabled.

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

```
(config-voip)# interface fxs-fxo
(fxs-fxo)# analog-port-enable <module>/<port> [on|off]
Where
```

- *module* is the module number
- *port* is the port number

For example, to disable port 2 on module 1:

```
(fxs-fxo)# analog-port-enable 1/2 off
```

Applicable Products: Mediant 500/L MSBR; Mediant 8xx.

3.1.1.109 User-defined Tone Played for ISDN Q.931 Release Cause Codes

This feature provides support for playing a user-defined pre-recorded tone (PRT) to the Tel side from a PRT file for specific ISDN Q.931 release cause codes. The release cause code indicates to the Tel side the reason for the call release (e.g., busy) by the IP side.

A new parameter (see below) has been introduced that specifies the release code(s). The tone played to the Tel side for the specified release code(s) is configured when creating the PRT file using AudioCodes DConvert utility. The tone must be assigned to the "acSpecialConditionTone" (Tone Type 21) option in DConvert. The PRT file must be installed on the device.

If the SIP release reason received from the IP side is mapped to the Q.931 release code specified in the parameter, then the device plays the user-defined tone. Otherwise, if not specified and the release code is 17 (User Busy), the device plays the busy tone and for all other release codes, the device plays the reorder tone.

Note: To enable this feature, the existing 'Play Busy Tone to Tel' (PlayBusyTone2ISDN) parameter must be enabled (set to 1 or 2).

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

CLI: configure voip > gw digitalgw digital-gw-parameters > q850-reason-code-2play-user-tone [Q850ReasonCode2PlayUse	Defines the ISDN Q.8931 release cause codes that if received, play the specified tone from the PRT file. The parameter can be configured with up to 10 release codes. When configuring multiple codes, use commas (without spaces) to separate them. For example: Q850ReasonCode2PlayUserTone = 1,18,24

rTone]	Note: If the release code 17 (User Busy) is not specified in this parameter, the device plays the busy tone. For all other release codes not specified, the device plays the reorder tone.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.110 ISDN BRI Terminal Endpoint Identifier (TEI) Configuration

This feature provides enhanced support for configuring terminal endpoint identifier (TEI) management for the BRI port interfaces. TEI is part of Layer 2 (OSI). The new configuration can be done per BRI interface or for all BRI interfaces, which can be Network or User side and in point-to-point (P2P) or point-to-multipoint (P2MP) service mode.

Note: The new configuration replaces the previous configuration requirement to use the NS_EXPLICIT_INTERFACE_ID bit for the 'Q931 Layer Response Behavior' parameter (ISDNIBehavior). If this parameter has been used to configure BRI interfaces, it must be set to 0 and the new parameters used instead.

To support this feature, the following new parameters have been added. (The CLI parameters are located under config-voice > interface bri module/port.)

CLI: tei-config-p2p [BriTEIConfigP2P_x]	Defines the BRI terminal endpoint identifier (TEI) when in point-to-point (P2P) mode. The valid value is 0 to 63, 127. The default is 0. ▪ Network Side: ✓ 0-63: Static TEI is accepted. ✓ 127: Any possible TEI is accepted. Dynamic TEI allocation is supported. ▪ User Side: ✓ 0-63: Static TEI is used. ✓ 127: Dynamic TEI allocation is supported (TEI request procedure initiated). Note: The value 127 replaces the previous configuration requirement to set the ISDNIBehavior parameter to NS EXPLICIT INTERFACE ID (1).
CLI: tei-config-p2mp [BriTEIConfigP2MP_x]	Defines the BRI TEI when in point-to-multipoint (P2MP) mode. The valid value is 0 to 63, 127. The default is 127. ▪ Network Side: Not applicable - In network side in P2MP configuration, any TEI must be accepted. ▪ User Side: ✓ 0-63: Static TEI is used. ✓ 127: Dynamic TEI allocation is supported (TEI request procedure initiated).
CLI: tei-assign-trigger [BriTEIAssignTrigger_x]	Defines when to start the TEI assignment procedure. The valid values are (bit-field parameter): ▪ Bit#0: LAYER1_ACTIVATION ▪ Bit#1: BRI_PORT_CONFIG ▪ Bit#2: CALL_ESTABLISH The default is 0x02. This parameter is applicable only to the User side (for Dynamic TEI).
CLI: tei-remove-trigger [BriTEIRemoveTrigger_x]	Defines the following: ▪ Network Side: When to "forget" all existing TEIs and wait for the User side to start a new TEI assignment procedure. This is also applicable to static TEI. ▪ User Side: When to start a new TEI assignment verification procedure. The valid values are (bit-field parameter):

	▪ Bit#0: LAYER1_DEACTIVATION ▪ Bit#1: BRI_DL_RELEASED ▪ Bit#2: TEI_0_P2MP_NET_SIDE The default is 0x00.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B.

3.1.1.111 Configurable Trunk Name

This feature provides support for configuring an arbitrary name for each trunk on the device. This is relevant for ISDN BRI and PRI trunks.

To support this feature, the following new parameter has been added to the existing Trunk Settings page:

Web: Trunk Name CLI: name (config-voip > interface <e1|t1|bri> name [DigitalPortInfo_x]	Defines an arbitrary name to easily identify the trunk. The valid value is a string of up to 40 characters. By default, the value is undefined. Note: For the ini file parameter, the *x* denotes the trunk number.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.112 Collect Call Detection in Reverse Charging Indication IE of ISDN Setup

This feature provides support for detecting collect calls using the Reverse Charging Indication information element (IE) received in the Q.931 ISDN Setup message, for Tel-to-IP calls. This is applicable to the Euro ISDN protocol variant. Up until this release, the device could only detect collect calls in the Facility IE of the Setup message. Now, both methods are supported (does not require any special configuration). As in previous releases, when the device detects a collect call, it adds a proprietary header to the outgoing SIP INVITE message (X-Siemens-Call-Type: collect call).

Applicable Products: Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.113 Manual Switchover of D-Channels in CLI

This feature provides support for initiating a manual switchover between D-channels (primary and backup) pertaining to the same NFAS group, in the CLI. Up until this release, this could only be performed on the other management tools such as the Web interface.

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

```
# pstn nfas-group-switch-activity [1-12]
```

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B.

3.1.1.114 Interworking SIP MWI NOTIFY Message to NI-2 ISDN Facility

This feature provides support for interworking SIP Message Waiting Indication (MWI) NOTIFY messages to ISDN PRI NI-2 Message Waiting Notification (MWN) sent in the ISDN Facility IE message. This feature is used for voicemail applications when the device is connected to a PBX through an ISDN PRI trunk configured to NI-2.

To support this feature, a new option, [9] has been added for NI-2 to the existing parameter, VoiceMailInterface:

Web: Voice Mail Interface CLI: vm-interface [VoiceMailInterface]	▪ [9] = ISDN PRI trunks set to NI-2.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.115 SIP-PSTN Mapping of CPC for MFC-R2 Variant Argentina

This feature provides support for SIP-PSTN mapping of the calling party category (CPC) for the MFC-R2 variant Argentina. Up until this release, the device supported CPC mapping of the MFC-R2 variant Brazil. The CPC characterizes the station used to originate a call (e.g., a payphone or an operator).

CPC mapping is supported in both call directions–IP to Tel and Tel to IP. The CPC in the SIP INVITE message is denoted by the 'cpc' parameter in the From or P-Asserted-Identity headers. For example,

```
INVITE sip:bob@biloxi.example.com SIP/2.0
To: "Bob" <sip:bob@biloxi.example.com>
From: <tel:+17005554141;cpc=payphone>;tag=1928301774
```

On the PSTN side, the CPC is denoted as ANI II digits in MFRC-R2 (or in the Originating Line Information / OLI Information Element of the ISDN Setup message for NI-2 ISDN PRI).

SIP CPC	MFC-R2	
	Argentina	**Brazil**
ordinary	II-1	II-1
priority	II-2	II-2
data	II-6	II-6
test	II-3	II-3
operator	II-5	II-5
payphone	II-4	II-7
unknown	II-1	II-1
subscriber	n/a	II-1
cellular	II-13	n/a
locutorio	II-11	n/a
servicio-publico	II-12	n/a
red-privada-virtual	II-14	n/a
linea-especial	II-15	n/a
operadora-con-intervencion	II-5	n/a

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

Web: Calling Party Category Mode CLI: cpc-mode [CallingPartyCategoryMode]	Defines the regional CPC mapping requirement for mapping between SIP and the PSTN. ▪ [0] None (default) ▪ [1] Brazil R2 ▪ [2] Argentina R2 **Notes:** ▪ To enable CPC mapping, set the EnableCallingPartyCategory parameter to 1. ▪ This parameter is applicable only to the E1 MFC-R2 variant.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.116 Timeout for ISDN Release Message before Releasing Channel

This feature provides support for configuring a timeout (in milliseconds) that the device waits for the receipt of an ISDN Q.931 Release message from the PSTN side before releasing the channel. The Release ACK is typically sent by the PSTN in response to the

device's Disconnect message to end the call. If the timeout expires and a Release ACK has not yet been received, the device releases the call channel.

This feature is applicable to digital PSTN.

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

Web: Wait before PSTN Release-Ack CLI: wait-befor-pstn-rel-ack [TimeToWaitForPstnReleaseAck]	Defines the timeout (in milliseconds) to wait for the release ACK from the PSTN before releasing the channel. The valid value is 1 to 360,000. The default is 6,000.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.117 Lock/Unlock per Trunk Group

This feature provides support for locking and unlocking a specific Trunk Group. When the user initiates the lock process, the device rejects all new incoming calls for the Trunk Group and immediately terminates active calls (busy channels), eventually taking the entire Trunk Group out of service. The Trunk Group can also be "gracefully" locked, whereby the device also rejects new incoming calls, but terminates busy channels only after a user-defined graceful period if the channel is still busy by the end of the period. The graceful period is configured by the existing GracefulBusyOutTimeout parameter (when configured to 0, graceful lock is disabled). When a Trunk Group is locked, the method for taking trunks/channels out-of-service is determined by the DigitalOOSBehaviorForTrunk parameter for per trunk or DigitalOOSBehavior parameter for all trunks.

To support the feature, the Lock and Unlock commands have been added to the Action drop-down list button in the Trunk Group Settings table (Configuration tab > VoIP > GW and IP to IP > Trunk Group > Trunk Group Settings). In addition, the table provides two new read-only fields:

- Admin State: Displays the administrators state – "Locked" or "Unlocked"
- Status: Displays the current status of the channels in the Trunk Group – "In Service", "Going Out Of Service", "Going Out Of Service (<time remaining of graceful period> sec / <number of calls still active> calls)", "Out Of Service"

Notes:

- If the device is reset, a locked Trunk Group remains locked. If the device is reset while graceful lock is in progress, the Trunk Group is forced to lock immediately after the device finishes its reset.
- Devices in High Availability (HA) mode:
  - After an HA switchover, a locked Trunk Group remains locked.
  - If an HA switchover is initiated while a Trunk Group is in locking progress, the locking process is stopped and only starts again (with the configured graceful period) once switchover completes.
  - When HA status is in "Synchronizing" state, the Trunk Group status is not updated in the Trunk Group Settings table. In addition, the lock/unlock actions cannot be invoked during this time. When HA synchronization finishes and HA status is in "Operational" state, the Trunk Group Settings table is refreshed with the lock/unlock status. The HA state is displayed on the Home page.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.118 New Out-of-Service Mode

This feature provides support for a new out-of-service mode that affects ISDN Service messages and the D-channel, which is configured by the existing parameters, DigitalOOSBehavior (global) and DigitalOOSBehaviorForTrunk (per trunk). A new optional value has been added to these parameters - Service and D-Channel [5]. For more information, refer to these parameters in the *User's Manual*.

Applicable Products: Mediant 500 MSBR; Mediant 500 SBC; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.119 High Availability 1+1 System Redundancy Support

This feature provides support for high availability (HA) 1+1 system redundancy by the Mediant 500 E-SBC and Mediant 800B Gateway & E-SBC (not Mediant 800 Gateway & E-SBC – previous hardware platform). Up until this release, HA was supported only by the Mediant 3000, Mediant 4000, Mediant 2600, and Mediant Software SBC.

HA provides full system redundancy, whereby if a failure occurs in the active device, a switchover occurs to the redundant device to take over the call handling processes. Thus, the continuity of call services is ensured. All active calls (signaling and media) are maintained upon switchover.

To support this feature, the following HA parameters are now supported:

- Maintenance interface configuration used for communication between the two devices
- HA configuration parameters in the HA Settings page

Notes:

- Currently, HA is supported only for IP calls. During a switchover upon failure of the active unit, PSTN calls (FXS, FXO, BRI, and E1/T1) are dropped (using a SIP BYE message).
- After switchover, it is recommended to connect the redundant device to the same PSTN equipment to which the primary device was connected (using identical ports). This includes, for example, FXS telephones and E1/T1 cable. This allows the use of Tel-IP call routing rules, which is already configured on the redundant device (copied configuration).
- For HA support, the device's installed Software License Key must include the HA Feature Key.

Applicable Products: Mediant 500 E-SBC; Mediant 800B Gateway & E-SBC.

3.1.1.120 Monitoring IP Entity and HA Switchover upon Ping Failure

This feature provides support for monitoring the connectivity integrity of a network entity for the applicable products listed below. This is achieved by sending a ping and performing a switchover to the redundant device if no ping response is received. Up until this release, this feature was supported only by Mediant 4000.

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 ping is sent from one of the device's IP network interfaces. 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 parameters are made available for Mediant 800 Gateway & E-SBC and Mediant Software SBC:

- Enable HA Network reachability (HAPingEnabled)
- HA Network reachability destination address (HAPingDestination)
- HA Network reachability source If name (HAPingSourceIfName)
- HA Network reachability ping timeout (HAPingTimeout)
- HA Network reachability ping retries (HAPingRetries)

Applicable Products: Mediant 500 E-SBC; Mediant 800B Gateway & E-SBC; Mediant 2600; Mediant 9000; Mediant SW.

3.1.1.121 High Availability Configuration in CLI

This feature provides support for configuring the High Availability feature in the CLI. Up until this release, HA could only be configured using the Web interface.

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

- Configuration commands under (config-system)# high-availability:
  - Sets ping destination address:
    ```
    (ha)# net-mon-destination
    ```
  - Enables network monitor:
    ```
    (ha)# net-mon-enable
    ```
  - Sets ping retries value:
    ```
    (ha)# net-mon-ping-retries
    ```
  - Sets ping timeout value:
    ```
    (ha)# net-mon-ping-timeout
    ```
  - Sets source interface name:
    ```
    (ha)# net-mon-source-interface
    ```
  - Sets the HA priority of the unit:
    ```
    (ha)# priority
    ```
  - Sets the HA priority of the redundant unit:
    ```
    (ha)# redundant-priority
    ```
  - Sets the unit ID name of the redundant unit:
    ```
    (ha)# redundant-unit-id-name
    ```
  - Sets Maintenance address of other HA unit:
    ```
    (ha)# remote-address
    ```
  - Enables HA priority mechanism:
    ```
    (ha)# revertive-mode
    ```
  - Sets the unit ID name:
    ```
    (ha)# unit-id-name
    ```
  - Switchover to Redundant device (under enable mode):
    ```
    # ha manual-switch-over
    ```
  - Reset redundant device (under enable mode):
    ```
    # ha reset-redundant-unit
    ```
- Displayed information (under root mode):
  - Display HA status:
    ```
    # show system high-availability status
    ```
  - Display HA network monitor status:
    ```
    # show system high-availability network-monitor-status
    ```
- Debug HA commands (under enable mode):
  - HA debug information:
    ```
    # debug ha
    ```
  - Clears HA debug counters (keep-alive packets sent between active and redundant devices):
    ```
    # debug ha clear-counters
    ```

Applicable Products: Mediant 500 E-SBC; Mediant 800B Gateway & E-SBC; Mediant Non-Hybrid SBC.

3.1.1.122 Hitless Software Upgrade Configuration in CLI

This feature provides support for initiating a Hitless Software upgrade procedure in the CLI. Up until this release, Hitless Software upgrade could only be done in the Web interface.

Hitless Software Upgrade is used to upgrade devices in High Availability (HA) mode without affecting traffic (i.e., current calls). It does this by 1) first upgrading the redundant device, 2) performing a switchover from the active device to the redundant device, 3) upgrading the previously active device, and then 4) switching over again to the previously active device.

The alternative to Hitless Software Upgrade is the non-Hitless method, whereby both the active and redundant devices are upgraded at the same time. Thus, this method is traffic-affecting and terminates current calls.

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

- Hitless Software Upgrade:

```
# copy firmware from <URL and file name>
```

  For example:

```
# copy firmware from https://1.1.1.1/device_SIP_F6.80A.cmp
```

- Non-Hitless Software Upgrade:

```
# copy firmware from <URL and file name> non-hitless
```

Applicable Products: Mediant 500 E-SBC; Mediant 800B Gateway & E-SBC; Mediant Non-Hybrid SBC.

3.1.1.123 Quality of Experience Profile

This feature provides an enhancement to the device's monitoring of call quality. Profiles of call quality, which define thresholds for MOS, jitter, delay and call color, can now be configured in a dedicated Quality of Experience (QoE) Profile table and associated with IP Groups, Media Realms, and Remote Media Subnets.

QoE Profiles are used for the following:

- Reporting QoE metrics to AudioCodes' Session Experience Manager (SEM)
- Access control and media enhancements based on QoE metrics
- Alternative routing based on QoE metrics

SEM uses QoE Profiles to define different call quality thresholds for different SEM links (when the latter is mapped to an IP Group, Media Realm, or Remote Media Subnet).

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

Web: Quality of Experience Profile CLI: qoe-profile [QOEProfile]	Defines QoE profiles, where each profile is configured with a name and either pre-configured or user-defined QoE parameter thresholds. For configuring user-defined thresholds, use the Quality of Experience Color Rules table. [QOEProfile] FORMAT QOEProfile_Index = QOEProfile_Name, QOEProfile_SensitivityLevel; [\QOEProfile] ▪ Index = Table index row. ▪ Profile Name = Arbitrary descriptive name. ▪ Sensitivity Level: ✓ Low = Pre-configured low sensitivity thresholds ✓ Medium = Pre-configured medium sensitivity thresholds ✓ High = Pre-configured high sensitivity thresholds ✓ User Defined = Need to define thresholds per monitored parameter in Quality of Experience Color Rules table
Quality of Experience Color Rules CLI: qoe-rules [QOEColorRules]	Defines thresholds for the QoE parameters. This table is a subset of the Quality of Experience Profile table. For each QoE parameter, thresholds can be configured for the remote side or for the device side. [QOEColorRules] FORMAT QOEColorRules_Index = QOEColorRules_QoeProfile, QOEColorRules_ColorRuleIndex, QOEColorRules_monitoredParam, QOEColorRules_direction, QOEColorRules_profile, QOEColorRules_GreenYellowThreshold,

	QOEColorRules_GreenYellowHysteresis, QOEColorRules_YellowRedThreshold, QOEColorRules_YellowRedHysteresis; [\QOEColorRules] ▪ Monitored Parameter: ✓ MOS ✓ Delay ✓ Packet Loss ✓ Jitter ✓ RERL (Echo) ▪ Direction = Defines monitoring direction: ✓ Device Side ✓ Remote Side ▪ Sensitivity Level: ✓ User Defined = Need to define thresholds ✓ Low Sensitivity = Pre-configured low thresholds ✓ Average Sensitivity = Pre-configured average thresholds ✓ High Sensitivity = Pre-configured high thresholds ▪ Green Yellow Threshold = Defines the parameter's threshold values between green (good quality) and yellow (medium quality) states. ▪ Green Yellow Hysteresis = Defines the hysteresis (fluctuation) for the green-yellow threshold at which the threshold is considered crossed. When the threshold exceeds this hysteresis value, the device reports this call state change to the SEM. ▪ Yellow Red Threshold = Defines the parameter threshold values between yellow (medium quality) and red (poor quality). ▪ Yellow Red Hysteresis = Defines the hysteresis (fluctuation) for the yellow-red threshold at which the threshold is considered crossed. When the threshold exceeds this hysteresis value, the device reports this call state change to the SEM. Notes: ▪ If the parameter crosses two thresholds at once (e.g., from Green to Red), the device ignores the hysteresis values and reports this call state change to the SEM. ▪ The valid threshold values are as follows: ✓ MOS values are in multiples of 10. For example, to denote MOS of 3.2, the value 32 (i.e., 3.2*10) is entered. ✓ Delay values are in msec. ✓ Packet Loss values are in percentage (%). ✓ Jitter is in msec. ✓ Echo measures the Residual Echo Return Loss (RERL) in dB.
IP Group Table	The following parameters have been added to the IP Group table to assign QoE, Bandwidth, and Media Enhancement profiles to an IP Group: ▪ [IPGroup_QOEProfile] QoE IP Profile = Assigns index from QoE Profile table ▪ [IPGroup_BWProfile] BW IP Profile = Assigns index from Bandwidth Profile table ▪ [IPGroup_MediaEnhancementProfile] Media Enhancement Profile = Assigns index from Media Enhancement Profile table
Media Realm Table	The following parameters have been added to the Media Realm table to assign QoE and Bandwidth profiles to a Media Realm: ▪ [CpMediaRealm_QoeProfile] QoE Profile = Assigns index from QoE Profile table ▪ [CpMediaRealm_BWProfile] BW Profile = Assigns index from Bandwidth Profile table Note: A Media Enhancement profile cannot be assigned to a Media Realm.

Applicable Products: All.

3.1.1.124 Bandwidth Profile

This feature provides an enhancement in the device's monitoring of bandwidth utilization. Bandwidth profiles, which define bandwidth utilization thresholds for audio and/or video calls, can now be configured in a dedicated Bandwidth Profile table and associated with IP Groups, Media Realms, and Remote Media Subnets.

Bandwidth Profiles are used for the following:

- Access control and media enhancements based on bandwidth
- Alternative routing based on bandwidth

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

Bandwidth Profile CLI: bw-managment [BWProfile]	Defines bandwidth utilization threshold profiles. [BWProfile] FORMAT BWProfile_Index = BWProfile_Name, BWProfile_EgressAudioBandwidth, BWProfile_IngressAudioBandwidth, BWProfile_EgressVideoBandwidth, BWProfile_IngressVideoBandwidth, BWProfile_TotalEgressBandwidth, BWProfile_TotalIngressBandwidth, BWProfile_WarningThreshold, BWProfile_hysteresis, BWProfile_GenerateAlarms; [\BWProfile]] ▪ Egress Audio bandwidth = Outgoing audio traffic (Kbps) ▪ Ingress Audio bandwidth = Incoming audio traffic (Kbps) ▪ Egress Video bandwidth = Outgoing video traffic (Kbps) ▪ Ingress Video bandwidth = Incoming video traffic (Kbps) ▪ Total Egress Bandwidth = Total (video and audio) outgoing bandwidth (Kbps) ▪ Total Ingress Bandwidth = Total (video and audio) incoming bandwidth (Kbps) ▪ Warning Threshold = Threshold (%) of total bandwidth (green-yellow threshold). Note that the yellow-red threshold alarm is activated if the bandwidth exceeds the total bandwidth. ▪ Hysteresis = Hysteresis of total threshold (%) ▪ Generate Alarm: ✓ [0] Disable (default) ✓ [1]Enable

Applicable Products: All.

3.1.1.125 Access Control and Media Enhancements based on QoE and Bandwidth

This feature provides support for access control and media quality enhancements based on call quality measurements and bandwidth utilization. The latter are defined in the QoE Profile and Bandwidth Profile tables, described previously. These tables contain color-coded thresholds that are used to trigger Access Control and/or Media Enhancements.

This feature introduces a new table – Media Enhancement Profile – that can be configured to do any one of the following actions when a specific color-coded threshold is exceeded:

- Reject new calls (until the corresponding metrics return to below the threshold). This can be used, for example, to reject new calls when bandwidth threshold is exceeded.
- Use a different IP Profile. For example, if packet loss is detected, the IP Group can switch to an IP Profile configured with a higher RTP redundancy level.
- Send an SNMP alarm.

A Media Enhancement Profile can be associated with an IP Group. However, when the device analyzes the call and determines whether Media Enhancement Profile should be applied or not, it searches for the "most relevant" QoE Profile or Bandwidth Profile in the following order: 1) Remote Media Subnet, 2) Media Realm, and then 3) IP Group. Thus, a Media Enhancement Profile associated with a specific IP Group may actually "respond" to QoE or bandwidth thresholds crossed at the Media Realm or Remote Media Subnet.

The ability to use a different IP Profile when call quality of bandwidth thresholds are crossed provides a wide range of options for media enhancement and traffic shaping. For example, it may be used to:

- switch to a low bit-rate coder,
- negotiate different p-time (and perform transrating, if required),
- increase RTP redundancy level,
- or block video calls.

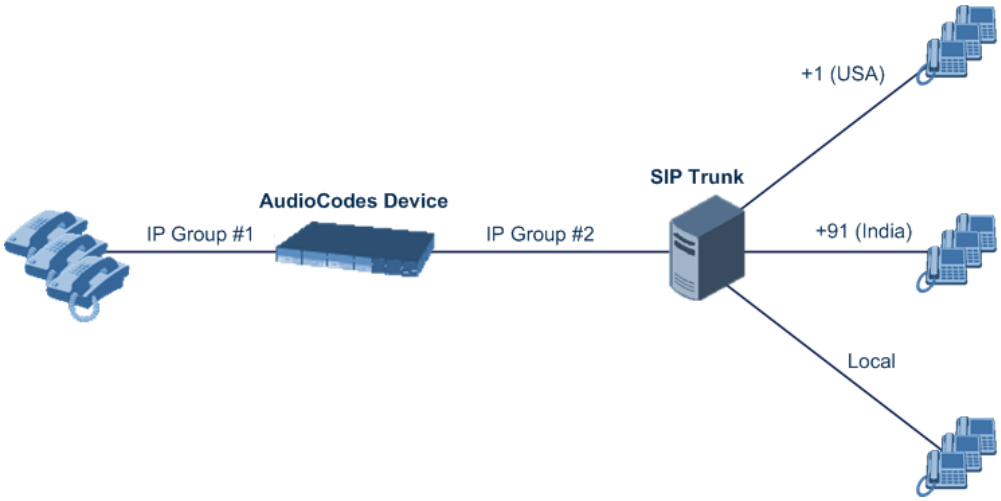
All media enhancements are performed for new calls only, based on the information gathered from previous and/or currently established calls.

Media Enhancement Profile CLI: media-enhancement [MediaEnhancementProfile]	Defines a Media Enhancement profile, which assigns a specific action if a color-coded threshold is crossed (green to yellow, and yellow to red). To define the action rules, use the subset table, Media Enhancement Rules table. [MediaEnhancementProfile] FORMAT MediaEnhancementProfile_Index = MediaEnhancementProfile_ProfileName; [\MediaEnhancementProfile
Media Enhancement Rules CLI: media-enhancement-rules [MediaEnhancementRules]	Defines action rules for the Media Enhancement profile. [MediaEnhancementRules] FORMAT MediaEnhancementRules_Index = MediaEnhancementRules_MediaEnhancementProfile, MediaEnhancementRules_Trigger, MediaEnhancementRules_Color, MediaEnhancementRules_ActionRule, MediaEnhancementRules_ActionValue; [\MediaEnhancementRules] ▪ Trigger: ✓ [0] MOS (default) ✓ [1] Delay ✓ [2] Packet Loss ✓ [3] Jitter ✓ [4] Bandwidth ▪ Color = Defines the color state of the parameter or bandwidth: ✓ [0] Red (default) ✓ [1] Yellow ▪ Rule Action: ✓ [0] Accept Calls (default) ✓ [1] Reject Calls ✓ [2] Alternative IP Profile ▪ Value: Alternative IP Profile (applicable only if Rule Action is set to Alternative IP Profile) Notes: ▪ The color-coded threshold is first calculated for the IP Group, and only then for its Media Realm. The minimal (worst) color-coded threshold crossing is chosen. For example, if a Media Realm crossed a green-yellow threshold and an IP Group a Yellow-Red threshold, the action defined for the Red color state is used. ▪ If a restrictive action (i.e., Alternative IP Profile or Reject Calls) is set for yellow and no action is set for red, the yellow action is also applied to red. ▪ If a permissive action (Accept Calls) is set for red and no action is set for yellow, the same action is applied to yellow.
IP Group Table	New parameter has been added to assign the Media Enhancement profile to the IP Group: ▪ [IPGroup_MediaEnhancementProfile] Media Enhancement Profile = index from Media Enhancement Profile table

Applicable Products: All.

3.1.1.126 Remote Media Subnets

This feature provides support for associating call quality and bandwidth profiles with remote media subnets, rather than IP Groups or Media Realms. Consider, for example, the following scenario:



IP Group #2 represents a SIP Trunk that routes international and local calls. As international calls typically are more prone to higher delay than local calls, different QoE profiles are assigned to them.

This feature introduces a new table – Remote Media Subnets – that defines a destination subnet for media (RTP/SRTP) traffic. Each remote media subnet may be associated with a different QoE Profile and Bandwidth Profile.

Remote Media Subnet Table CLI: subrealm [SubRealm]	Defines remote media subnet for media traffic (RTP/SRTP) and associates it with QoE and/or Bandwidth profile. [SubRealm] FORMAT SubRealm_Index = SubRealm_Realm, SubRealm_SubRealmIndex, SubRealm_PrefixLength, SubRealm_AddressFamily, SubRealm_DstIPAddress, SubRealm_QOEProfileName, SubRealm_BWProfileName; [\SubRealm] ▪ Prefix Length = Subnet mask in CIDR notation (e.g., 16 denotes 255.255.0.0). Default is 16. ▪ Address Family: ✓ [2] IPv4 Manual (default) ✓ [10] IPv6 Manual ▪ Destination IP = Destination IP address. Default is 0.0.0.0. ▪ QOE Profile Name = Index of QoE Profile to associate with this sub-media realm. ▪ BW Profile Name = Index of QoE Profile to associate with this sub-media realm.

Applicable Products: All.

3.1.1.127 Alternative Routing based on QoE and Bandwidth

This feature provides support for a new IP call termination reason related to QoE and bandwidth, which can be used as a reason for alternative routing. The device generates the internal Release Cause Code 806 (RELEASE_BECAUSE_MEDIA_LIMITS_EXCEEDED) when the thresholds are crossed of QoE metrics such as MOS, packet delay, and packet loss (configured in the Quality of Experience Profile table) and/or media bandwidth

(configured in the Bandwidth profile table). When this occurs, the device sends a SIP 480 (Temporarily Unavailable) response to the SIP entity.

To support this feature, the new optional value, '806 Media Limits Exceeded' has been added to the 'Release Cause' parameter in the following tables:

- Reasons for Tel-to-IP Alternative Routing (Gateway application)
- SBC Alternative Routing Reasons (SBC application)

This feature is implemented by assigning an IP Group a QoE and/or Bandwidth profile that rejects calls if the threshold is crossed, setting 806 as an alternative routing reason (as mentioned above), and then configuring an alternative routing rule.

Note that the code for the RELEASE_BECAUSE_IP_PROFILE_CALL_LIMIT release cause has been changed to 805. The device generates this reason when call admission control (CAC) limits are exceeded per IP Group. The CAC rules are configured in the Admission Control table for SBC calls, or in the IP Profile table for Gateway calls. When this occurs, the device sends a SIP 480 (Temporarily Unavailable) response to the SIP entity.

Applicable Products: All.

3.1.1.128 Reporting QoE to SEM/EMS Servers in Geo-Redundancy Mode

This feature provides support for reporting QoE metrics to the two SEM/EMS servers deployed in a Geographic Redundancy, High-Availability (HA) mode. Geographic Redundancy is when each EMS/SEM server is located in a different network subnet and has its own IP address. Thus, for the device to report QoE to both servers, the IP address of each server can now be configured on the device, using the new parameter described in the table below.

For regular HA mode, when both EMS/SEM servers are located in the same subnet, a single EMS/SEM server (global, virtual) IP address is used for all network components (EMS clients and managed devices). Thus, in such a setup, only this IP address needs to be configured on the device, which is done using the existing 'Server IP' parameter (QOEServerIp) parameter.

Redundant Server IP CLI: configure voip > qoe configuration > set secondary-server-ip [QOESecondaryServerIp]	Defines the IP address of the redundant SEM/EMS server to where the device sends QoE reports. Note: For this parameter to take effect, a device reset is required.

Applicable Products: All.

3.1.1.129 Reporting QoE Metrics of SBC Calls using SIP PUBLISH

This feature provides support for RTP Control Protocol Extended Reports (RTCP-XR) and Quality of Experience (QoE) metrics, according to RFC 6035. This information is sent at the end of the call using the SIP PUBLISH message. Below shows an example of a PUBLISH message sent with RTCP-XR and QoE information:

```
PUBLISH sip:10.8.4.61 SIP/2.0
    Via: SIP/2.0/UDP 10.8.61.16;branch=z9hG4bKac45186128
    Max-Forwards: 70
    From: <sip:10.8.61.16>;tag=1c44171734
    To: <sip:10.8.61.16>
    Call-ID: 4413389428420121558360@10.8.61.16
    CSeq: 1 PUBLISH
    Contact: <sip:10.8.61.16:5060>
    Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
    Event: vq-rtcpxr
```

```
    Expires: 3600
    User-Agent: Audiocodes-Sip-Gateway-Mediant 1000 - MSBG/v.6.40A.037.009
    Content-Type: application/vq-rtcpxr
    Content-Length: 710

    VQIntervalReport
    CallID=13746175212842012155835@10.8.61.16
    LocalID: <sip:12345@10.8.61.16>
    RemoteID: <sip:54321@10.8.61.18>
    OrigID: <sip:12345@10.8.61.16>
    LocalAddr: IP=10.8.61.16 Port=6110 SSRC=0xce110633
    RemoteAddr: IP=10.8.61.18 Port=6050 SSRC=0xffffffff
    LocalGroup:
    RemoteGroup:
    LocalMAC: 00:90:8f:2e:3c:67
    LocalMetrics:
    Timestamps: START=2012-04-28T15:58:36Z STOP=2012-04-28T15:58:36Z
    SessionDesc: PT=8 PD=PCMA SR=8000 FD=20 PLC=3 SSUP=Off
    JitterBuffer: JBA=3 JBR=0 JBN=0 JBM=0 JBX=300
    PacketLoss: NLR=0.00 JDR=0.00
    BurstGapLoss: BLD=0.00 BD=0 GLD=0.00 GD=0 GMIN=16
    Delay: RTD=0 ESD=0
    QualityEst:
    DialogID: 13746175212842012155835@10.8.61.16;to-tag=1c252030485;from-
tag=1c1374725246
```

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

Web: SBC RTCP XR Report Mode cli: sbc-rtcpxr-report-mode [SBCRtcpXrReportMode]	Enables the sending of RTCP-XR reports of QoE metrics at the end of each call session (i.e., after a SIP BYE). The RTCP-XR is sent in the SIP PUBLISH message. ▪ [0] Disable (default) ▪ [1] End of Call

Applicable Products: All.

3.1.1.130 Enhanced Voice Quality (RTCP-XR) Reporting

This feature provides support for additional optional values when enabling RTCP-XR functionality.

To support this feature, the following optional values – [1] and [2] – have been added to the existing parameter, Enable RTCP XR:

Web: Enable RTCP XR CLI: voice-quality-monitoring-enable [VQMonEnable]	Enables voice quality monitoring and RTCP XR, according to Internet-Draft draft-ietf-sipping-rtcp-summary-13. ▪ [0] Disable (default) ▪ [1] Enable Fully = Calculate voice quality metrics, use them for QoE calculations, report them to SEM (if configured), and send them to remote side using RTCP-XR. ▪ [2] Enable only Calculation = Calculate voice quality metrics, use them for QoE calculations, report them to SEM (if configured), but **do not** send them to remote side using RTCP-XR. Note: For this parameter to take effect, a device reset is required.

Applicable Products: All.

3.1.1.131 Display of QoS Media Statistics per IP Group in CLI

This feature provides support for displaying the following QoS metrics per IP Group in the CLI:

- QoE profile metrics per IP Group and its associated Media Realm on currently

established calls such as MOS, jitter, packet loss, and delay. Metrics are displayed as average amounts.

- Bandwidth Profile (BW) metrics for Tx and Rx traffic per IP Group and/or Media Realm. Metrics are displayed with a status color for each specific port.
- QoE profile metrics for the remote (far-end) such as MOS, jitter, packet loss, and delay. Each metric is displayed with a specific color.
- Group MSA metrics for the IP Group and the Media Realm. Metrics are displayed as an aggregated value.

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

```
#show voip voip-network ip-group <IP Group ID> media-stats
```

For example:

```
# show voip voip-network ip-group 1 media-stats
Group 1
Group MSA: 0
Averages: MOS 0  Remote MOS 0 Delay 0 Remote Delay 0 Jitter 0
Remote Jitter 0
Fraction loss  tx 0 Fraction loss rx 0
Packet sent 0 Packet received 0
Audio Tx BW 0, Audio Tx Status Green
Audio Rx BW 0, Audio Rx Status Green
Total Tx BW 0, Total Tx Status Green
Total Rx BW 0, Total Rx Status Green
Video Tx BW 0, Video Tx Status Green
Video Rx BW 0, VIdeo Rx Status Green
MSA color Gray MSA remote color Gray
MOS color Gray MSA remote MOS color Gray
Delay color Gray MSA remote Delay color Gray
PL color Gray MSA remote PL color Gray
Jitter color Gray MSA remote Jitter color Gray
Media Realm 255 MSA: -1
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.132 Display of Number and Percentage of Active Channels per Coder

This feature provides support for displaying the number and percentage of active channels using each audio coder in the CLI.

To support this feature, the following new CLI command has been added (under the Enable mode):

```
# show voip coders-stats
```

For example:

```
# show voip coders-stats
There are 266 active channels.
Coder     Number of Channels      Percentage
-------------------------------------------
G729e           67                25.18
G726            76                28.57
G722            123               46.24
```

In the example, 67 channels (25.18%) of the 266 active channels are using the G729e coder, 76 (28.57%) are using the G726 coder, and 123 (46.24%) are using the G722 coder.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.133 SNMP Trap Event for Connectivity Loss per Proxy Server

This feature provides support for a new SNMP trap event—acProxyConnectivity–that is sent to notify of connectivity loss with a specific proxy server belonging to a specific Proxy Set. The connectivity status is determined by the device's existing, proxy keep-alive mechanism, which sends keep-alive messages to the proxy ('Enable Proxy Keep Alive' parameter set to Enable). When connectivity with the proxy server returns, this trap event is sent again to notify of this new state. Up until this release, a trap event (acProxyConnectionLost) was sent only when all the proxies of a Proxy Set were down.

Applicable Products: All.

3.1.1.134 Performance Monitoring MIBs for Packet Loss Statistics

This feature provides support for new performance monitoring SNMP MIBs that indicate packet loss statistics per Media Realm:

- acPMMediaRealmPacketLossRx: Indicates the maximum received RTP packet loss (reported by RTCP) per Media Realm up to this point in time during the collection interval, as indicated by the time Interval.
- acPMMediaRealmPacketLossTx: Indicates the maximum received RTP packet loss (reported by RTCP) per Media Realm up to this point in time during the collection interval, as indicated by the time Interval.

Applicable Products: All.

3.1.1.135 Performance Monitoring MIBs for SIP Transactions per Second

This feature provides support for a new performance monitoring SNMP MIB, acPMSIPActiveSIPTransactionsPerSecondTable. This MIB table indicates the number of active incoming and outgoing SIP transactions (e.g., INVITE message) per second. This MIB table includes the following:

- acPMSIPActiveSIPTransactionsPerSecondDirection
- acPMSIPActiveSIPTransactionsPerSecondInterval
- acPMSIPActiveSIPTransactionsPerSecondVal

This feature also supports the configuration of low and high thresholds for SIP transactions per second, which when crossed, the existing SNMP trap event, acPerformanceMonitoringThresholdCrossing is sent. These high and low thresholds are configured by the SNMP MIBs acPMSipAttributesActiveSIPTransactionsPerSecondHighThreshold and acPMSipAttributesActiveSIPTransactionsPerSecondLowThreshold, respectively.

Applicable Products: All.

3.1.1.136 Performance Monitoring MIBs for HA Maintenance Connection

This feature provides support for new performance monitoring SNMP MIBs (gauges) that provide packet loss statistics concerned with the High-Availability (HA) mode. The performance monitoring MIBs monitor the connection (i.e., Maintenance interface) between the Active and Redundant units. They calculate the packet loss in percentage (%) from Active to Redundant and from Redundant to Active units, where 0% indicates no packet loss. This feature also supports the configuration of high (by default 30%) and low (by default 5%) thresholds for the packet loss, which when crossed, the existing SNMP trap event, acPerformanceMonitoringThresholdCrossing is sent by the device.

- acPMHALinkRedundantToActivePacketLossPercentageTable
  - acPMHALinkRedundantToActivePacketLossPercentageInterval

- acPMHALinkRedundantToActivePacketLossPercentageVal
- acPMHALinkRedundantToActivePacketLossPercentageAverage
- acPMHALinkRedundantToActivePacketLossPercentageMax
- acPMHALinkRedundantToActivePacketLossPercentageMin
- acPMHALinkRedundantToActivePacketLossPercentageTimeBelowLowThreshold
- acPMHALinkRedundantToActivePacketLossPercentageTimeBetweenThresholds
- acPMHALinkRedundantToActivePacketLossPercentageTimeAboveHighThreshold
- acPMHAAttributesHALinkRedundantToActivePacketLossPercentageHighThreshold
- acPMHAAttributesHALinkRedundantToActivePacketLossPercentageLowThreshold

- acPMHALinkActiveToRedundantPacketLossPercentageTable
  - acPMHALinkActiveToRedundantPacketLossPercentageInterval
  - acPMHALinkActiveToRedundantPacketLossPercentageVal
  - acPMHALinkActiveToRedundantPacketLossPercentageAverage
  - acPMHALinkActiveToRedundantPacketLossPercentageMax
  - acPMHALinkActiveToRedundantPacketLossPercentageMin
  - acPMHALinkActiveToRedundantPacketLossPercentageTimeBelowLowThreshold
- High and low threshold MIBs:
  - acPMHALinkActiveToRedundantPacketLossPercentageTimeBetweenThresholds
  - acPMHALinkActiveToRedundantPacketLossPercentageTimeAboveHighThreshold
  - acPMHAAttributesHALinkActiveToRedundantPacketLossPercentageHighThreshold
  - acPMHAAttributesHALinkActiveToRedundantPacketLossPercentageLowThreshold

Applicable Products: Mediant 500 E-SBC; Mediant 800B Gateway & E-SBC; Mediant Non-Hybrid SBC.

3.1.1.137 New Attributes for Performance Monitoring MIB acPMSIPIPGroupInviteDialogsTable

This feature provides new attributes for the performance monitoring SNMP MIB table, acPMSIPIPGroupInviteDialogsTable:

- Minimum
- Average
- Maximum
- Distribution below/above/between thresholds
- Low and high thresholds

When the thresholds are crossed, the device sends the existing trap, acPerformanceMonitoringThresholdCrossing.

Applicable Products: All.

3.1.1.138 Caller and Callee Names in CDR and VQM

This feature provides support for sending the caller and callee names in Call Detail Records (CDR) and in Voice Quality Monitoring (VQM) sent to the Session Experience Manager (SEM).

- Signaling CDR fields (applicable only to SBC):
  - "Caller"
  - "Callee"
- VQM:
  - <Caller>John</Caller>
  - <Callee>Susan</Callee>

Applicable Products: All.

3.1.1.139 Sequence Numbering of CDR Syslog Messages

This feature provides support for disabling the inclusion of the sequence number in CDR Syslog messages. Up until this release, the device always included the sequence number in CDR Syslog messages.

By default, the device sequentially numbers CDR Syslog messages using the format [S=<number>], for example, "[S=6699]". A skip in the number sequence of messages indicates a loss of a message packet:

```
15:18:05.828 : 10.33.3.102 : INFO    : [S=6699] [SID:793745892] |CALL_END
|72   |793745892      |1    |12   |248  |2    |ISDN      |LCL
|10.33.3.102         |10.33.3.102          |0    |0    |26802754
```

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

Web: CDR Session ID CLI: cdr-seq-num [CDRSyslogSeqNum]	Enables the inclusion of the sequence number to CDRs. ▪ [0] Disable ▪ [1] Enable (default)

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.140 CDR Field Customization for Syslog and Stored CDRs

This feature provides support for customizing CDRs generated by the device and sent in Syslog messages (SBC media and signaling, and Gateway) and SBC CDRs stored locally on the device (only Mediant 9000 and Mediant Software).

The customized CDR field name can include the equals (=) sign (e.g., connect-time=) as well as enclosed by single (') or double (") apostrophes.

Syslog and locally stored CDR-field customization is configured through CLI using two tables – one for SBC calls and one for Gateway calls.

CDR-field customization is configured using the following CLI commands:

```
# configure voip > services cdr
(services-cdr)# cdr format gw-cdr-format | sbc-cdr-format <table
row index>
(gwsbc-cdr-format-0)# cdr-type history-sbc | syslog-media |
syslog-sbc | syslog-gw
(gwsbc-cdr-format-0)# col-type <default CDR field>
(gwsbc-cdr-format-0)# title <new CDR field name>
```

Applicable Products: All.

3.1.1.141 User Registration Activation and Status in CLI

This feature provides support for triggering user registration (and un-registration) with a proxy server, in the CLI. Up until this release, user activation could only be done in the Web interface.

To support this feature, the following CLI command has been added (basic command mode):

```
# admin register
```

- or -

```
# admin unregister
```

The following commands specify what to register / unregister:

- Entire Gateway:
  ```
  # admin register gw
  ```
- BRI or FXS endpoints (defined in the Supplementary Service table):
  ```
  # admin register suppserv <phone number as defined in
  Supplementary Service table>
  ```
- Analog ports:
  ```
  # admin register ports <module number> <port number>
  ```
  For example:
  ```
  # admin register ports 3 1
  ```
- Accounts:
  ```
  # admin unregister account <table row index of Account>
  ```
  For example:
  ```
  # admin unregister account 1
  ```
- User in the Gateway User Info table:
  ```
  # admin register userinfo gw <PBX extension>
  ```
  For example:
  ```
  # admin register userinfo gw 400
  ```
- User in the SBC User table:
  ```
  # admin register userinfo sbc <SBC Local User name>
  ```
  For example:
  ```
  # admin register userinfo sbc john
  ```

The following show commands have been modified:

- Displays users in the SBC or Gateway User Info table:
  ```
  # show voip register user-info <sbc|gw>
  ```
- Displays registration status ("REGISTERED" / "NOT REGISTERED") of Gateway ports (FXS, FXO, BRI):
  ```
  # show voip register ports
  ```
- Displays registration status of Gateway device (if Registration Mode is set to Per Gateway):
  ```
  # show voip register board
  ```
- Displays registration status of Accounts of SBC or Gateway calls:
  ```
  # show voip register accounts <sbc|gw>
  ```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.142 Status Display of SBC User Registration per AOR in CLI

This feature provides support for displaying the registration status of all the contacts of a specific user's Address of Record (AOR) listed in the device's Users' Registration database (SBC User Info table). This also includes showing the IP Group to which the contact belongs.

To support this feature, the following command has been added (to the root CLI level):

```
# show voip register db sbc user <Address Of Record>
```

For example:

```
# show voip register db sbc user 2017
```

```
*** SBC Registered Contacts for AOR '2017' ***
================================================================
sip:2017@10.8.2.225:5080;expire=90; Active: YES; IPG#4
```

"ACTIVE:YES" indicates that the user has been successfully registered; "ACTIVE:NO" indicates that the user has yet to be registered.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.143 Display of VoIP Call Statistics in CLI

This feature provides changes and enhancements to the CLI commands for displaying VoIP call statistics. These new CLI commands replace the commands from the previous release, and include the following (from the basic command mode):

- Displays all active calls (INVITE only) in ascending order by call duration:

  ```
  # show voip calls list
  ```

- Displays active calls that match the filter:

  ```
  # show voip calls list [filter: <session-id>|call-
  id|gw|sbc|summary]
  ```

  - *session ID:* Displays detailed session information for the specified session ID. For example:

    ```
    # show voip calls list 565445954
    ```

  - *descending*: Displays active calls in descending order by call duration
  - *gw*: Displays call information of active Gateway calls in ascending order by call duration
  - *ip2ip*: Displays call information of active IP-to-IP calls in ascending order by call duration
  - *sbc*: Displays call information of active SBC calls in ascending order by call duration
  - *summary*: Displays a summary of active calls

- Displays all call statistics (Gateway and SBC):

  ```
  # show voip calls statistics
  ```

- Gateway calls:

  - Displays Gateway call statistics:

    ```
    # show voip calls statistics gw
    ```

  - Displays IP-to-Tel Gateway call statistics:

    ```
    # show voip calls statistics gw ip2tel
    ```

  - Displays Tel-to-IP Gateway call statistics:

    ```
    # show voip calls statistics gw tel2ip
    ```

- Displays SBC call statistics:

  ```
  # show voip calls statistics sbc
  ```

- SIP SUBSCRIBE dialog statistics:

  - Displays SUBSCRIBE dialog sessions:

    ```
    # show voip subscribe list
    ```

  - Displays SUBSCRIBE dialogs that match the filter:

    ```
    # show voip subscribe list [filter: <session-
    id>|descending|summary]
    ```

    - *session ID*: Displays detailed session information for the specified session ID
    - *descending*: Displays active SUBSCRIBE dialogs in descending order by call duration

- *summary*: Displays summary of active SUBSCRIBE dialogs
- Displays SUBSCRIBE dialog statistics:

```
# show voip subscribe statistics
```

- Displays other dialog statistics:

```
# show voip other-dialog statistics
```

- Displays E911 information (ELIN):

```
# show voip e911
```

- Reset statistics (counters):
  - Clears all gateway-related statistics:

```
# clear voip gw
```

  - Clears VoIP-network signalling statistics:

```
# clear voip calls
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 2600; Mediant 4000.

3.1.1.144 Display of Proxy Set Status in CLI

This feature provides support for displaying the status of the Proxy Sets in the CLI. The status indicates IP connectivity with the proxy server and can be "OK" or "FAIL".

To support this feature, the following new CLI command has been added (basic command mode):

```
# show voip proxy sets status
```

For example:

```
        Active Proxy Sets Status
ID          IP ADDRESS                    STATUS
0           Not Used    --
1           10.33.4.241(10.33.4.241)      OK
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.145 SBC Performance Monitoring MIBS

This feature provides support for new SBC performance monitoring (counter) SNMP MIBs:

- AcPMSIPIPGroupInviteDialogsTable: Number of calls (initiated by SIP INVITE) per IP Group.
- acPMSIPIPGroupSubscribeDialogsTable: Number of SUBSCRIBE dialogs per IP Group.
- acPMSIPIPGroupInInviteDialogsTable: Number of incoming calls (SIP INVITE) per IP Group.
- acPMSIPIPGroupInSubscribeDialogsTable: Number of incoming SUBSCRIBE dialogs per IP Group.
- acPMSIPIPGroupOutInviteDialogsTable: Number of outgoing calls (SIP INVITE) per IP Group.
- acPMSIPIPGroupOutSubscribeDialogsTable: Number of outgoing SUBSCRIBE dialogs per IP Group.
- acPMSIPInvitedDialogsTable
- acPMSIPSubscribeDialogTable
- acPMSBCRegisteredUsersTable (increments for each registered user and decrements

when it deregisters)

Applicable Products: All.

3.1.1.146 SBC Performance Monitoring MIB for Utilized Media Sessions

This feature provides support for a new SNMP Performance Monitoring MIB, acPMSBCMediaLegsTable, which indicates the number of currently used media sessions. The MIB can be configured with high and low thresholds, which if crossed, cause an existing trap event (acPerformanceMonitoringThresholdCrossing) to be sent.

Applicable Products: All.

3.1.1.147 Performance Monitoring MIBs for Attempted SBC Calls

This feature provides support for new performance monitoring SNMP MIBs that indicate attempted SBC calls, including high and low thresholds:

- acPMSIPSBCAttemptedCallsTable
  - acPMSIPSBCAttemptedCallsInterval
  - acPMSIPSBCAttemptedCallsVal
  - acPMSIPSBCAttemptedCallsAverage
  - acPMSIPSBCAttemptedCallsMax
  - acPMSIPSBCAttemptedCallsMin
  - acPMSIPSBCAttemptedCallsTimeBelowLowThreshold
  - acPMSIPSBCAttemptedCallsTimeBetweenThresholds
  - acPMSIPSBCAttemptedCallsTimeAboveHighThreshold
  - acPMSIPSBCAttemptedCallsTotal
- acPMSipAttributesSBCAttemptedCallsHighThreshold
- acPMSipAttributesSBCAttemptedCallsLowThreshold

Applicable Products: All.

3.1.1.148 Performance Monitoring MIBs for Established SBC Calls

This feature provides support for new performance monitoring SNMP MIBs that indicate established SBC calls, including high and low thresholds:

- acPMSIPSBCEstablishedCallsTable
  - acPMSIPSBCEstablishedCallsInterval
  - acPMSIPSBCEstablishedCallsVal
  - acPMSIPSBCEstablishedCallsAverage
  - acPMSIPSBCEstablishedCallsMax
  - acPMSIPSBCEstablishedCallsMin
  - acPMSIPSBCEstablishedCallsTimeBelowLowThreshold
  - acPMSIPSBCEstablishedCallsTimeBetweenThresholds
  - acPMSIPSBCEstablishedCallsTimeAboveHighThreshold
  - acPMSIPSBCEstablishedCallsTotal
- acPMSipAttributesSBCEstablishedCallsHighThreshold
- acPMSipAttributesSBCEstablishedCallsLowThreshold

Applicable Products: All.

3.1.1.149 New CDR Field for Media Realms for SBC Signaling

This feature provides support for a new Call Detail Record (CDR) field—"MediaRealmId"—which is sent in the CDR for SBC signaling. This field provides information on the specific Media Realm used by the call.

Applicable Products: All.

3.1.1.150 SBC CDR Local Storage

This feature provides support for configuring the device to store generated Call Detail Records (CDR) of SBC calls on its local hard disk. Once CDRs are saved locally, you can view them any time or send them to a remote destination through, for example, HTTP or FTP.

The CDRs are stored as a single text field in comma-separated value (CSV) format. The CSV format consists of a table where the first row header defines the fields and the second row the corresponding values. For example:

```
Title:    Session ID,Duration,Source URI,Destination
URI,Termination Reason
CDR Data: 5678123,45,1000@abc.com,2000@company.com,BYE
```

The maximum CDR storage size is 1,024 bytes and the maximum size of the cache is 4,096 CDRs.

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

configure voip > services cdr > cdr-local-storage [CDRLocalStorage]	Enables the <device> to store CDRs locally on its hard disk (in CSV file format). ▪ [0] Disable (default) ▪ [1] Enable
configure voip > services cdr > cdr-local-max-file-size [CDRLocalMaxFileSize]	Defines the size (in kilobytes) of each stored CDR file. Once the file size is reached, the <device> creates a new file for subsequent CDRs, and so on. The valid value is 100 to 10000. The default is 1024.
configure voip > services cdr > cdr-local-max-files [CDRLocalMaxNomOfFiles]	Defines the maximum number of stored CDR files. If the maximum number is reached, the <device> replaces (overwrites) the oldest created file with a subsequent new file, and so on. The valid value is 2 to 4096. The default is 5.
configure voip > services cdr > cdr-local-interval [CDRLocalInterval]	Defines how often (in minutes) the <device> creates a new CDR file. For example, if configured to 60, it creates a new file every hour. This occurs even if the maximum configured file size has not been reached (see the CDRLocalMaxFileSize parameter). However, if the maximum configured file size has been reached and the interval configured by the parameter has not been reached, a new CDR file is created. The valid value is 2 to 1440. The default is 60.

Applicable Products: Mediant 9000; Mediant SW.

3.1.1.151 Gateway CDR History Storage

This feature provides support for displaying historical Call Detail Record (CDR) information of Gateway calls. CDR history information is stored in the device's memory. The CDR history can store up to the latest 4,096 calls. Note that if the device is reset, CDR history information is deleted from memory.

The CDR history can be viewed using the following management platforms:

- **Web interface:** CDR History page (Status & Diagnostics tab > VoIP Status menu >

CDR History).

- **CLI:**
  - All CDR history:

```
# show voip calls history
```

For example:

```
| Call End Time                |End Point      |     Caller        |     Callee        |Direction|  Remote IP    |Duration| Termination Reason | Session ID
=============================================================================================================================================================
|15:06:36.000  UTC Tue Aug 12 2014|ISDN-1/1/2     |100                |400                |Incoming |10.33.8.51     |        |NO_ANSWER           |1596538769
|15:05:56.000  UTC Tue Aug 12 2014|FXS-3/1        |200                |100                |Outgoing |10.33.8.51     |00:00:14|NORMAL_CALL_CLEAR   |1596538762
|15:05:54.000  UTC Tue Aug 12 2014|ISDN-1/1/1     |400                |200                |Outgoing |10.33.8.52     |00:01:20|NORMAL_CALL_CLEAR   |1596538765
|15:04:27.000  UTC Tue Aug 12 2014|               |100                |444                |Incoming |10.33.8.51     |        |GENERAL_FAILED      |1596538766
|15:04:25.000  UTC Tue Aug 12 2014|ISDN-1/1/1     |100                |400                |Incoming |10.33.8.51     |00:00:02|NORMAL_CALL_CLEAR   |1596538764
|15:04:14.000  UTC Tue Aug 12 2014|ISDN-1/1/1     |400                |202                |Outgoing |10.33.8.52     |00:00:03|NORMAL_CALL_CLEAR   |1596538754
|15:04:06.000  UTC Tue Aug 12 2014|FXS-3/1        |200                |201                |Outgoing |10.33.8.52     |00:00:04|NORMAL_CALL_CLEAR   |1596538750
```

  - CDR history for a specific session ID:

```
# show voip calls history <session ID>
```

For example:

```
SessionId: 1596538762
End Point Type: FXS
SIP Call ID: 212600834012820141554O@10.33.8.70
Call Direction: Outgoing
Source IP: 10.33.8.70
Dest IP: 10.33.8.51
Call Duration: 00:00:14
Setup Time: 15:05:40.000  UTC Tue Aug 12 2014
Connection Time: 15:05:42.000  UTC Tue Aug 12 2014
Disconnect Time: 15:05:56.000  UTC Tue Aug 12 2014
Source Num Before Map: 200
Dest Phone Number: 100
Source Host Name: 10.33.8.70
Destination Host Name: 10.33.8.51
TrunkId: -1
B-Channel/Port ID: 4
Termination Side: LCL
Termination Reason: GWAPP_NORMAL_CALL_CLEAR
Termination Reason Category: NORMAL_CALL_CLEAR
Termination SIP Reason:
Termination SIP Description:
Termination PSTN Reason: 0
Cid: 4
Coder: g711Alaw64k
```

As part of this feature, the `show voip calls list` command has been replaced by `show voip calls active`. The displayed call information has been enhanced and now includes Call Start Time.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B.

3.1.1.152 Performance Monitoring MIB for Busy Trunks per Trunk Group

This feature provides support for a new Trunk Group performance monitoring SNMP MIB, gwTrunkGroupPercentageUtilization (Trunk Group Utilization in Percentage). This MIB indicates the percentage (%) of channels currently in use (busy) per Trunk Group. Up until this release, the device provided an indication of the number of channels currently busy per Trunk Group, using the SNMP MIB, gwTrunkGroupUtilization (Trunk Group Utilization).

The device also supports the configuration (SNMP) of a busy channel threshold per Trunk Group, which when exceeded, sends the existing SNMP trap event, acPerformanceMonitoringThresholdCrossing. For example, assume the device has 200

voice channels and the threshold is set to 90%. If the number of concurrent busy channels exceeds 90% (i.e. 180 channels), this threshold alarm is sent.

This performance monitoring parameter can also be viewed in the Web interface's Trunk Utilization page (Status & Diagnostics tab > Performance Monitoring > Trunk Utilization).

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.153 Performance Monitoring MIB for All Busy Channels per Trunk Group

This feature provides support for a new Trunk Group performance monitoring SNMP MIB (gauge), gwTrunkGroupAllTrunksBusyPercentage (All Channels Busy or commonly referred to as *All Trunks Busy* or *ATB*). This MIB indicates the percentage (%) of time, within a 15-minute polling interval, that all channels in a specific Trunk Group were busy simultaneously. This measurement is sent only at the end of the interval (beginning of the current interval) and thus, each measurement reflects the previous interval.

For example, assume that all trunks of a Trunk Group were busy for 6 minutes during an interval. The measurement sent by this MIB will be 40% (i.e., 6 minutes / 15 minutes * 100). In other words, all trunks of the Trunk Group were simultaneously busy for 40% of the time during this 15-minute interval.

This feature also supports the configuration of low and high busy-channel thresholds per Trunk Group, which when crossed, the existing SNMP trap event, acPerformanceMonitoringThresholdCrossing is sent. The low and high thresholds are configured by the SNMP MIBs acPMSipAttributesTrunkGroupAllTrunksBusyPercentageHighThreshold and acPMSipAttributesTrunkGroupAllTrunksBusyPercentageLowThreshold, respectively. Using the above example, if the high threshold is set to 40%, the trap event will be sent at the end of the 15-minute interval for which the threshold was crossed.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.154 Performance Monitoring MIB for Failed Calls per Trunk Group

This feature provides support for a new Trunk Group performance monitoring SNMP MIB, gwTrunkGroupNoResourcesCalls. This MIB indicates the number of calls that could not be established due to unavailable device resources (e.g., no free channels) per Trunk Group.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.155 Performance Monitoring MIB for Call Duration per Trunk Group

This feature provides support for a new Trunk Group performance monitoring SNMP MIB, gwTrunkGroupCallDuration. This MIB indicates the average call duration (in sec) of calls per Trunk Group.

Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.1.156 Test Call Enhancements

This feature provides the following enhancements for the Test Call feature:

- Playing prerecorded tones (PRT) from an installed PRT file to the called party. The played tone is Dial Tone #2. This is configured using the existing Test_Call_Play parameter. Up until this release, only DTMF signals were supported.
- By default, the device now plays DTMF signals to the called party. Up until this release, play of tone was disabled (Test_Call_Play parameter was set to 0).
- Test calls can now be assigned Quality of Experience (QoE) Profiles and Bandwidth Profiles, which are configured in the Quality of Experience Profile table and Bandwidth Profile table, respectively. This enables the displayed test call status to now include QoE and bandwidth statistics:

- MOS Status: MOS count and color threshold status of local and remote sides according to the assigned QoE Profile.
- Delay Status: Packet delay count and color-threshold status of local and remote sides according to the assigned QoE Profile.
- Jitter Status: Jitter count and color-threshold status of local and remote sides according to the assigned QoE Profile.
- Packet Loss Status: Packet loss count and color-threshold status of local and remote sides according to the assigned QoE Profile.
- Bandwidth Status: Tx/Rx bandwidth and color-threshold status according to the assigned Bandwidth Profile.

Web: Play CLI: play [Test_Call_Play]	Enables and defines the playing of a tone to the answered side of the call. ▪ [0] Disable ▪ [1] DTMF (default) = Plays a user-defined DTMF string, configured in Configuring DTMF Tones for Test Calls. ▪ [2] PRT = Plays a non-DTMF tone from the PRT file (Dial Tone 2). For this option, a PRT file must be loaded to the device (see Prerecorded Tones File). Notes: ▪ To configure the DTMF signaling type (e.g., out-of-band or in-band) use the 'DTMF Transport Type' parameter. ▪ This parameter is applicable only if 'Call Party' is set to Caller.
Web: QoE Profile CLI: qoe-profile [Test_Call_QOEProfile]	Assigns a QoE Profile to the test call.
Web: Bandwidth Profile CLI: bandwidth-profile [Test_Call_BWProfile]	Assigns a Bandwidth Profile to the test call.

Applicable Products: All.

3.1.1.157 Re-Initialization with "Purified" Configuration

This feature provides support for applying a "purified" version of the current configuration to enable proper functioning of the device. This is useful when the device has correct configuration, but for some or other reason it doesn't function properly. This may be attributed to accumulated "mess" due to lengthy and numerous configurations. This feature enables the device to do a "fresh-and-clean" start with the current configuration.

When this feature is activated, the device 1) creates a CLI script file of the current configuration, 2) restores to factory defaults, 3) undergoes a reset, 4) applies (loads) the script file, and then 5) resets again, if required, for configuration settings to take effect.

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

```
# copy startup-script from running-config
```

Applicable Products: Mediant MSBR.

3.1.1.158 Display of Available CPU Resources in CPU Overload Alarm

This feature provides support for indicating the percentage of CPU resources remaining on the device, using the existing acBoardOverloadAlarm SNMP alarm. Up until this release, this alarm indicated only that a CPU overload existed on the device.

When this alarm is raised, the following alarm description appears:

```
"System CPU overload condition - IdleUtilization percentage=%d"
```

Where *%d* is the percentage of available CPU resources.

When this alarm is cleared, the following description appears:

```
"System returns to normal CPU usage - IdleUtilization
percentage=%d"
```

Applicable Products: All.

3.1.1.159 Display of Device CPU Utilization for VoIP Application

This feature provides support for displaying the current utilization of the device's CPU for the VoIP application (not data-routing), in percentage (%). To support this feature, the following new CLI command has been added (run from the basic command mode):

```
# show voip cpu-stats
```

For example:

```
# show voip cpu-stats
CPU percentage: 8%
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.160 Disconnection of Active Calls in CLI

This feature provides support for disconnecting active (established) calls, using the CLI. To support this feature, the following new CLI commands (basic command mode) have been added:

- Disconnects all active calls:

  ```
  # clear voip calls
  ```

- Disconnects active calls belonging to a specified Session ID:

  ```
  # clear voip calls <Session ID>
  ```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.161 Web Activity Notifications to Syslog in CLI

This feature provides support for determining the type of device-management operations (activity) to report to the Syslog server, in the CLI. Up until this release, this configuration could only be done using the ini file (ActivityListToLog parameter) and Web interface: Activity Types to Report via 'Activity Log' Messages in the Syslog Settings page (Configuration tab > System menu > Syslog Settings).

```
(config-system)# logging
(logging)# activity-log
(activity-log)# <activities to log>
```

Where *activities to log* can be:

- **config-changes:** changes in parameter value
- **defaults:** disables all activity log events
- **device-reset:** device resets
- **files-loading:** loading of auxiliary file(s)
- **flash-burning:** saving configuration with burn to flash memory
- **login-and-logout:** Web interface login and logout events
- **restricted-access:** Access to restricted Web pages
- **sensitive-config-changes:** Changes in values of "sensitive" parameters
- **software-update:** upgrade to device's software (cmp file)
- **unauthorized-access:** Unauthorized Web login attempts

To enable the Activity Log list, the following command must be entered after all the log settings:

```
(activity-log)# activate
```

The Activity Log list can be viewed using the existing, show running-config command. For example:

```
# show running-config
logging
    activity-log
     config-changes on
     files-loading off
     device-reset on
     flash-burning off
     software-update off
     restricted-access off
     unauthorized-access off
     sensitive-config-changes off
     login-and-logout off
    exit
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.162 Enhanced Debug Level and Reporting

This feature provides an enhancement to the device's debug configuration and mechanism. Due to an improved design, debug reporting is now more efficient regarding performance, using less CPU resources as in previous releases. In addition, configuration is now more user-friendly, enabling the user to choose between basic and detailed debug levels, where each of the following additional features can also be enabled, regardless of chosen debug level:

- Syslog Optimization: The device accumulates and bundles multiple debug messages into a single UDP packet and then sends it to a Syslog server. The benefit of this feature is that it reduces the number of UDP Syslog packets, thereby improving (optimizing) CPU utilization. In addition, the Syslog traffic is more efficient due to less overhead of headers (IP, UDP, and syslog).
- Syslog CPU Protection: If CPU resources drop (i.e., high CPU usage) to a critical level (user-defined threshold), the device lowers the debug level to free up CPU resources otherwise needed for the previous debug level. When CPU resources become available again, the device increases the debug level. The benefit of this feature is that it safeguards CPU resources vital for voice traffic.

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

Web/EMS: Debug Level CLI: configure system/logging/debug-level [GwDebugLevel]	(Modified Parameter) Enables Syslog debug reporting and logging level. ▪ [0] No Debug = (Default) Debug is disabled. ▪ [1] Basic = Sends debug logs of incoming and outgoing SIP messages. ▪ [5] Detailed = Sends debug logs of incoming and outgoing SIP message as well as many other logged processes. Note: When debug reporting is enabled, in order to view Syslog messages with Wireshark, you need to install AudioCodes Wireshark plug-in (acsyslog.dll). Once the plug-in is installed, the Syslog messages are decoded as "AC SYSLOG" and are displayed using the ‘acsyslog’ filter instead of the regular ‘syslog’ filter.

Syslog Optimization CLI: configure system/logging/syslog-optimization [SyslogOptimization]	Enables the device to accumulate and bundle multiple debug messages into a single UDP packet and then send it to a Syslog server. The benefit of this feature is that it reduces the number of UDP Syslog packets, thereby improving (optimizing) CPU utilization. ▪ [0] Disable ▪ [1] Enable (default) Note: The size of the bundled message is configured by the MaxBundleSyslogLength parameter.
Syslog CPU Protection CLI: configure system/logging/syslog-cpu-protection [SyslogCpuProtection]	Enables the protection of the device's CPU resources during debug reporting, ensuring voice traffic is unaffected. If CPU resources drop (i.e., high CPU usage) to a critical level (threshold), the device automatically lowers the debug level to free up CPU resources that were required for the previous debug-level functionality. The threshold is configured by the 'Debug Level High Threshold' parameter (see below). ▪ [0] Disable ▪ [1] Enable (default)
Debug Level High Threshold CLI: debug-level-high-threshold [DebugLevelHighThreshold]	Defines the threshold (in percentage) for automatically switching to a different debug level, depending on CPU usage. The parameter is applicable only if the 'Syslog CPU Protection' parameter is enabled. The valid value is 0 to 100. The default is 90. The debug level is changed as follows: ▪ CPU usage equals threshold: Debug level is reduced one level. ▪ CPU usage is at least 5% greater than threshold: Debug level is reduced another level. ▪ CPU usage is 5 to 19% less than threshold: Debug level is increased by one level. ▪ CPU usage is at least 20% less than threshold: Debug level is increased by another level. For example, assume that the threshold is set to 70% and the Debug Level to Detailed (5). When CPU usage reaches 70%, the debug level is reduced to Basic (1). When CPU usage increases by 5% or more than the threshold (i.e., greater than 75%), the debug level is disabled - No Debug (0). When the CPU usage decreases to 5% less than the threshold (e.g., 65%), the debug level is increased to Basic (1). When the CPU usage decreases to 20% less than the threshold (e.g., 50%), the debug level changes to Detailed (5). Note: The device does not increase the debug level to a level that is higher than that configured for the 'Debug Level' parameter.

Applicable Products: All.

3.1.1.163 Enhanced Debug CLI Commands

This feature provides support for enhanced debugging in the CLI. This is achieved by easily accessible debug commands located under the same folder (debug) and run from the enabled mode:

- Fax debug:

```
# debug fax {basic | detail} <number of fax/modem sessions>
```

  - *basic:* Basic debugging level
  - *detail:* Detailed debugging level

For example, below enables detailed debug level trace of the next 5 fax/modem sessions:

```
# debug fax detail 5
```

- SIP debug:

```
# debug sip <level>
```

Where <level> is the debug level. If not specified, level 5 is used by default.

- PSTN debug:

```
# debug voip voip interface <e1-t1 | bri> <module(slot)/trunk>
trace-level (full-isdn | full-isdn-with-duplications | layer3
| layer3-no-duplications | no-trace | q921-raw-data | q931 |
q931-q921-raw-data | q931-raw-data)
```

Enables PSTN trace:

```
# debug pstn
```

Displays current PSTN trace level of a specific trunk:

```
# debug voip interface <e1-t1 | bri> <module(slot)/trunk>
```

- Syslog server configuration:

```
# debug syslog-server <IP address> <port>
```

If the port is not specified, it is set to 514 by default.

- "Raw data" debug (debug recording):

```
# debug debug-recording <destination IP address> <port>
{signaling|signaling-media|signaling-media-pcm}
```

If port is not specified, it is set to the default port.

To disable a debug command, prepend it with the `no` prefix, for example:

```
# no debug debug-recording
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.164 Debug File upon Device Crash

This feature provides support for creating a debug file upon a device crash. The file contains the following information:

- Exception information, indicating the specific point in the code where the crash occurred
- Latest log messages that were recorded prior to the crash
- Core dump (if enabled) - contains an image of the device's memory at the time of the crash and provides a powerful tool for determining the root cause of the crash. When cored dump is enabled, it is saved to the device's flash (non-volatile memory) and can also be sent to a user-defined server (IP address).

The Debug file can be retrieved from the device using the Web interface (Maintenance tab > Maintenance menu > Debug > Save Debug File link) to save it to a folder on a local PC. This file can be sent to AudioCodes support team for troubleshooting the device crash.

The Debug file is saved with the following name:

- Filename extension: ".log"
- Filename: "debug_<device name>_ver_<firmware version>_mac_<MAC address>_<date>"

For example: debug_acMediant_1000_ver_680-8-4_mac_00908F099096_1-11-2013_3-29-29[2].log

To support this feature, the following parameters and button have been added under a new folder (Maintenance tab > Maintenance menu > Debug Utilities):

Web: Enable Core Dump	Enables the saving of a core dump file upon a device crash.

[EnableCoreDump]	▪ [0] Disable (disable) ▪ [1] Enable
Web: Core Dump Destination IP [CoreDumpDestIP]	Defines the IP address of the remote server where you want the device to send the core dump file. By default, no IP address is defined.
Save Debug File button	Saves the debug file to a folder on a local PC.

Applicable Products: All.

3.1.1.165 Debug Capture on Physical VoIP Interfaces in CLI

This feature provides support for capturing traffic on the device's physical (Ethernet LAN) VoIP interfaces (Layer-2 VLAN tagged packets). This feature allows the captured output to be saved in a PCAP-format file (suitable for Wireshark) to a TFTP (default) or an FTP server. Note that the generated PCAP file is in the Extensible Record Format (ERF). For Mediant 5xx and Mediant 8xx products, the capture can also be saved to a USB device. Up until this release, traffic capturing could only be done on the data-router interfaces.

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

- Starts physical VoIP debug capture:

```
# debug capture voip physical eth-lan
# debug capture voip physical start
```

- Captures packets continuously in a cyclical buffer (packets always captured until stop):

```
# debug capture VoIP physical cyclic buffer
```

- Retrieves latest capture (PCAP file) saved on a specified server:

```
# debug capture VoIP physical get_last_capture <TFTP/FTP
server IP address>
```

  The file is saved to the device's memory (not flash) and is erased after a device reset.

- Marks the captured file (useful for troubleshooting process):

```
# debug capture VoIP physical insert-pad
```

  Before running this command, the debug capture must be started.

- Displays debug status and configured rules:

```
# debug capture VoIP physical show
```

- Specifies the destination (FTP, TFTP, or USB) to send the PCAP file:

```
# debug capture VoIP physical target <ftp|tftp|usb>
```

- Stops the debug capture, creates a file named debug-capture-voip-<timestamp>.pcap, and sends it to the TFTP or FTP server:

```
# debug capture voip physical stop <TFTP/FTP server IP
address>
```

  If no IP address is defined, the capture is saved on the device for later retrieval.

  The maximum file size of debug captures that can be saved to the device is 20 MB for Mediant 5xx, Mediant 8xx, and Mediant 1000B, and 100 MB for Mediant 2600/4000.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 2600; Mediant 4000.

3.1.1.166 Debug Captures to FTP Server

This feature provides support for sending debug captures to an FTP server. Up until this release, debug captures could only be sent to a TFTP server.

To support this feature, the `ftp-server` argument has been added to the `debug` CLI command. For example:

- Data-related debug capturing:

```
# debug capture data interface GigabitEthernet 0/0 proto udp
host any port any ftp-server 192.168.0.15
```

- Voice-related debug capturing:

```
# debug capture voip interface vlan 1 proto all host any port
any ftp-server 10.4.2.58
```

Applicable Products: Mediant MSBR.

3.1.1.167 Saving Current Configuration to Remote Server

This feature provides support for saving device configuration to a file and then sending it to a user-defined URL path of a remote server (TFTP or HTTP/S), or to a USB storage stick plugged into the device (applicable only to Mediant 5xx and Mediant 8xx). The device first saves the configuration to its flash memory and then sends the file to the defined URL. The configuration in the saved file is based only on CLI commands. The feature is useful, for example, for reverting the device's configuration to a previously backed-up configuration (for whatever reason).

To support the feature, the following CLI command (root level) has been added:

- Remote server:

```
# write-and-backup to <URL path with file name>
```

- USB:

```
# write-and-backup to usb:///<file name>
```

Applicable Product: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SW.

3.1.1.168 EMS and SEM Support

This feature provides support for management of Mediant 5xx and Mediant Software SBC through AudioCodes EMS management tool and SEM monitoring tool. These management tools are already supported by the other AudioCodes products.

Applicable Product: Mediant 5xx; Mediant SW.

3.1.1.169 Product Key

This feature provides support for a Product Key for AudioCodes' Mediant SE SBC and Mediant VE SBC product lines. The Product Key is used to identify a specific purchase of these products for the purpose of subsequent correspondence with AudioCodes (e.g., for technical support or product upgrades). The Product Key is provided to the customer at the time of purchase.

In the Web interface, the customer should enter the Product Key in the Software Upgrade Key Status page (Maintenance tab > Software Update menu > Software Upgrade Key) for safekeeping for future reference (e.g., for support and upgrade purposes). Once added, it can be viewed on the same page or on the Device Information page (Status & Diagnostics tab > System Status menu > Device Information).

Product Key [ProductKey] CLI: configure system > product-key	Defines the Product Key. The valid value is a string of up to 40 characters.

Applicable Products: Mediant SW.

3.1.1.170 Detection of Incompatible Hardware Components

This feature provides support for indicating incompatible hardware components (e.g., network card) of the hardware platform on which the device is installed.

- Mediant SE SBC: During installation (from a CD), if an incompatible hardware

component is detected, a warning message. The user can abort installation or continue the installation process, as desired.

- Mediant VE SBC: Each time Mediant VE SBC is started it validates its Virtual Machine (VM) configuration and issues a warning if incompatible hardware and/or VM configuration is detected. The warning is displayed at the VM console for 10 seconds during the boot up sequence, after which normal start up sequence continues.

In addition, details of the hardware platform (and VM configuration for Mediant VE SBC) on which the software is installed can be viewed using the following new CLI command:

```
# show system hardware
```

Incompatible components are indicated with an asterisk (*).

Mediant SW (example showing incompatible NIC):

```
# show system hardware
    cpu: Intel<R> Xeon<R> CPU E31220 @ 3.10GHz, total 4 cores
    memory:  16376 MB
    chassis: ProLiant DL120 G7
    network:
         Intel Corporation 82574L Gigabit Network Connection
         Intel Corporation 82574L Gigabit Network Connection
         * Realtek Semiconductor Co., Ltd. RTL-8169 Gigabit
Ethernet (rev 10)
         * Realtek Semiconductor Co., Ltd. RTL-8169 Gigabit
Ethernet (rev 10)
```

Mediant 9000:

```
Mediant 9000> show system hardware
  CPU: Intel(R) Xeon(R) CPU E5-2690 0 @ 2.90GHz, total 16 cores
  Memory: total RAM: 65536 MB
  Chassis: ProLiant DL360p Gen8
  Network:
    Intel Corporation 82580 Gigabit Network Connection (rev 01)
    Intel Corporation 82580 Gigabit Network Connection (rev 01)
    Intel Corporation 82580 Gigabit Network Connection (rev 01)
    Intel Corporation 82580 Gigabit Network Connection (rev 01)
    Intel Corporation 82580 Gigabit Network Connection (rev 01)
    Intel Corporation 82580 Gigabit Network Connection (rev 01)
    Intel Corporation 82580 Gigabit Network Connection (rev 01)
    Intel Corporation 82580 Gigabit Network Connection (rev 01)
  Virtual env: None
```

Applicable Products: Mediant 9000; Mediant SW.

3.1.1.171 Saving Current Configuration to Remote Server or USB

This feature provides a change in the method for saving the current configuration (system, voice, and data functionalities) to a file on a remote server or USB. For Mediant MSBR, up until this release, current data configuration was saved to an external file, using the CLI command `copy data-configuration to`, which is now obsolete.

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

```
# copy cli-script to <TFTP, HTTP, HTTPS, or USB address>
```

For example:

```
# copy cli-script to tftp://192.168.0.3/device1.txt
# copy cli-script to usb://device1.txt
```

Note: The USB option is applicable only to Mediant 5xx and Mediant 8xx.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.172 Progress Indication for File Transfer in CLI

This feature provides support for the display of file transfer progress information when a file is transferred from/to the device, using the `copy from/to` CLI command. This feature is applicable to the TFTP, HTTP/S, FTP/S, and USB protocols. (The USB option is applicable only to the `copy to` command for Mediant 5xx and Mediant 8xx.)

Below is an example of a file download progress display:

%	Total	%	Received	%	Xferd	Average Dload	Speed Upload	Time Total	Time Spent	Time Left	Current Speed
100	29.2M	100	29.2M	0	0	939k	0	0:00:31	0:00:31	--:--:--	945k

Where:

- %: Percentage of total bytes transmitted (downloaded and uploaded) - downloaded is displayed only when downloading a file (i.e., `copy from` command)
- Total: Total bytes transmitted - downloaded and uploaded
- %: Percentage of downloaded bytes (for `copy from` command)
- Received: Currently downloaded bytes (for `copy from` command)
- %: Percentage of uploaded bytes (for `copy to` command)
- Xferd: Currently uploaded bytes (for `copy to` command)
- Average Dload: Average download speed in bytes/sec (for `copy from` command)
- Speed Upload: Average upload speed in bytes/sec (for `copy to` command)
- Time Spent: Elapsed time
- Time Left: Duration remaining to complete file transfer
- Current Speed: Current transmission speed in bytes/sec

Note: For Mediant MSBR, when downloading a file using FTP through the WAN interface (data source), the only progress information displayed is the number of transferred bytes.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.173 Descriptive Names for Configuration Rules

This feature provides support for configuring an arbitrary descriptive name for certain configuration rules. This description allows the user to easily identify configured rules.

To support this feature, the new field, 'Name' has been added to the following tables for entering a string-based description:

- SBC:
  - Classification Table – 'Classification Name'
  - IP-to-IP Routing Table (SBC) – 'Route Name'
  - IP to IP Inbound Manipulation – 'Manipulation Name'
  - IP to IP Outbound Manipulation – 'Manipulation Name'
  - Admission Control – 'Admission Name'
- Gateway:
  - Outbound IP Routing Table – 'Route Name'
  - Inbound IP Routing Table – 'Route Name'
  - Gateway Manipulation tables (seven tables) – 'Manipulation Name'
- Common:

- Proxy Sets Table – 'Proxy Name'
- SIP Interface Table – 'Interface Name'
- Message Manipulations – 'Manipulation Name'

Applicable Products: All.

3.1.1.174 Device Reset not Required for Specific Configurations

The following existing parameters no longer require a device reset for their settings to take effect:

- Max. Hook-Flash Detection Period (FlashHookPeriod)

  Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B.

- Min. Hook-Flash Detection Period (MinFlashHookTime)

  Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B.

- TDM Bus Clock Source (TDMBusClockSource)

  Applicable Products: Mediant 500/L MSBR; Mediant 8xx; Mediant 1000B; Mediant 3000.

- Tables:
  - Media Realm table. Note that if a Media Realm is changed during a call that is on this Media Realm, no Quality of Experience of the call is done. If the Media Realm is deleted while there is a call using it, the call is maintained until the parties end it.
  - Interface table
  - SRD table
  - SIP Interface table

  Applicable Products: All.

- CED Transfer Mode (CEDTransferMode)

  Applicable Products: All.

3.1.1.175 "MSBG" Replaced with "MSBR"

This feature completes the transition in the product name change from "MSBG" to "MSBR", introduced in Release 6.6. This replacement has been done in all the management interfaces (Web, EMS, CLI, and ini) as well as in the firmware file name.

Applicable Products: Mediant MSBR.

3.1.1.176 Automatic Provisioning from USB Flash Drive

This feature provides support for automatic provisioning of the device using a USB flash drive plugged into the device's USB port. Configuration is pre-configured by the user in a text-based file using CLI commands. The file is saved with the name "ac_autorun.txt" and copied to the USB flash drive. Once the USB is plugged in, the device runs the commands specified in the file, line-by-line, similar to a Telnet connection. The device writes the output of the commands in the file "ac_output.txt", which it sends to the USB flash drive.

This tool can be used for configuring the device as well as for status and diagnostics where show and debugging commands can be used, the output of which is shown in the "ac_output.txt" file.

For more information on using this feature, refer to the *User's Manual*.

Applicable Products: Mediant MSBR.

3.1.1.177 Configurable TFTP Block Size for Automatic Update

This feature provides support for configuring the TFTP block size (according to RFC 2348), used when downloading a file from a TFTP server for the Automatic Update mechanism. TFTP block size is the physical packet size (in bytes) that a network can transmit. When configured to a value higher than the default (512 bytes) but lower than the client network's Maximum Transmission Unit (MTU), the file download speed can be significantly increased.

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

CLI: config-system > automatic-update tftp-block-size [AUPDTftpBlockSize]	Defines the size of the data blocks (packets) of the sent file when using TFTP for the Auto Update mechanism. The valid value is 512 to 8192. The default is 512.

Notes:

- A higher value does not necessarily mean better performance.
- The block size should be small enough to avoid IP fragmentation in the client network (i.e., below MTU).
- This feature is applicable only to TFTP servers that support this option.

Applicable Products: All.

3.1.1.178 Continuous Automatic Firmware Update

This feature provides support for an additional method for automatically updating the device's software (.cmp file), using the HTTP If-Modified-Since header. Each time automatic update is activated (upon bootup and/or periodically), the device checks for an updated software file at the provisioning server by sending an HTTP Get request containing the HTTP If-Modified-Since header. If the file has not been modified since the date and time specified in the header, the server replies with an HTTP 304 response and the device does not download the file. If the file has been modified (i.e., receives a 2xx response), the device downloads the file and compares its software version with the currently installed version. If the file is a later version, the device installs it (and resets). An example of this header is shown below:

```
If-Modified-Since: Mon, 1 Jul 2013 19:43:31 GMT
```

Notes:

- The device updates the value of the If-Modified-Since header to the date and time of the last received file. This is regardless of whether the file was installed or not.
- If URLs of both CLI Script and .cmp files are configured, the .cmp URL is downloaded first. This is done as the new CLI script may require a new software version.

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

CLI: automatic-update > auto-firmware [AutoCmpFileUrl]	Defines the path (URL) to the remote server and file name from where the software file (.cmp) can be downloaded, based on timestamp. The valid value is an IP address in dotted-decimal notation or an FQDN.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.179 HTTP User-Agent Header for Automatic Update

This feature provides support for including the User-Agent header in the device's HTTP Get request. Each time automatic update is activated (upon bootup and/or periodically), the device checks for an updated software file at the provisioning server by sending an HTTP Get request The User-Agent header indicates the software version that is currently installed on the device. This header may be used by the provisioning server based on the server's requirements. The information sent in the User-Agent header is user-defined by a new

parameter, AupdHttpUserAgent, and can include any string value or the following supported string variable tags (case-sensitive):

- <NAME> - product name (according to the installed Software License Key), e.g. "Mediant 800"
- <MAC> - device's MAC address
- <VER> - software version currently installed on the device, e.g. "6.60.200.001"
- <CONF> - configuration version, as configured in the ini file parameter, INIFileVersion (or CLI command, configuration-version)

The device automatically populates these tag variables with actual values in the sent header.

For example:

- Configuration: AupdHttpUserAgent = <NAME>;<VER>
- User-Agent header:
  - Before sent: User-Agent: Mozilla/4.0 (compatible; AudioCodes; <NAME>;<VER>)
  - Sent: User-Agent: Mozilla/4.0 (compatible; AudioCodes; Mediant 800;6.60.200.001)

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

CLI: automatic-update > http-user-agent [AupdHttpUserAgent]	Defines the User-Agent HTTP header in the Auto-Update HTTP Get requests. The valid value is a string of up to 511 characters. By default, this parameter is not defined. In other words, the User-Agent header is set to "Mozilla/4.0 (compatible; AudioCodes; <NAME>;<VER>)", where the tags are replaced with actual values. Notes: ▪ The variable tags are case-sensitive. ▪ The tags can be defined in any order. ▪ The tags must be defined adjacent to one another (i.e., no spaces or special characters).

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.180 Zero Configuration Certificate for Automatic Update

This feature provides support for using the Zero Configuration certificate when retrieving configuration files from a remote provisioning server using the Automatic Update feature.

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

CLI: config-system > automatic-update > use-zero-conf-certs [AupdUseZeroConfCerts]	Enables the use of the Zero Configuration TLS certificate (TLS Context) for the Auto-Update mechanism when connecting to the HTTPS server. ▪ [0] Disable (default) = The device uses the regular TLS certificate ▪ [1] Enable

Applicable Products: Mediant MSBR.

3.1.1.181 Password Display in .ini File

This feature provides support for determining how the device displays passwords in the ini file. The passwords can be displayed in one of the following formats:

- Obscured: the password characters are concealed and displayed as encoded, with the prefix 1 followed by the obscured password, for example, "1S3p+fno="
- Hidden: the password is replaced with an asterisk (*)

When saving an ini file from the device to a PC, the passwords are displayed according to the enabled format, described above.

When loading an ini file to the device, obscured passwords are parsed and configured in the device; hidden passwords are ignored.

The device uses obscured passwords by default, thus enabling their full recovery in case of configuration restore or copy to another device. Up until this release, only the hidden format was supported and thus, passwords were lost.

When configuring a password in the ini file, one of the following formats can be used:

- 1<obscured password>: password in obscured format (as generated by the device); useful for restoring device configuration and copying configuration from one device to another.
- 0<plan text>: password in plain text; useful for configuring a new password.

[INIPasswordsDisplayType]	Defines how passwords are displayed in the ini file. ▪ [0] Disable (default) = Passwords are obscured (concealed or encoded). The passwords are displayed in the following syntax: 1<obscured password>. ▪ [1] Enable = All passwords are hidden, using asterisk (*).

Applicable Products: All.

3.1.1.182 New Utility for Viewing and Modifying ini Files

This feature provides support for a new AudioCodes proprietary utility—INI Viewer & Editor—for viewing and editing ini files. This utility is available from AudioCodes website at www.audiocodes.com/downloads and can be installed on any Windows-based PC.

The utility provides a user-friendly, graphical user interface (GUI), allowing the user to easily view and modify configuration. The utility supports auto-completion of parameter names where the user can simply type the first characters of the name, press Ctrl + space bar, and a drop-down list appears from which the required parameter can be chosen. For parameters whose value needs to be selected from a list of optional values, the user can also press Ctrl + space bar to display a drop-down list from which the required value can be chosen.

The utility provides a special edit mode for tables, where they are displayed in table-bordered format. Table rows can be easily added or removed using the Add or Remove buttons, respectively. The tables provide text boxes for values that need to be typed in or drop-down lists where a value can be selected. When a new row is added, the utility assigns default settings to its columns.

Below is a list of additional features:

- Invalid parameters entered by the user are displayed in red for easy identification.
- Search function (Ctrl + F), allowing the user to search any parameter or string in the ini file.
- When a new software version is available, the utility automatically prompts the user to upgrade the current installation.
- The utility stores a dictionary of parameters, which is used for the auto-completion function. This dictionary can be updated automatically from an FTP server.

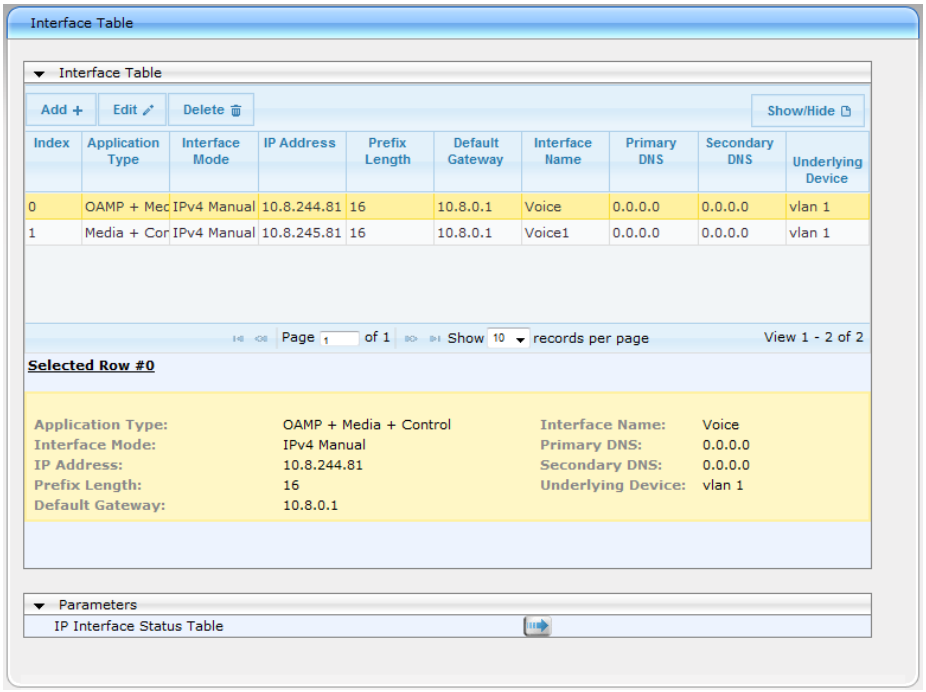
For more information on using this utility, refer to the IN*I Viewer & Editor Utility User's Guide*.

Applicable Products: All.

3.1.1.183 New Table Design of Configuration Tables

This feature provides support for an enhancement in the design of the Web configuration tables to simplify operation and facilitate configuration.

- The new table design implements a new layout and color scheme, such as shown in the figure below:



- When a new entry is added (i.e., the Add button is clicked), the next available table row index number is automatically assigned to the new entry (it can be changed manually).
- The Edit dialog box (accessed when the Edit button is clicked) now groups related parameters under tabs.
- The Up and Down buttons have been added to many tables. These buttons enable the user to change the table position (index) of a selected row.
- Show/Hide button has been added to some tables to toggle between displaying and hiding the full configuration of a selected row. The full configuration is displayed below the table and is useful for large tables that cannot display all its columns in the work pane.

The new table design has been applied to the majority of the configuration tables.

Applicable Products: All.

3.1.1.184 Modifications to Navigation Tree

The Navigation tree has been re-organized to provide a more consistent navigation experience. The name of the "Full" radio button has been changed to "Advanced" and some commonly used configuration pages were moved from "Advanced" to "Basic" view (e.g. Media Realms Table).

Applicable Products: All.

3.1.1.185 User Info Tables Configurable in Web Interface

The SBC User Info table and Gateway User Info table (databases) can now be configured in the Web interface. Up until this release, these tables could only be configured in the CLI or by loading a User Info file.

- Gateway User Info Table: This table is applicable to the Gateway application. It maps PBX extensions connected to the device to "global" IP numbers, and registers each PBX user to an external registrar server.

- SBC User Info Table: This table is applicable to the SBC application and can be used for the following:
  - Register to an external registrar server on behalf of a specific user
  - Authenticate (for any SIP request and as a client) on behalf of a specific user if challenged by an external server
  - Authenticate (as a server) incoming user requests

These tables can also be used to register or un-register a configured user. This is done using the table's Register and Un-Register buttons, respectively.

To support this feature, the following new tables have been added under the VoIP > SIP Definitions > User Information folder in the Navigation tree:

Web: SBC User Info Table CLI: sbc-user-info [SBCUserInfoTable]	Defines the SBC User Info table. [SBCUserInfoTable] FORMAT SBCUserInfoTable_Index = SBCUserInfoTable_LocalUser, SBCUserInfoTable_Username, SBCUserInfoTable_Password, SBCUserInfoTable_IPGroupID, SBCUserInfoTable_Status; [\SBCUserInfoTable]
Web: GW User Info Table CLI: gw-user-info [GWUserInfoTable]	Defines the Gateway User Info table. [GWUserInfoTable] FORMAT GWUserInfoTable_Index = GWUserInfoTable_PBXExtension, GWUserInfoTable_GlobalPhoneNumber, GWUserInfoTable_DisplayName, GWUserInfoTable_Username, GWUserInfoTable_Password, GWUserInfoTable_Status; [\GWUserInfoTable]

Note: If a User Info file is loaded to the device, all previously configured entries are removed from these tables (Gateway and SBC) and replaced with the users in the loaded User Info file.

Applicable Products: All.

3.1.1.186 Modifications to Parameter Name Options

This feature introduces changes to the names of the following parameter options:

Parameter	Option	
	Old	New
Alternative DTMF Method [IpProfile_SBCAlternativeDTMFMethod]	▪ Transparent ▪ Don't care	▪ In Band ▪ As Is
P-Asserted-Identity [IpProfile_SBCAssertIdentity]	Don't care	As Is
Diversion Mode [IpProfile_SBCDiversionMode]	Don't care	As Is
History-Info Mode [IpProfile_SBCHistoryInfoMode]	Don't care	As Is

Applicable Products: All.

3.1.1.187 New CLI Wizard for Initialization

This feature introduces a new tool—the *CLI Wizard*—for quick-and-easy configuration of the device's basic OAMP management settings. The tool is typically used for first-time configuration of the device, and is performed through a **direct** RS-232 serial cable

connection with a computer. Configuration is done using the device's CLI under a new CLI mode, `configure-wizard` (run from the "privileged" enable mode). Once configured through the tool, access to the device's management interface can be done over the IP network.

The CLI Wizard enables users to configure the following management settings:

- Users' login passwords for accessing the device's embedded Web and CLI servers.
- IP network OAMP interface
- SNMP community strings (read-only and read-write)

Note: The CLI Wizard can only be used on device's running factory default settings (applicable to all products except Mediant 3000). Best practice for restoring the device to factory defaults before using the CLI Wizard would be to use the CLI `write factory` command.

Applicable Products: All.

3.1.1.188 CLI Access to all User Levels

This feature provides support for allowing Monitor and Administrator user access levels to also access the CLI. Up until this release, only Security Administrator and Master access levels could access the CLI. In addition, to allow configuration of secured device parameters, the Security Administrator and Master levels no longer need to run the `enable` command after logging in to the CLI; Administrator and Monitor levels do need to run this command.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.189 Maximum Permitted Concurrent Telnet/SSH Sessions

This feature provides support for configuring the maximum number of concurrent Telnet/SSH sessions permitted on the device.

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

Web: Maximum Telnet Sessions CLI: telnet-max-sessions [TelnetMaxSessions]	Defines the maximum permitted number of concurrent Telnet/SSH sessions. The valid range is 1 to 5 sessions. The default is 2. Note: Before changing the value, make sure that not more than this number of sessions are currently active; otherwise, the new settings will not take effect.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.190 Display and Termination of Current CLI Sessions

This feature provides support for displaying and terminating users that are currently logged into the device's CLI. This applies to users logged into the CLI through RS-232 (console), Telnet, or SSH.

For each logged-in user, this feature displays the type of interface (console, Telnet, or SSH), user's username, remote IP address from where the user logged in, and the duration (days and time) of the session. Each user is displayed with a unique index (session ID).

- To view currently logged-in CLI users, the following new CLI command has been added:

```
# show users
[0]  console      Admin       local             0d00h03m15s
[1]  telnet       John        10.4.2.1          0d01h03m47s
[2]* ssh          Alex        192.168.121.234   12d00h02m34s
```

The current session from which the show command was run is displayed with an asterisk (*).

Note: The device can display management sessions of up to 24 hours. After this time, the duration counter is reset

- To end the CLI session of a specific CLI user, the following new command has been added:

```
# clear user <session id>
```

When this command is run, it drops the Telnet/SSH session or logs out the RS-232 session and displays the login prompt.

Note: The session from which the command is run cannot be terminated.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.191 Failure Reasons Display for CLI Commands

This feature provides support for displaying the failure reason of a run command in the CLI. The produced failure message is identical to the notification failure message sent via Syslog. For example, an invalid Syslog server IP address is displayed in the CLI as follows:

```
(logging)# syslog-ip 1111.1.1.1
Parameter 'SyslogServerIP' does NOT accept the IP-Address:
1111.1.1.1, illegal IPAddress.
Configuration failed
Command Failed!
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.192 Number of Displayed Output Lines in CLI Terminal Window

This feature provides support for configuring the maximum number of lines (height) displayed in the terminal window for the output of CLI commands. The number of displayed lines can be specified from 0 to 65,535, where 0 is all lines, or it can be determined by re-sizing the terminal window by mouse-dragging the window's border.

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

- Configures a specific number of lines:

```
(config-system)# cli-terminal
<cli-terminal># window-height [0-65535]
```

If *window-height* is set to 0, the entire command output is displayed. In other words, even if the output extends beyond the visible terminal window length, the *--MORE--* prompt is not displayed.

- Configures the number of lines according to dragged terminal window:

```
(config-system)# cli-terminal
<cli-terminal># window-height automatic
```

When the automatic mode is configured, each time the user changes the height of the terminal window by dragging one of the window's borders or corners, the number of displayed output command lines is changed accordingly.

This feature is applicable for SSH and Telnet sessions.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.193 Automatic Assignment of Indices for New CLI Table Rows

This feature provides support for automatically assigning the next consecutive, available index number to a newly added table row. The index number can be changed by the user.

If desired (as done in previous releases). In addition, when adding a new row, the device accesses the row's configuration mode.

To support this feature, the new command, `new` has been added to configuration table commands:

```
# <table name> new
```

For example, if three rows are currently defined in the Account table (account-0, account-1, and account-2) and a new entry is subsequently defined, account-3 is automatically created and its configuration mode is accessed:

```
(config-voip)# sip-definition account new
(account-3)#
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.194 Inserting Rows in CLI Tables

This feature provides support for adding a table row to any specific index number, even if a row has already been configured for that index entry. The row that previously contained that index number is subsequently incremented to the next index number, as well as all the index entries listed further down in the table. When a new row index is added, its configuration mode is automatically accessed.

To support this feature, the new command, `insert` has been added to configuration table commands:

```
# <table name> <index> insert
```

For example, if three rows are currently defined in the Account table (account-0, account-1, and account-2) and a new row is added with index 1, the previous account-1 becomes account-2 and the previous account-2 becomes account-3, and so on. The following command is run for this example:

```
(config-voip)# sip-definition account 1 insert
```

Note: This feature is applicable only to tables that do not have "child" tables (sub-tables).

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.195 CLI Prefix Command "set" Now Obsolete

The `set` prefix command is no longer used in the VoIP and System configuration modes (i.e., config-voip or config-system, respectively).

For example, in the previous release the following configuration was required with the `set` command:

```
configure voip
  interface network-if 0
     set ip-address 10.22.11.240
```

This configuration is now done without the `set` command:

```
configure voip
  interface network-if 0
     ip-address 10.22.11.240
```

Note that for certain CLI context, the `set` command may be required. This is documented in the relevant section of the CLI Reference Guide

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.1.196 Modifications of Existing CLI Commands

The following modifications have been made to the CLI:

- The command, `control-network` has been renamed `voip-network`. For example:

```
(config-voip)# voip-network sip-interface 1
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

- The path to the command, `realm` (configures the Media Realm table) has been relocated from `media` to `voip-network`. For example:

```
(config-voip)# voip-network realm 1
```

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

- The commands, `search-dn` and `search-dns` have been replaced by `ldap-servers-search-dns`

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

- The command, use-different-rtp-port-after-hold has been renamed dfrnt-port-after-hold.

Applicable Products: Mediant 8xx; Mediant 1000B.

- Dynamic Routing CLI Commands: As a result of CLI improvements which include support for multiple argument types, the argument prefix names (such as number-range-1, number-range-2, and ip-address) are no longer required:

CLI Command	Removed Arguments
ip community-list	number-range-1; number-range-2
ip extcommunity-list	number-range-1; number-range-2
Border Gateway Protocol (BGP):	
bgp cluster-id	ip-address; number
aggregate-address	ip-address; network
neighbor	ip-address; word
network	ip-address; network
Open Shortest Path First (OSPF):	
area	ip-address; number
network * area	ip-address; number
OSPF under Interface Configuration:	
ip ospf authentication-key	ip-address
ip ospf cost	ip-address
ip ospf dead-interval	ip-address
ip ospf hello-interval	ip-address
ip ospf priority	ip-address
ip ospf retransmit-interval	ip-address
ip ospf transmit-delay	ip-address
Routing Information Protocol (RIP) under route-map:	
match community	number-range-1; number-range-2; word
match extcommunity	number-range-1; number-range-2; word
set comm-list	number-range-1; number-range-2; word
set metric	number; relative-change

CLI Command	Removed Arguments
network network <A.B.C.D/M>	The second network argument
Show commands:	
clear ip bgp	ip-address; as-number; network
show data ip community-list	word; number
show data ip extcommunity-list	word; number

Applicable Products: Mediant MSBR.

3.1.1.197 Enhanced Security for SNMP Community Strings using ACL Rules

This new feature provides support for applying access control list rules (ACL) to SNMP Community strings -- read-only (RO) or read-write (RW). By associating an ACL rule with an SNMP Community string, the source and/or destination address of the packet, received from the management station and in which the Community string is received, can be specified. This adds enhanced security by reducing the likelihood of malicious attacks on the device if the Community string is discovered by an attacker.

Note that SNMP Community strings are used only for SNMPv1 and SNMPv2c (SNMPv3 uses username-password authentication, along with an encryption key).

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

```
<snmp># snmp-acl community-string <Community string> rw|ro <ACL
rule string name>
```

For example, the below configuration applies ACL rule named "MGMT" to the read-only SNMP Community string "public1":

- Configured ACL:

```
(config-data)# access-list MGMT deny udp any any eq 68
```

- Configured SNMP Community string:

```
(config-system)# snmp
<snmp># ro-community-string public1
```

- Binding SNMP Community string to ACL:

```
<snmp># snmp-acl community-string public1 ro MGMT
```

To delete a community string- ACL association, simply add single apostrophes at the end of the command line, for example:

```
<snmp># snmp-acl community-string public1 ro MGMT ''
```

Applicable Products: Mediant MSBR.

3.1.1.198 TR-098 Data Model for TR-069

This feature provides support for TR-098, a data model for TR-069. For more information, contact your AudioCodes sales representative.

Applicable Products: Mediant MSBR.

3.1.1.199 Remote Trigger for TR-069 Connection Request using SIP NOTIFY

This feature provides support for remotely triggering the device to request TR-069 connection with the Auto-Configuration Server (ACS). This is done using SIP NOTIFY messages with a TR-069 Connection Request. The device forwards the NOTIFY, received from the PBX, to the ACS. This feature is typically required when the ACS is unable to "reach" the device's management IP address (e.g., due to NAT) and thus, unable to send a "standard" TR-069 Connection Request. In such a scenario, the ACS requests the PBX to send a special SIP NOTIFY message to the device. Upon receipt, the device proceeds as if

it received a "standard" TR-069 Connection Request. In other words, it establishes a TR-069 connection with the ACS and sends an Inform TR-069 RPC method containing the "6 CONNECTION REQUEST" event code.

The SIP NOTIFY message contains an Event header set to the following proprietary value to activate connection request for TR-069:

```
Event: cwmp-connect
```

An example of a 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: cwmp-connect
```

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

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 (AudioCodes proprietary) 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. ▪ 'cwmp-connect': triggers connection with TR-069 The valid values: ▪ [0] Disable (default) ▪ [1] Enable Note: This feature does not trigger the automatic update mechanism based on the Zero Configuration feature.

Applicable Products: Mediant MSBR.

3.1.1.200 DHCP Option 43 for Obtaining URL of ACS

This feature provides support for the device to obtain the URL of the TR-069 Auto-Configuration Server (ACS), using DHCP Option 43. Up until this release, the URL had to be configured manually.

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

URL Provisioning Mode CLI: acs-url-provisioning-mode [Tr069AcsUrlProvisioningMode]	Defines the method for configuring the URL of the TR-069 ACS. ▪ [0] Manual (default) = URL must be configured manually on the device. ▪ [1] Automatic = Device uses DHCP Option 43 to obtain URL address of ACS.

Applicable Products: Mediant MSBR.

3.1.2 Known Constraints

This section lists known constraints discovered in the GA version.

3.1.2.1 SIP Constraints

This release includes the following known SIP constraints:

1. The Jitter Buffer for SBC calls can be configured on both legs (with or without DSPs) only when using G.711. For coders other than G.711, the Jitter Buffer can only be configured for one specific leg, which must have DSPs.

   Applicable Products: Mediant 3000.

2. Transrating of G.711, G.726, and G.729 for SBC calls from packetization time (ptime) 100/120 msec to 10/30/50 msec is not supported.

   Applicable Products: Mediant 1000B.

3. Some CDR values are not saved after a device switchover in High Availability mode.

   Applicable Products: Mediant 500 E-SBC; Mediant 800 GW & SBC; Mediant Non-Hybrid SBC.

4. When SBC termination features are used so that the device handles them locally (i.e., 'Remote Can Play Ringback', 'Play Held Tone', and 'Play RBT To Transferee'), Extension Coders Group ID must be configured, even if only one coder is used. This is especially relevant for the RBT to transferee feature.

   Applicable Products: All.

5. Graceful Shutdown is supported when the device operates in Gateway application mode only.

   Applicable Products: All.

6. Ring to Hunt Group feature is not functioning when Early Media is enabled.

   Applicable Products: Mediant 500 MSBR; Mediant 8xx.

7. The Gateway / IP-to-IP application is not supported.

   Applicable Products: Mediant Non-Hybrid SBC.

8. 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: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

9. 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: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

10. 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 8xx; Mediant 1000B; Mediant 3000.

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

    Applicable Products: Mediant 5xx; Mediant 8xx.

12. 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 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

13. Publishing of RTCP XR is sent only at call termination.

    Applicable Products: Mediant 3000.

3.1.2.2 Media Constraints

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

1. The On-Demand Jitter Buffer does not function correctly when transrating is also required (may cause packets loss).

   Applicable Products: Mediant 3000.

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.

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

   Applicable Product: Mediant 9000; Mediant SW.

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 5xx; Mediant 8xx.

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 5xx; Mediant 8xx.

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, and Speex. A workaround is to use SRTP full encryption / decryption on the forwarding calls.

   Applicable Products: 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 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000; Mediant Non-Hybrid 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 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: Mediant 5xx; Mediant 8xx; Mediant 1000B; 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: Mediant 5xx; Mediant 8xx; 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: Mediant 5xx; Mediant 8xx; Mediant 1000B; 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: Mediant 5xx; Mediant 8xx; Mediant 1000B; 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: Mediant 5xx; Mediant 8xx; Mediant 1000B; 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.

3.1.2.3 PSTN Constraints

This release includes the following known PSTN constraints:

1. The ISDN BRI American variants (NI2, DMS100, 5ESS) are partially supported by the device. Please contact your AudioCodes representative before implementing this protocol.

   Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B.

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

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

3.1.2.3.1 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.

3.1.2.3.2 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.

3.1.2.4 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 1000B.
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 1000B.
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 1000B.
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 1000B.
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 1000B.
6. The "Regular Expression Digitmaps" MSCML feature is not supported.

   Applicable Products: Mediant 1000B.

3.1.2.5 Networking Constraints

This release includes the following known networking constraints:

1. Adding more than 25 firewall rules in the Firewall Settings table (AccesList) may cause a device crash. As a workaround, it is recommended that no more than 19 rules be configured.

   Applicable Products: Mediant 2600; Mediant 4000.
2. 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 3000.
3. 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: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

4. 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.

5. Debug Recording:
   - Only one IP target is allowed.
   - Maximum of 50 trace rules are allowed simultaneously.

   Applicable Products: All.

6. 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: Mediant MSBR.

7. 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: Mediant MSBR.

8. When the device is setup with WAN ADSL/VDSL, CLI commands are missing for L2TP server interface configurations.

   Applicable Products: Mediant MSBR.

3.1.2.6 High Availability Constraints

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

1. After an HA switchover, if a very high volume of media traffic is present, a temporary low rate of packet loss may occur during the first few minutes (approx. 3 min.).

   Applicable Products: Mediant SE.

2. To upgrade from Version 6.6 to 6.8, do the following:
   a. Delete core dumps from the redundant device through CLI (Telnet).
   b. Perform a manual switchover from active to redundant.
   c. When the system is operational again, delete core dumps from the current redundant device through CLI (Telnet).
   d. Start the Hitless Software Upgrade procedure.

   Note: Core dump deletion can take up to 10 minutes.

   Applicable Products: Mediant 2600 HA; Mediant 4000 HA.

3. 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.

4. 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.

5. The Voice Prompt file needs be reloaded to the device after the completion of a Hitless software upgrade.

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

3.1.2.7 Infrastructure Constraints

This release includes the following known infrastructure constraints:

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

   Applicable Products: Mediant 2600; Mediant 4000.

2. Hyper-Threading (HT) is not supported. HT should be disabled in the BIOS setting of the server.

   Applicable Products: Mediant SW.

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
   - EnableDHCPLeaseRenewal
   - 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.

3.1.2.8 Management Constraints

3.1.2.8.1 General Features

This release includes the following known general management constraints:

1. Software upgrade to Version 6.8 requires a clean installation from CD.

   Applicable Products: Mediant SW.

2. RADIUS authentication is not supported. Using a RADIUS server may result in instability issues and therefore, it should be avoided.

   Applicable Products: Mediant SW.

3.1.2.8.2 Web Constraints

This release includes the following known Web constraints:

1. Enabling access by management stations (Web clients) to the Web-based management tool through any of the device's interfaces (in addition to the OAMP interface), by configuring the EnableWebAccessFromAllInterfaces parameter to 1, works flawlessly only under any one of the following conditions:
   a. The IP address of the Web client resides in the same subnet of the device's interface through which the Web client is accessing the Web interface.
   b. The IP address of the Web client does not reside in the same subnet as mentioned in a) above, but the device is configured with a Static Route rule (in the Static Routes table) where the destination ('Destination' field) is the IP address of the Web client and the assigned Ethernet Device ('Device Name' field) is the one associated with the device's network interface through which the Web client is accessing the Web interface.

   Applicable Products: All.
2. The AMD file cannot be deleted through the Web interface.

   Applicable Products: Mediant 1000; Mediant 3000.
3. The 'Monitor Destination Status' read-only field on the HA Settings page does not refresh automatically.

   Applicable Products: Mediant 4000 HA
4. If the device detects a duplicated IPv6 address (as result of an IPv6 DAD message), even though the relevant interface does not become active, the IP Interface Status table (Web interface and SNMP) erroneously display this interface as active. Duplicated IPv6 address occurrence can be identified in Syslog messages or in the CLI (showing active interfaces), where the problematic interface is correctly not displayed (as it is not active).

   Applicable Products: All.
5. An unnecessary scroll bar appears on many of the Web pages when using 1280 x 1024 screen resolution.

   Applicable Products: All.
6. 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.
7. 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 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000; Mediant Non-Hybrid SBC.
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: Mediant 5xx; Mediant 8xx; Mediant 1000B; 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 8xx; Mediant 1000B; 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 9000; Mediant SW.

14. 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.

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

    Applicable Products: Mediant 8xx; Mediant 1000B; Mediant 3000.

3.1.2.8.3 SNMP Constraints

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

1. The device does not support the acSysRedundantModuleTable acSysEthernetRedundantStatusTable.

   Applicable Products: Mediant 9000; Mediant SW HA.

2. The MIB-II ifTable, ifxTable, and entPhysicalTable are not supported.

   Applicable Products: Mediant 9000; Mediant SW.

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

   Applicable Products: Mediant 3000.

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

   Applicable Products: Mediant 3000 with TP-6310.

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

   Applicable Products: Mediant 3000 with TP-6310.

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

   Applicable Products: Mediant 3000 with TP-6310.

7. The dsx3Total Table is not supported.

   Applicable Products: Mediant 3000 with TP-6310.

8. The Admin State does not change to "Redundant".

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

9. 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: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000; Mediant 2600; Mediant 4000.

3.1.2.8.4 EMS Constraints

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

1. EMS Version 6.6 is not supported.

   Applicable Products: Mediant 5xx; Mediant 9000; Mediant SW.

2. EMS Version 6.4 GA is not supported:

   Applicable Products: Mediant 8xx; Mediant 1000B; Mediant Non-Hybrid SBC.

3.1.2.8.5 CLI Constraints

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

1. After changing the port used for Telnet or SSH sessions, it is required to disable and then enable the Telnet or SSH accordingly, in order for the port change to take effect. When the port is changed from the Telnet/SSH session itself, the Telnet/SSH should be disabled and then enabled using SNMP or Web.

   Applicable Products: All.

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

   Applicable Products: Mediant 9000; Mediant SW.

3. 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: Mediant MSBR.

3.1.3 Resolved Constraints

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

3.1.3.1 Media Resolved Constraints

The following media constraint has been resolved:

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 5xx; Mediant 8xx; Mediant Non-Hybrid SBC.

3.1.3.2 Networking Resolved Constraints

The following networking constraints have been resolved:

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 8xx; Mediant 1000B; Mediant 2600; Mediant 4000.

3. A maximum of five media stream recordings (debug) are allowed simultaneously.

   Applicable Products: All.

4. T1 WAN interface is not supported.

   Applicable Products: Mediant MSBR.

5. 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: Mediant MSBR.

6. A maximum of five media stream recordings (debug) are allowed simultaneously.

   Applicable Products: All.

7. PPTP server is not supported.

   Applicable Products: Mediant MSBR.

8. 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: Mediant MSBR.

3.1.3.3 PSTN Resolved Constraints

The following PSTN constraint has been resolved:

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: Mediant MSBR.

3.1.3.4 Infrastructure Resolved Constraints

The following infrastructure constraint has been resolved:

1. 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 – Mediant 3000
   - VLANNativeVLANID – Mediant 3000
   - RoutingTableDestinationsColumn - All
   - RoutingTableDestinationPrefixLensColumn – All
   - RoutingTableInterfacesColumn - All
   - RoutingTableGatewaysColumn - All
   - RoutingTableHopsCountColumn - All
   - RoutingTableDestinationMasksColumn - All
   - EnableDHCPLeaseRenewal – Mediant 3000
   - RoutingTableDestinationMasksColumn - All

   Applicable Products: All.

3.1.3.5 Web Resolved Constraints

The following Web constraints have been resolved:

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

   Applicable Products: All.
2. 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.
3. RADIUS is not supported.

   Applicable Products: Mediant 9000; Mediant SW.

3.1.3.6 SNMP Resolved Constraints

The following SNMP constraints have been resolved:

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: All.
3. SNMP is not supported.

   Applicable Products: Mediant 9000; Mediant SW.

3.1.3.7 CLI Resolved Constraints

The following CLI constraint has been resolved:

1. When connecting to the device using Telnet (CLI), Syslog messages do not appear by default. The **`show log`** command can be used to enable this feature.

   Applicable Products: Mediant 3000.

3.2 Patch Version 6.80A.292

No new features or constraints for this patch version.

3.2.1 Resolved Constraints

The following constraints from previous versions have been resolved in this patch version:

1. Mediant 9000 SBC in High-Availability (HA) mode "freezes" in certain scenarios. The workaround is to manually reset the device.

   The constraint has now been resolved.

   SR: 765925

   Applicable Products: Mediant 9000.

2. A high rate of SNMP activity results in memory leakage, causing the Mediant 3000 with TP-8410 blade, running firmware version 6.80A.285 to crash.

   The constraint has now been resolved.

   SR: 765971

   Applicable Products: Mediant 3000/TP-8410.

3. Trying to retrieve call history through the CLI causes the Mediant 9000 in HA mode to crash and subsequently reset.

   The constraint has now been resolved.

   SR: 765387

   Applicable Products: Mediant 9000.

4. If a cable is not connected to the Ethernet port and the device resets, the port's LED lights up constantly (does not turn off). The workaround is to connect a cable to the port.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 800.

6. Repeated occurrences of broken LDAP connections (for example, DNS problem or incorrect port) cause the device to crash.

   The constraint has now been resolved.

   SR: 763257

   Applicable Products: Mediant 3000.

7. Only up to four users can be concurrently logged into the device's Web interface.

   The constraint has now been resolved and up to five users can be concurrently logged in.

   SR: N/A

   Applicable Products: Mediant 3000.

8. The device sends a SIP 500 Internal Error response (instead of 100 Trying) in scenarios where call transfer is done from a regular call to a direct-media call. This causes media negotiation failure and thus, the call fails.

   The constraint has now been resolved.

   SR: 762207

   Applicable Products: Mediant 3000.

3.3 Patch Version 6.80A.295

3.3.1 New Features

This section describes the new features.

3.3.1.1 Registered Users Capacity Increase

This feature provides support for an increase from 500 to 600 in the number of users that can be registered with the device.

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

3.3.2 Known Constraints

This patch version includes the following known constraints:

1. The device reports incorrect trunk utilization values to the EMS.

   SR: 768545.

   Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

3.3.3 Resolved Constraints

The following constraints from previous versions have been resolved in this patch version:

1. The device reports incorrect trunk utilization values to the EMS.

   The constraint has now been resolved.

   SR: 768545.

   Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

2. The device sends REGISTER requests for configured user Accounts from the WAN interface to the proxy server, but the device's CLI shows the incorrect IP address (Contact URI) in the Account's status.

   The constraint has now been resolved.

   SR: N/A.

   Applicable Products: Mediant MSBR.

3. The device rejects SBC calls (SIP 488 response) before the number of calls have exceeded the maximum number of calls according to the installed Feature Key.

   The constraint has now been resolved.

   SR: 766577.

   Applicable Products: All.

4. The device crashes (and then resets) when attempting to update CAS channels on-the-fly (without first stopping the trunk).

   The constraint has now been resolved.

   SR: 767557.

   Applicable Products: Mediant 1000.

5. The device crashes (and then resets) when performing SBC call transfer during a SIPRec session (configured by setting the 'SBC Refer Mode' parameter to Handle Locally).

   The constraint has now been resolved.

   SR: N/A.

   Applicable Products: All.

6. No voice occurs on inbound calls when the IP Network interface is configured on Index 1. The workaround is to configure the interface on Index 0.

The constraint has now been resolved.

SR: 767311.

Applicable Products: All.

7. The LDAP username and password appear as clear text in Syslog, exposing this sensitive information to possible hackers. The workaround is to use TLS with the LDAP server.

   The constraint has now been resolved (credentials are hidden in Syslog).

   SR: N/A.

   Applicable Products: All.

8. The device's Automatic Update process through HTTP fails. This is due to an erroneous DNS lookup during device boot up.

   The constraint has now been resolved.

   SR: 764397.

   Applicable Products: All.

9. SIP message manipulation rules cannot be applied to un-REGISTER request messages.

   The constraint has now been resolved.

   SR: N/A.

   Applicable Products: All.

10. The device doesn't convert the SIP History-Info header into a Diversion header when the SIP response is 303 (Redirect).

    The constraint has now been resolved.

    SR: 767523.

    Applicable Products: All.

11. When a user is configured in the Account table and a SIP REFER triggers the device to generate an INVITE to the user, user authentication fails.

    The constraint has now been resolved.

    SR: 767481.

    Applicable Products: All.

12. A second REFER request for the same call is rejected if the first REFER failed.

    The constraint has now been resolved.

    SR: 766673.

    Applicable Products: All.

13. Call recording through SIPRec fails when the device receives a re-INVITE from the SRS. The following error appears in the Syslog: "maResourcePort::ConnectPorts - Can't connect".

    The constraint has now been resolved.

    SR: N/A.

    Applicable Products: Mediant 3000.

14. When the device is configured to handle REFER requests locally and it receives an INVITE from one leg and a REFER from the second leg at the same time, it fails to handle the REFER correctly and rejects the call with a SIP 491 response.

    The constraint has now been resolved.

    SR: 764835.

    Applicable Products: All.

15. The SNMP alarm acBoardEthernetLinkAlarm displays the related Ethernet interface as FE even though it is GE.

    The constraint has now been resolved.

SR: 762573.

Applicable Products: MSBR.

16. If the number of SBC sessions licensed in the Feature Key is low, after a few calls the device rejects calls with a SIP 488 response and includes the text "no more free ID" in the Syslog.

    The constraint has now been resolved.

    SR: 765835.

    Applicable Products: All.

17. Delay of responses from the LDAP server causes the device to crash and subsequently to reset.

    The constraint has now been resolved.

    SR: 757547

    Applicable Products: Mediant 3000.

20. If the password of the Admin user account is configured to more than 19 characters, the user cannot log in to the device's management interfaces.

    The constraint has now been resolved.

    SR: N\A

    Applicable Products: Mediant 500; Mediant 800.

3.4 Patch Version 6.80A.298.004

No new features or constraints for this patch version.

3.4.1 Resolved Constraints

The following constraints from previous versions have been resolved in this patch version:

1. If the device receives a SIP REFER message with a Refer-To header that contains an FQDN, it routes the call according to the Routing table instead of the Refer-To or contact. As a result, the call is not routed correctly.

   The constraint has now been resolved.

   SR: 771025

   Applicable Products: All.

2. When the device is configured to test calls continuously (endlessly), the Test Call feature terminates after a few weeks and no new test calls can be added or removed. The workaround is to reset the device.

   The constraint has now been resolved.

   SR: 768271

   Applicable Products: SBC.

3. If the device receives an invalid SIP message (i.e., missing the ">" character at the end of a header), it crashes and resets.

   The constraint has now been resolved.

   SR: 770617

   Applicable Products: SBC.

4. The device's RTP-only Mode (RTPOnlyMode) is not functioning - no RTP is sent and thus, no voice is sent over the network.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateways.

5. If the device receives a SIP INFO message during call establishment, it disconnects the call.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: SBC.

6. If the device employs digit maps (DigitMapping) or dial plans and it receives digits in the voice stream, the device crashes (resets).

   The constraint has now been resolved.

   SR: 768431

   Applicable Products: Digital Gateways.

7. When a PSTN call is put on hold, the device plays Music On Hold (MOH) for only three minutes and therefore, the held party does not hear the MOH.

   The constraint has now been resolved (play duration increased).

   SR: 770371

   Applicable Products: Digital Gateways.

8. Call forwarding does not function properly (SIP REFER) in this scenario: 1) The device receives a REFER with Replaces which it handles locally. 2) The replaced call exists on the device and thus, the REFER is done without a new INVITE. 3) The device receives a re-INVITE from one leg and forwards it to the second leg. 4) The device receives an answer with the same coder as in the SDP offer and therefore, the device rejects the call.

   The constraint has now been resolved.

   SR: 768577

   Applicable Products: SBC.

9. For call transfer where the transfer target does not answer, the device does not re-connect the initiator of the transfer (transferor) and the party being transferred (transferee). This is due to the ringback tone that the device plays to the transferee. A workaround is to disable play of ringback tone by the device.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Digital Gateways.

3.5 Patch Version 6.80A.300.009

No new features or constraints for this patch version.

3.5.1 Resolved Constraints

The following constraints from previous versions have been resolved in this patch version:

1. The device cannot be configured with payload type 125 for the Clearmode (Transparent) coder and thus, cannot negotiate transparent coder payload type.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateway.

2. After transferring a SIPRec call, the "transferred" SIPRec call does not terminate when the call ends.

   The constraint has now been resolved.

   SR: 774253

   Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SE/VE.

3. The device crashes (resets) when it starts DNS resolution immediately after sending a SIP CANCEL.

   The constraint has now been resolved (i.e., does not send a DNS request when call cancelled).

   SR: N/A

   Applicable Products: All.

4. The device performs alternative routing without audio in the following call scenario: 1) the device receives a call from the PSTN and sends an INVITE to the IP side; 2) the IP side rejects the call with a SIP 488; 3) the device performs alternative routing to itself. The no voice is due to the SDP in the alternative routing call which includes the device's WAN address.

   The constraint has now been resolved.

   SR: 771311

   Applicable Products: Gateway.

5. No voice occurs after call transfer when the device handles the REFER locally. During the call transfer, the device plays a held tone to one leg and ringback tone to the second leg, but after that no voice occurs. A workaround is to disable play of held tone or ringback tone.

   The constraint has now been resolved.

   SR: 773091

   Applicable Products: All.

6. When the parameter TrunkStatusReportingMode is set to 3 (Don't reply and send), and the trunk is taken out of service, the device still sends SIP OPTIONS to this trunk.

   The constraint has now been resolved.

   SR: 765637

   Applicable Products: Digital Gateway.

7. SBC Test calls are not routed correctly as the device uses the Gateway SRD instead of the SBC SRD.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant SE/VE.

8. When using LDAP with TLS, after few days of operation, the device fails to send SIP messages to the network, issuing the error "timer is not running". Calls consequently fail.

   The constraint has now been resolved.

   SR: 772305

   Applicable Products: All.

9. Call transfer fails in the following scenario: 1) the device sends a re-INVITE to one leg to play ringback tone; 2) the leg answers with a 200 OK at the same time as the new destination and 3) the device fails to handle it correctly.

   The constraint has now been resolved.

   SR: 770427

   Applicable Products: All.

3.6 Patch Version 6.80A.303.006

No new constraints for this patch version.

3.6.1 New Features

The section describes the new features.

3.6.1.1 Interworking BRI Call Forwarding Services to SIP

This feature provides support for indicating the type of call forwarding (CF) service, initiated by BRI phones connected to the device, in the Request-URI of the outgoing SIP INVITE message. Upon receipt of an ISDN Facility message for call forward (Diversion) from the BRI phone, the device indicates the call forwarding service in the Request-URI header using a proprietary parameter "facility=<call forward service>", for example:

```
INVITE sip:400@10.33.2.48;user=phone;facility=cfu-activate SIP/2.0
```

<call forward service> can have the following options:

- "cfu-activate" Call Forwarding Unconditional activated
- "cfu-deactivate" Call Forwarding Unconditional deactivated
- "cfb-activate" Call Forward on Busy activated
- "cfb-deactivate" Call Forward on Busy deactivated
- "cfnr-activate" Call Forward on No Reply activated
- "cfnr-deactivate" Call Forward on No Reply deactivated

To enable the feature, a new parameter has been added, USEFACILITYINREQUEST (CLI use-facility-in-req), which must be configured to 1 (default is 0, disabled).

To configure the digit codes used by the BRI endpoint to activate or deactivate the call forwarding services, the following existing parameters are used: SuppServCodeCFU, SuppServCodeCFUDeact, SuppServCodeCFB, SuppServCodeCFBDeact, SuppServCodeCFNR, and SuppServCodeCFNRDeact. The device sends these codes as a prefix to the number in the To header of the outgoing SIP INVITE message.

Applicable Products: All Supporting BRI Interfaces.

3.6.2 Resolved Constraints

The following constraints from previous versions have been resolved in this patch version:

1. No CLI command to disable RS-232. The workaround is to disable RS-232 through the Web interface.

   The constraint has now been resolved (new CLI command, `configure system > cli-terminal > rs232-console`).

   SR: N/A

   Applicable Products: All.

2. When using SIPRec, recording an incoming leg fails when SIP REFER is received on the incoming leg.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 3000; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SW.

3. The device does not route calls correctly when using LDAP and a 302 response is received. The call scenario is as follows: The device performs an LDAP query

according to the Routing table and then routes the call according to the LDAP result. If it receives a SIP 302 Moved Temp response, the device routes the new call according to the Routing table instead of the SIP Refer-To or Contact.

The constraint has now been resolved.

SR: 775055

Applicable Products: Gateway.

4. When the device needs to process an SRTP-to-RTP call and the initial SIP INVITE includes audio and fax images, the call fails. A workaround is to enable "Force Transcoding".

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: SBC.

5. When the device uses LDAP-based routing and the ADDNPIANDTON2CALLEDNUMBER parameter is set to 1 (adds NPI and TON to called number), it adds NPIs twice to the called number and therefore, the called number is incorrect.

   The constraint has now been resolved.

   SR: 774473

   Applicable Products: Digital Gateway.

6. The Char Conversion table (CharConversion) does not convert non-ASCII characters for IP-to-Tel calls in SIP P-Asserted-Identity headers. Therefore, the wrong name is sent to the PSTN.

   The constraint has now been resolved.

   SR: 775429

   Applicable Products: Digital Gateway.

7. When using SIPRec, the second SIPRec call for the consultation part of the call transfer does not terminate when the call is transferred, and the transfer fails.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 3000; Mediant 2600; Mediant 4000; Mediant 9000; Mediant SW.

8. In a WebRTC video call, only one-way video occurs.

   The constraint has now been resolved.

   SR: 772375

   Applicable Products: SBC.

9. The clearmode coder (Transparent coder) can only be configured with a payload type of up to 120. Therefore, negotiation of the coder for payload type 125 fails.

   The constraint has now been resolved (supports 125).

   SR: N/A

   Applicable Products: Gateway.

3.7 Patch Version 6.80A.306.006

No new features or constraints for this patch version.

3.7.1 Resolved Constraints

The following constraints from previous versions have been resolved in this patch version:

1. When the device operates in High-Availability mode (HA) and an HA switchover occurs, the speed of the fans of the Fan Tray module increase (even though the chassis temperature is normal).

   The constraint has now been resolved.

   SR: 778041

   Applicable Products: Mediant 3000.

2. On rare occasions, the device automatically resets for no reason.

   The constraint has now been resolved.

   SR: 778863

   Applicable Products: Mediant 2600; Mediant 4000.

3. When the SBCKeepContactUserInRegister parameter is set to 1 (keeps original contact name) and there is an associated contact, the device rejects the INVITE from the associated contact. As a result, these calls fail. A workaround is to disable the parameter.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: SBC.

4. If the device receives fragmented SIP messages at a very high rate, the device drops some of the packets and SIP messages are not received.

   The constraint has now been resolved.

   SR: 776693

   Applicable Products: SBC.

5. If a call recorded by SIPRec is transferred, the device does not send a re-INVITE message to the SIPRec server (SRS) to record the new call.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: All.

6. When the user tries to send more than 70 bytes of Q.931 raw data field, the device crashes and causes a reset.

   The constraint has now been resolved.

   SR: 775123

   Applicable Products: Digital-interface Supporting Devices.

7. When the device receives complicated and lengthy SIP INFO messages during a call, it crashes and resets.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateway.

8. When transcoding RTP to SRTP for SBC calls, the device waits for a SIP PRACK request even though PRACK isn't required. As a result, no voice occurs.

   The constraint has now been resolved.

   SR: 775535

   Applicable Products: SBC.

9. The possible values in CLI of the corresponding ini file parameter ISDNTxOverlap were changed but were not backward compatible and therefore, the parameter could not be configured through CLI.

   The constraint has now been resolved.

   SR: N/A

   Applicable Products: Gateway.

10. When a management user attempts to establish a new connection with the device through Telnet or SSH and provides incorrect username and password, a device resource "leak" occurs and as a result existing calls disconnect. A workaround is to disable Telnet and SSH.

    The constraint has now been resolved.

    SR: 777447

    Applicable Products: All.

3.8 Patch Version 6.80A.310.002

No new features or constraints for this patch version.

3.8.1 Resolved Constraints

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

Table 3-1: Resolved Constraints for Patch Version 6.80A.310.002

Incident	Description
135135	When an IP phone puts an SBC call that is SRTP on hold for longer than 30 minutes, the device disconnects the call. **Applicable Products:** Mediant 3000.
134881	In setups where the device interworks between Microsoft Lync Server and a SIP trunk, if Lync mutes the SBC call, Lync sends RTP version 0 (not valid RTP) packets to the device, but the device does not forward the packets. As a result, the SIP trunk terminates the call after five minutes. **Applicable Products:** Mediant 5xx; Mediant 8xx; Mediant 4000; Mediant SW.
134780	In SNMP, the ipGroupProxySetId field allows only values -1 to 5, instead of -1 to 50. As a result, all the Proxy Sets cannot be configured through SNMP. A workaround is to configure this through the Web interface, CLI, or ini file. **Applicable Products:** All.
133735	For Gateway calls, when the device receives a SIP re-INVITE without MKI, it responds with an MKI even though the remote side expects to receive the crypto without MKI (MKIsize=0). As a result, voice problems occur. A workaround is to configure the global parameter SRTPTXPACKETMKISIZE to 0 instead of 1. **Applicable Products:** Gateway.
133454	When the device is configured for Physical Network Separation, it tries to resolve the domain name but fails as no DNS server is configured for the specific interface. As a result, the device does not route the calls. (The resolved constraint: if no DNS server is configured for the interface, the device uses the DNS server configured for the OAMP interface if the EnableDNSasOAM parameter is enabled (default); otherwise, the DNS configured for the Control interface is used.) **Applicable Products:** Mediant 3000.
134124	When the device is enabled for Direct Media, if during call establishment the SBC call is picked up by another user, the device crashes and resets. **Applicable Products:** SBC.
134621	The device fails to query the LDAP server after it receives a SIP 302 response. As a result, calls are not routed correctly. **Applicable Products:** Gateway.
134390	If the management user configures the Channels field to "1-32" (instead of "1-31") in the Trunk Group Table for E1, the configuration is removed from the table due to a validation error and the Trunk Group is not saved to configuration. **Applicable Products:** Digital Gateway.

Incident	Description
134668	For a Tel-to-IP call, if the device receives a SIP 183 with a different to-tag (forking), it does not send a PROGRESS message to the Tel side. As a result, early media from the called party is not received by the calling party. **Applicable Products:** Digital Gateway.
134603	When the device forwards a SIP 200 OK in response to a SIP REGISTER message, it removes the "reg-ID" parameter in the Contact header (received in the original 200 OK). A workaround is to configure a Message Manipulation rule that keeps the "reg-ID" parameter in the forwarded 200 OK. **Applicable Products:** SBC.
134610	After performing a successful Web login based on RADIUS authentication, the device erroneously issues an error message in the Syslog. **Applicable Products:** All.
134338	During an SBC call, if one side sends a session timer refresh and the other side states no support for the session timer, the device erroneously disconnects the call after the timer expires. (Resolved constraint - the device ignores the timer in such a scenario and maintains the call.) **Applicable Products:** SBC.
129618	The device sends an alarm to the EMS for dry-contact ports even though the device does not have such ports. **Applicable Products:** Mediant 1000B.
134166	During a three-way call conference, if one of the participants does not speak, the device's Voice Activity Detection (VAD) feature mutes the voice, causing the other participants to hear a "dead air" background, which may be annoying to participants. (The resolved constraint disables noise suppression in conferencing.) **Applicable Products:** All.
133998	The Web interface displays the incorrect TLS certificate expiration date. **Applicable Products:** All.
134058	The output of the CLI command “show system version” shows the BRI interface twice (instead of once). **Applicable Products:** Gateway.

3.9 Patch Version 6.80A.316.005

No new features or constraints for this patch version.

3.9.1 Resolved Constraints

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

Table 3-2: Resolved Constraints for Patch Version 6.80A.316.005

Incident	Description
136572	The device is unable to process calls when a large number of INVITE messages are received at one time, for example, in Shared Call Appearance (SCA) groups. **Applicable Products:** SBC.
136049	When routing is based on LDAP queries, the device cannot perform call forking. **Applicable Products:** All.
135857	For on-board three-way conferencing, the device crashes (resets) after more than three concurrent three-way conferences are handled. **Applicable Products:** FXS Gateways.
136383	When the device tries to make a call with SRTP and the call fails, it initiates alternative routing to a destination that does not require SRTP. However, the device still offers (requires) SRTP. As a result, the call fails. **Applicable Products:** Gateway.
135222	When trying to connect to the device through TLS mutual authentication, the connection fails every second. As a result, calls cannot be made. **Applicable Products:** All.
130988	A "squealing" noise is heard by users in calls from FXO equipment. This occurs when high load (electricity) is detected by the FXO. The bug has been resolved by a new parameter, EnableAnalogOverloadProtection. **Applicable Products:** FXO Gateway.
135236	BRI interfaces using Clearmode codec (transparent) results in BER errors after 12 minutes of the call, thereby posing possible call quality problems. **Applicable Products:** Mediant 500 MSBR; Mediant 800 MSBR.
135732	When the device plays voice announcements, after each new call it doesn't free up DSP resources and as a result, after 20 calls it rejects new ones. **Applicable Products:** Mediant 1000.
134742	If an HA switchover occurs during an established TCP call (SBC) and the call parties later want to end the call, the device does not disconnect the call. This is because the TCP connection (port) changed as a result of the switchover and the device sends the SIP BYE to the wrong destination. **Applicable Products:** HA Devices.
135054	For BRI interfaces where the negotiated payload type for Clearmode (transparent) coder is the same as that configured for RFC 2833, no voice is sent to the Tel side (i.e., one-way voice occurs). A workaround is to configure different payload types for RFC 2833. **Applicable Products:** Gateway.

Incident	Description
135155	Device sends SIP PUBLISH messages with incorrect jitter values (127). **Applicable Products:** All.
133857	The RAM size displayed in the ini file saved from the device is incorrect. **Applicable Products:** All.
135333	When an LDAP query response produces no results (i.e., LDAP_ERR), the device shows the incorrect LDAP attribute in Syslog (even though routing is done correctly). **Applicable Products:** All.
135253	If the user part of the destination URI is missing, the host part is not sent to SEM. As a result, SEM does not report some calls. **Applicable Products:** All.
135102	When doing debug recording by IP trace rule and a filter is set for a specific payload type, the filter does not work. As a result, the device sends all packets (which may cause overload). **Applicable Products:** All.
134866	The device does not send a session timer on SIP 200 OK, but disconnects the SBC call because the session timer expired. A workaround is to disable the session timer. **Applicable Products:** SBC.
135345	When setting the 'Debug Level' parameter for Syslog to **Detailed**, the device crashes (resets). **Applicable Products:** Mediant 4000.
134881	The device does not forward keep-alive STUN messages. Scenario: Lync – SBC – SIP trunk. When Lync puts the call on mute, it sends keep-alive STUN messages, but the device does not forward them to the SIP trunk and after five minutes, the SIP trunk disconnects the call (due to no RTP). To resolve the bug, the new parameter EnableStunForward was added. **Applicable Products:** SBC.
135135	One-way voice occurs in the following call scenario: SRTP call between A and B. B transfers the call to C. If C puts the call with A on hold and then resumes the call, one-way voice occurs. **Applicable Products:** Mediant 3000.

3.10 Patch Version 6.80A.323.002

No new constraints for this patch version.

3.10.1 New Features

The section describes the new features.

3.10.1.1 Local Handling of BRI Call Forwarding

This feature provides support for the device to handle BRI call forwarding (CF) supplementary services locally (according to ETSI 300 207-1). Up until now, the device supported only BRI call forwarding remotely, whereby it sent call forwarding information received from the BRI endpoint to the server which handled the call forwarding process.

To support the feature, the following new parameters have been introduced:

- Supplementary Services table (ISDNSuppServ) has new parameters for defining call forwarding (phone number) - ISDNSuppServ_CFB2PhoneNumber (call forwarding busy), ISDNSuppServ_CFNR2PhoneNumber (call forwarding no reply), ISDNSuppServ_CFU2PhoneNumber (call forwarding unconditional), ISDNSuppServ_NoReplyTime (no reply time).
- BriCallForwardHandling – defines remote (0) or local (1) handling of BRI call forwarding.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000.

3.10.1.2 SIP Proxy Set Keep-Alive Enhancements

This feature provides support for the following Proxy Set keep-alive configuration enhancements:

- Success Detection Retries: If the Proxy Set is offline, the parameter defines the minimum number of consecutive successful keep-alive messages before the device considers the proxy as being online.
- Success Detection Interval: If the Proxy Set is offline, the parameter defines the interval between each keep-alive retries cycle (as defined by the above parameter).
- Failure Detection Retransmissions: Defines the maximum number of UDP retransmissions before the device considers the proxy as offline.
- The Call Routing Status page has been replaced by the new Active Proxy Sets Status page (Monitor menu > Monitor tab > VoIP Status folder > Proxy Sets Status). The page displays the status of all addresses configured for the Proxy Set, including FQDN DNS resolved addresses. The status includes number of keep-alive success and failure attempts as well as proxy server status ("Active", "Standby", "Offline" and "Not Resolved".

Applicable Products: All.

3.10.2 Resolved Constraints

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

Table 3-3: Resolved Constraints for Patch Version 6.80A.323.002

Incident	Description
138017	If an invalid packet is received on a T.38 port, the device incorrectly "reads" the T.38 packet length and as a result, the device crashes (and resets). **Applicable Products:** SBC.
137875	The device matches incoming calls to incorrect IP-to-IP Routing rules when the length of the configured suffix number is longer than the number itself. As a result, calls are routed to the wrong destination. **Applicable Products:** SBC.
137956	The device does not allocate DSP resources correctly when on-board 3-way conferencing occurs and as a result, the maximum number of concurrent 3-way conferencing sometimes cannot be attained and sometimes the device crashes when other FXS lines become active (e.g., off hook). **Applicable Products:** Mediant 5xx; Mediant 8xx; Mediant 1000B.
137842	If the device receives a SIP message, but due to specific conditions there is a failure in allocating raw buffering for the message, the device crashes (and resets). **Applicable Products:** SBC.
137721	If the device receives a SIP INVITE message containing a large SDP, it crashes (and resets). **Applicable Products:** SBC.
137745	For SIPRec, if the prefixes (recorded source or recorded destination) configured in the SIP Recording Rules table is over 50 characters, the device does not send the INVITE message to the recording server and as a result, calls are not recorded. A workaround is to use short prefixes. **Applicable Products:** SIPRec supporting products.
137370	When the parameter ENABLESBCDIALOGINFOINTERWORKING is enabled and the device receives a SIP NOTIFY message containing an XML body that has more than two dialog ID elements, the device crashes (and resets). **Applicable Products:** SBC.
137414	For SIPRec, the unique ID that the device sends to the recording server is incorrect and as a result, calls are not recorded. **Applicable Products:** SIPRec supporting products.

3.11 Patch Version 6.80A.328.004

No new features or constraints for this patch version.

3.11.1 Resolved Constraints

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

Table 3-4: Resolved Constraints for Patch Version 6.80A.328.004

Incident	Description
139564	When calls are received on non-configured B-channels, the device activates the B-channel, but the SID of all calls is the same. This causes problems for debugging. **Applicable Products:** Digital Gateways.
139078	If a call from the PSTN is received without a destination number, the device uses the number plan and type (NPI\TON) from the previous call. As a result, incorrect number format is generated. **Applicable Products:** Digital Gateways.
138038	When configuring SIP message manipulation on the SDP body and the body is configured to be greater than 1,350 characters, the message is sent without the body. As a result, calls fail. **Applicable Products:** SBC.
136942	When disconnecting the WAN cable from the redundant device in the HA pair, no SNMP alarm is sent. **Applicable Products:** HA Products.
138214	If during an SBC call transfer, the device receives a SIP 18x without SDP, it crashes (and resets). **Applicable Products:** HA Products.
138557	The device does not answer ping-pong keep-alive messages over TLS. **Applicable Products:** SBC.
139167	Debug recording rules that include media to file target are not recorded because the media traverses the C5 media processor. As a result, debug recording cannot be performed. A workaround is to use an external capture and not a file target. **Applicable Products:** Mediant 3000.
138986	If the device receives a flash-hook (RFC 2833), it doesn't forward it to the CAS side. **Applicable Products:** CAS Gateways.
13944	The device erroneously reports system warnings to the EMS as yellow color (alert) while on the device they did not appear. **Applicable Products:** All.
138664	When the device is used as an IP media server, it only partially plays requested announcement files. **Applicable Products:** IP Media Servers.
138213	If a long value is configured in the logging filter, the static route and resource priority tables disappear after a switchover and the device can no longer be accessed. A workaround is to configure the static route manually or remove the long filter. **Applicable Products:** HA Products.

Incident	Description
137568	The LDAP cache value is not shown correctly in Syslog messages. **Applicable Products:** All.
137873	When upgrading from Version 6.6 to 6.8, the BRI parameter "EXPLICIT_INTERFACE_ID" (bit from ISDNIBehavior_0 = 512 (EXPLICIT_INTERFACE_ID:512)) is not parsed correctly to Version 6.8 (i.e., incompatible). A workaround is to configure the parameter manually afterward. **Applicable Products:** Digital Gateways.
138564	Major SSL vulnerability problem discovered, causing a security issue. **Applicable Products:** All.
138610	Many watchdog warnings appear in Syslog even though there is no problem. **Applicable Products:** All.
138272	BRI configuration is excluded from the exported CLI script file. A workaround is to configure it through the Web interface. **Applicable Products:** Digital BRI Gateways.

3.12 Patch Version 6.80A.333.004

No new features or constraints for this patch version.

3.12.1 Resolved Constraints

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

Table 3-5: Resolved Constraints for Patch Version 6.80A.333.004

Incident	Description
139815	Some CLI commands fail to load when installing from a Startup script file. A workaround is to configure the parameters manually. **Applicable Products: All**.
137610	The device fails to download the ini file through SNMP. **Applicable Products:** All.
137760	A bug in the way the device handles SRTP results in one-way voice. **Applicable Products:** SBC.
139564	When a call is received on B-channel 31 which is not configured in the Trunk Group, all calls use the same SID. As a result, debug cannot be done for specific calls. A workaround is to configure channel 31 in the Trunk Group. **Applicable Products:** Digital Gateway.
140986	When the device receives "garbage" packets, it crashes (resets). **Applicable Products:** SBC.
139713	If the device receives a SIP 183 with 'sendonly' and then a SIP 200 OK with 'sendonly', it sends a re-INVITE and tries to allocate DSP resources even though there aren't any available and DSP resources are not required. As a result, the call fails. A workaround is to add the 'telephony-event' to the incoming 200 OK that is received after the re-INVITE. **Applicable Products:** SBC.
139784	Number manipulation is executed before Call Setup Rules even though it was configured to execute after CSR. As a result, the wrong number occurs. **Applicable Products:** Gateway.
140145	Due to a bug in calculation, incorrect MOS scores are reported by the device to SEM. **Applicable Products:** All.

3.13 Patch Version 6.80A.338.003

No new features or constraints for this patch version.

3.13.1 Resolved Constraints

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

Table 3-6: Resolved Constraints for Patch Version 6.80A.338.003

Incident	Description
142121	The device issues a CPU overload alarm even though there is no overload. **Applicable Products:** Gateway.
139823	When certain messages are received from the PSTN, the device crash (resets). **Applicable Products:** Gateway.
140656	Performance monitoring MIB for packet loss shows incorrect values. **Applicable Products:** Gateway.
142580	The proxy keep-alive feature using REGISTER messages does not function. As a result, the proxy is indicated as offline and calls are not routed to it. **Applicable Products:** All.
142381	The device crashes (resets) due to incorrect randomization method of code. **Applicable Products:** SBC.
141608	When using SIP overlap dialing, the device does not send the "to-tag" in ACK messages. As a result, the call fails. **Applicable Products:** Gateway.
141899	When using LDAP-based login over TLS, the device crashes (resets). A workaround is not to use TLS. **Applicable Products:** All.
140774	When a server attempts to download a file to the device, the device crashes (resets). **Applicable Products:** All.
141174	When the device uses the SAS application and receives a large number of REGISTER requests in a short time span, the device freezes. **Applicable Products:** SAS.

3.14 Patch Version 6.80A.346.005

This patch includes new features and resolved constraints.

3.14.1 New Features

The section describes the new features.

3.14.1.1 Removing "sips:" on Unsecured SBC Leg

This feature provides support for enabling the device to replace the "sips:" URI scheme with "sip:" for the following SIP headers in the outgoing SIP-initiating dialog request when the destination transport type is unsecured (e.g., UDP): Request-URI, Contact, From, To, P-Asserted, P-Preferred, and Route headers. Up until now (and when the feature is disabled), the device performs this only on the Request-URI and Contact headers. (The "sips:" URI scheme indicates secured transport, for example, TLS.)

The feature is enabled using the new parameter, SBCRemoveSIPSFromNonSecuredTransport.

Applicable Applications: SBC.

Applicable Products: All.

3.14.2 Resolved Constraints

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

Table 3-7: Resolved Constraints for Patch Version 6.80A.346.005

Incident	Description
143806	The device does not play a ringback tone (from the installed Pre-recorded Tone file) to a destination on the WAN through the RMX. **Applicable Products:** MSBR in Single Network Mode.
144383	Large number of Busy Lamp Field (BLF) NOTIFY messages cause a lack of resources and as a result, the device is unable to handle the NOTIFY messages. **Applicable Products:** SBC.
144875	The host name configured in tables (e.g., Classification table) is case sensitive and thus, if the case is not the same, classification fails and as a result, the device does not register the users (far-end users) **Applicable Products:** SBC.
144183	If a call is not established due to 'unassigned number', the device erroneously reports to the SEM that the call has failed. **Applicable Products:** SBC.
144597	The device crashes (and resets) when it receives two REGISTER requests for the same SIP dialog (where the second REGISTER is received before the first one gets a response). **Applicable Products:** SBC.
143700	The device does not update the voice stream after it sends a SIP 183 with SDP and 200 OK with SDP. As a result, no voice occurs. **Applicable Products:** SBC.

Incident	Description
143760	Even if the License Key is the same on both devices in the HA system, the device sends a License Key mismatch alarm. **Applicable Products:** SBC HA.
143755	The creation of a new TLS connection causes device memory leaks and after a while, the TLS connection fails. **Applicable Products:** All.
142196	Certain SIP messages do not appear in the Web interface's message log. **Applicable Products:** All.
141745	The passwords configured in the Account table appear in SNMP in clear text, thus posing a security risk. **Applicable Products:** All.
142950	If the device receives a SIP REFER message before all media synchronizes, the call transfer fails. **Applicable Products:** SBC.
142525	The device crashes (and resets) when BRI CFU deactivation is performed through the BRI phone. **Applicable Products:** Gateway (BRI).

3.15 Patch Version 6.80A.348.001

This patch includes only resolved constraints.

3.15.1 Resolved Constraints

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

Table 3-8: Resolved Constraints for Patch Version 6.80A.348.001

Incident	Description
152106	When running the SAS application, the device crashes / resets (GetIncomingTransportObject) when the device forwards REGISTER requests to a server and then a "race" occurs between several types of events. **Applicable Products:** SAS Products.
150574	When the device uses the IP-media feature NetAnn (conferencing), instead of sending the SIP 18x and 200 OK with an empty user part in the Contact header, it includes "playFrom_early" and the address of the WAV file as the user part in the Contact header. **Applicable Products:** Mediant 1000.
147080	When the device is configured to route the call to an ENUM server, if the regular expression (regex) defined on the ENUM server for a specific user is empty (i.e., invalid), the device crashes (resets) after performing the ENUM query. **Applicable Products:** SBC Products.

This page is intentionally left blank.

4 MSBR Series

This chapter describes new features, known constraints and resolved constraints relating to MSBR functionalities.

4.1 Version GA

This section describes new features, known constraints and resolved constraints in the GA version.

4.1.1 New Features

This section describes new features.

4.1.1.1 DHCP Option 121 as a DHCP Client

This feature provides support for DHCP Option 121 (Classless Static Route) when the device is configured as a DHCP client. This option, sent by the DHCP server, provides the device with static routes, each of which consists of a destination descriptor and the IP address of the router that should be used to reach that destination. The static routes are automatically added to the device's Static Route table.

Note: This option is already supported when the device acts as a DHCP server.

Applicable Products: Mediant MSBR.

4.1.1.2 DHCP Options 120 and 43 as DHCP Server in Lync Deployments

This feature provides support for the AudioCodes' device to act as a DHCP server for AudioCodes' Lync-enabled IP phones, by supporting DHCP Options 120 and 43. DHCP Option 120 enables SIP clients to discover a domain name system (DNS) FQDN (Fully-Qualified Domain Name) of a SIP server (SIP Server Discovery). For detailed information on DHCP Option 120, see RFC 3361. DHCP Option 43 enables devices to discover the Microsoft Lync Server Certificate Provisioning service. For detailed information on how to configure DHCP Option 120 and DHCP Option 43, see http://technet.microsoft.com/en-us/library/gg412828%28v=ocs.14%29.aspx.

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

```
# ip dhcp-server sip-server <FQDN of SIP server – Option 120)
# ip dhcp-server lync-cert-provisioning <Microsoft Lync Server
Certificate Provisioning service – Option 43>
```

For example:

```
# ip dhcp-server sip-server sip.customer.com
# ip dhcp-server lync-cert-provisioning lync.customer.com
```

The `lync-cert-provisioning` command accepts either an FQDN of the enterprise's Lync server or a full URL such as https://lync.customer.com:443/CertProv/CertProvisioningService.svc.

Applicable Products: Mediant MSBR.

4.1.1.3 Automatic xDSL and SHDSL Settings to Match Far End

This feature provides support for automatic xDSL and SHDSL settings in order to match those of the far-end side:

- When configured for SHDSL, the device automatically changes between Ethernet in the first mile (EFM) and Asynchronous Transfer Mode (ATM) to suit the far-end side. For example, if the device is configured with ATM and is connected to a far-end side configured with EFM, the device automatically switches to EFM.
- When configured for DSL, the device automatically changes between ADSL and VDSL to suit the far-end side. For example, if the device is configured with ADSL and is connected to a far-end side with VDSL, the device automatically switches to VDSL.

Note: Mediant 1000B supports only SHDSL.

Applicable Products: Mediant MSBR.

4.1.1.4 Reassembly of Fragmented IP Packets

This feature provides support for defragmenting received fragmented IP packets from an interface and then reassembling the packets before forwarding them. The Wireshark packet analyzer is typically used to identify fragmented frames.

To support this feature, the following new CLI command has been added under a data-router interface:

```
# [no] ip reassembly
```

This capability is applied per interface and therefore, the CLI command must be set for the relevant IP interface. By default, this capability is disabled per interface.

For example:

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# ip reassembly
```

Applicable Products: Mediant MSBR.

4.1.1.5 Dynamic Routing with Virtual Routing and Forwarding (VRF)

This feature provides support for implementing dynamic routing protocols (BGP, OSPF and RIP) with Virtual Routing and Forwarding (VRF) tagging. Up until now, dynamic routing could not be configured with VRF tagging. One BGP, one OSPF, and one RIP protocol can be enabled per VRF table. Up to five dynamic routing protocols can be enabled in all defined VRF tables.

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

- Enables a dynamic routing protocol on a VRF:

  ```
  (config-data)# [no] ip vrf <vrf-name> [enable bgp|ospf|rip]
  ```

- Specifies the router ID (as an IP address) and optionally associates it with a VRF:

  ```
  (config-data)# router-id <IP address> [vrf <VRF name>]
  ```

- Enables dynamic routing protocol associated with a VRF:

  ```
  (config-data)# router bgp|ospf|rip [vrf <VRF name>]
  ```

- Configures the order'th entry in route map name with match policy of permit or deny, associated with a VRF:

  ```
  (config-data)# route-map <route map name> [vrf <VRF name>]
  deny|permit <order or sequence number of route map>
  ```

- Configures prefix-based filtering mechanism associated with a VRF:

  ```
  (config-data)# ip prefix-list <name> [vrf <VRF name>] [seq
  <prefix-list seq number>] permit|deny <prefix to filter> [le
  <len>] [ge <len>]
  ```

le <len>: prefix list is applied if the prefix length is less than or equal to the le prefix length

ge <len>: prefix list is applied if the prefix length is greater than or equal to the le prefix length

- Configures the key string for RIPv2 authentication and associates it with a VRF:

```
(config-data)# key chain <name> [vrf <VRF name>]
```

The following new show CLI commands have also been added:

- Displays dynamic routing protocol routes associated with a VRF:

```
# show data ip bgp|ospf|rip [vrf <VRF name>]
```

- Displays configured prefix-list associated with a VRF:

```
# show data ip prefix-list <name> [vrf <VRF name>]
```

- Displays configured route-map associated with a VRF:

```
# show data route-map <name> [vrf <VRF name>]
```

- Removes peers of the specified peer associated with a VRF:

```
# clear ip [vrf <VRF name>] bgp <peer - ip address or AS
number of peer>
```

- Clears the counters on prefix-list associated with a VRF:

```
# clear ip [vrf <VRF name>] prefix-list <name> [A.B.C.D/M]
```

< A.B.C.D/M>: optional prefix address

- Debugs dynamic routing protocol routes associated with a VRF:

```
# debug bgp|ospf|rip|zebra [vrf <VRF name>]
```

Applicable Products: Mediant MSBR.

4.1.1.6 Enable and Disable Wi-Fi Functionality

This feature provides support for enabling or disabling Wi-Fi functionality. This can be done by the following:

- New Wi-Fi button, located on front panel, to enable and disable Wi-Fi hardware interface.
- New CLI command to enable and disable the Wi-Fi interface:
  - Enable Wi-Fi:

```
(config-data)# radio shutdown
```

  - Disable Wi-Fi:

```
(config-data)# no radio shutdown
```

Applicable Products: Mediant 500 MSBR; Mediant 800/B MSBR.

4.1.1.7 IEEE 802.1p Priority Marking of Bridged Traffic

This feature provides support for scenarios where the device is used as a bridging device (Layer 2) and IEEE 802.1p priority marking for the bridged traffic is required. When this feature is used, outgoing packets belonging to a specified VLAN interface are marked with the configured priority value. Up until this release, packets could only be marked according to separately defined queues (QOS Match-Map option).

To support this feature, the following CLI commands are used to assign priority levels per interface:

```
(config-data)# interface <interface_type> <interface_ID>
(conf-if-VLAN 1)# priority <priority level>
```

Where *priority level* can be any value from 0 (lowest) through 7 (highest).

Note: 802.1p priority marking for bridged traffic cannot be configured using the QOS Match-Map menu options (existing from previous releases). However, in a Layer 3 configuration, this menu option can be used. If both methods are used to configure 802.1p priority marking, the settings done through the QOS Match-Map menu takes precedence.

Applicable Products: Mediant MSBR.

4.1.1.8 Application Binding to Data-Router Interfaces

This feature provides support for enabling the connection to a specified application through a specific data-router interface (or all VRFs) on the device. These applications can include, for example, Web interface, Telnet, SSH, TR-069, SNMP, Syslog, NTP, and file download using the copy command. For example, the device's SNMP agent can be configured to be available from the WAN network (which is connected to the device's WAN interface). Up until this release, these applications could be reached only through the OAMP interface, which was on the voice module.

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

- Application (e.g., OAMP) is available ("binded") through a specified interface:

```
(config-system)# bind interface <interface name> oamp
```

- Application (e.g., OAMP) is available ("binded") through a specified VRF:

```
(config-system)# bind vrf <VRF name> oamp
```

- Application (e.g., OAMP) is available ("binded") through all VRFs:

```
(config-system)# bind vrf all-vrfs oamp
```

- Application available through a source IP address (outgoing packets will have this source address):

```
(config-system)# bind source-address interface <interface
name>
```

Applicable Products: Mediant MSBR.

4.1.1.9 SNMP Trap Binding to Source Address or VRF

This feature provides support for binding SNMP trap requests to a source address or VRF. In other words, the administrator can specify from which data interface (address or VRF) to send the traps (as an SNMP client) to the SNMP manager.

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

- To bind SNMP traps to a source address:

```
(config-system)# snmp
(snmp)# bind source-address interface <interface name> trap-
pdu
```

- To bind SNMP traps to a VRF:

```
(config-system)# snmp
(snmp)# bind vrf <VRF name> trap-pdu
```

Applicable Products: Mediant MSBR.

4.1.1.10 Source-based Static IP Routing

This feature provides support for configuring source-based static IP routing to specific destinations. Source-based routing can include VLANs and is applicable only to IPv4.

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

```
(config-data) # ip route source <IP address/prefix length or
subnet mask > destination <IP address/prefix length or subnet
mask> gateway <IP address>
```

For example:

```
(config-data) # ip route source 10.3.0.0/16 destination 0.0.0.0/0
gateway 10.4.0.1
(config-data) # ip route source 2.2.2.2 255.255.255.255
destination 10.31.0.0 255.255.0.0 192.168.0.100 VLAN 1
```

Note: Source-based routing must not be configured with dynamic route protocols.

Applicable Products: Mediant MSBR.

4.1.1.11 Forwarding DNS Queries to DNS Server based on Source

This feature provides support for enabling the device to reply to DNS queries using direct queries to specific DNS servers. This feature configures the device as a DNS server, and forwarder for DNS queries from hosts.

The device implements this feature by configuring *DNS views*, which defines the DNS queries based on source address and the DNS server to which the device must forward these specific queries. If a query does not meet the conditions of any of the DNS views, the device forwards the query to all DNS servers (as done up until this release). In addition, DNS queries received from the device's VoIP (internal) interfaces are forwarded to all DNS servers.

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

- Defines a DNS view:

  ```
  (config-data)# dns-view <view name>
  ```

- Defines the DNS queries by source address for the DNS view:

  ```
  (dns-view <view name>)# match source address <source IP
  address of DNS query> <source netmask of DNS query>
  ```

- Defines the interface associated with the DNS server:

  ```
  (dns-view <view name>)# set server interface <interface name>
  ```

  Where *interface name* is the name of the interface that is configured with the desired DNS server (static or dynamic). This allows configuration of name servers received dynamically by DHCP or PPP.

- Defines the DNS server to where the queries matching this DNS view are forwarded:

  ```
  (dns-view <view name>)# set server address <server IP address>
  ```

  The *server IP address* is one of the device's DNS server's IP address (configured as part of an interface properties); otherwise, the device will not forward to it.

The DNS-views can be displayed using the `show running-config` command, which can list up to 20 DNS-views. For each DNS-view, the first 5 matches and the first 5 actions (set) are displayed (if there are more than this, they can be viewed in the Syslog).

Applicable Products: Mediant MSBR.

4.1.1.12 SMS Text Messaging through 3G Cellular Modem

This feature provides support for sending an SMS text message through a 3G cellular connection. Cellular connectivity is achieved by attaching a third-party, 3G cellular modem to the device's USB port.

To support this feature, the following new CLI command has been added under the cellular interface:

```
(conf-cellular)# sms <mobile-number> "<message text>"
```

The message can include up to 127 characters and must be enclosed in double quotes (").

For example:

```
(config-data)# interface cellular 0/0
(conf-cellular)# shutdown
(conf-cellular)# sms 0546342171 "Hello John Doe!"
```

Applicable Products: Mediant MSBR.

4.1.1.13 IPv6 Support

This feature provides support for IPv6 (voice and data-routing functionalities) on the MSBR product series. This support is provided only if the Software License Key installed on the device includes the new Feature Key "IPv6" for enabling IPv6.

Note that IPv6 is already supported on Mediant 800 E-SBC, Mediant 1000 E-SBC, Mediant 3000, and Mediant Non-Hybrid SBC.

Applicable Products: Mediant MSBR.

4.1.1.13.1 Enable IPv6 per Data-Router Interface in CLI

This feature provides support for enabling IPv6 per data-router interface. Up until now, if the Software License Key, installed on the device, included the IPv6 feature key, IPv6 was enabled for all interfaces and could not be disabled (unless a new Software License Key without IPv6 was subsequently installed).

When the IPv6 feature is included in the Software License Key, IPv6 is disabled per interface, by default. An IPv6-disabled interface will not have global IPv6 addresses enabled, nor will it have link-local addresses. In addition, the `show data ipv6 route` command does not display routes of IPv6 interfaces that are disabled, but the interface is displayed by the `show running config` command. Configuration of IPv6 addresses can be done at any stage, but will only be active if IPv6 is enabled on the required interface.

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

```
# [no] ipv6 enable
```

For example:

```
(config-data)# interface gigabitethernet 0/0
(config-if-GE 0/0)# ipv6 address 2010:18::40:81/640
(config-if-GE 0/0)# ipv6 enable
```

Applicable Products: Mediant MSBR.

4.1.1.13.2 IPv6 Static Routes

This feature provides support for configuring IPv6 static routes (destination prefix). To support this feature, the following new CLI commands have been added:

```
(config-data)# ipv6 route [vrf <VRF name>] <IPv6 destination
address>/<prefix> [<IPv6 gateway address>] <interface name>
<interface ID> [<distance value>]
```

- *distance value*: priority (0 to 255) of the route in the routing table (the smaller the value, the higher the priority of the route).

- *interface name*: can be one of the following:
  - bvi: Bridge interface
  - cellular: Cellular 3G interface
  - gigabitethernet: Gigabit Ethernet interface
  - gre: GRE tunnel interface
  - ipip: IPIP tunnel interface
  - l2tp: L2TP tunnel interface
  - loopback: PPPoE interface
  - pppoe: PPPoE interface
  - pptp: PPTP tunnel interface
  - vlan: VLAN interface
  - vti: VTI tunnel interface

For example:

```
(config-data)# ipv6 route 2001:10::/64 2050:8:: GigabitEthernet
0/0 1
```

The IPv6 static route can be displayed using the regular `show running-config` command or the following new IPv6 command:

```
# show data ipv6 route [<ipv6-address[prefix]>] [connected]
[kernel] [static] [summary]
```

Note that IPv6 support is available only if the installed Software License Key contains the IPv6 Feature Key.

Applicable Products: Mediant MSBR.

4.1.1.13.3 Acquiring IPv6 Address from DHCPv6 Server

This feature provides support for configuring the device as a DHCPv6 client to obtain an IPv6 address from a DHCPv6 server, according to RFC 3315. The device as a DHCPv6 client also supports the Rapid Commit option. This option lets the device quickly obtain configuration parameters from the DHCP server through a rapid two-message exchange (solicit, reply), instead of the usual four-message exchange (solicit, advertise, request, reply). Note that Rapid Commit must be supported and enabled on the DHCP server as well.

To support this feature, the following new CLI command has been added to enable DHCPv6 per interface:

```
(conf-if-GE 0/0)# ipv6 address dhcp [rapid-commit]
```

The received IPv6 address can be viewed using the existing command, `show data interfaces <interface>`.

To disable this feature, the following command is used:

```
(conf-if-GE 0/0)# no ipv6 address
```

Note: For this feature, the installed Software License Key must contain the IPv6 Feature Key.

Applicable Products: Mediant MSBR.

4.1.1.13.4 Acquiring IPv6 Address Automatically via Router Advertisement

This feature provides support for automatically acquiring an IPv6 address using stateless auto-configuration on a specified WAN interface. This is instead of using a DHCPv6 server for acquiring an IPv6 address.

When this feature is enabled, the device waits for a router advertise (RA) message from the router. When received, the device generates its own address using a combination of locally available information and information received in the RA message. The RA message contains prefixes that identify the subnet(s) associated with a link, while the device

generates an "interface identifier" that uniquely identifies an interface on a subnet. A global address is formed by combining the two. In the absence of routers, the device can only generate link-local addresses. However, link-local addresses are sufficient for allowing communication among nodes attached to the same link.

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

```
(conf-if-GE 0/0)# ipv6 address autoconfig
```

Applicable Products: Mediant MSBR.

4.1.1.13.5IPv6 Router Advertisement Daemon

This feature provides support for the Router Advertisement Daemon for automatic configuration of IPv6 addresses, according to RFC 4861. The IPv6 Router Advertisement (RA) implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes, using the Neighbor Discovery Protocol (NDP), as specified in RFC 4861. The RA process is used for stateless auto-configuration of network hosts on IPv6 networks.

When IPv6 hosts (for example, PCs) configure their network interfaces, they broadcast router solicitation (RS) requests to the network to discover available routers. The device answers these requests with RA messages. The device also periodically broadcasts RA packets to the attached link to update the network hosts. The RA messages contain the routing prefix used on the link, the link maximum transmission unit (MTU), and the address of the responsible default router. From this information, the hosts can automatically configure their IPv6 addresses.

The device can be configured as an RA advertiser or RA solicitor. In case of the latter, the device serves only as a host and thus, does not send RA messages.

IPv6 nodes on the same link use NDP to discover each other's presence to determine each other's link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors.

- NDP (under interface command):
  - Sets advertised "Managed address configuration" flag, which indicates hosts should use DHCPv6 for address configuration - the [no] option sets to default (0):
    ```
    # [no] ipv6 nd managed-config-flag
    ```
  - Sets advertised "Other configuration" flag (indicates hosts should use DHCPv6 for non-IPv6 address, e.g., NTP address) - the [no] option sets to default (0):
    ```
    # [no] ipv6 nd other-config-flag
    ```
  - Sets advertised “Retrans Timer” (interval between retransmitted Neighbor Solicitation messages) value - the [no] option sets to default (0 - disables retransmit advertisements):
    ```
    # [no] ipv6 nd ns-interval <1000-3600000 msec>
    ```
  - Sets advertised “Reachability time” (time a neighbor is considered reachable after receiving a reachability confirmation) value - the [no] option sets to default (0):
    ```
    # [no] ipv6 nd reachable-time <0-3600000 msec>
    ```
  - Sets advertised “Router preference” value - [no] option sets to default (Medium):
    ```
    # [no] ipv6 nd router-preference <High|Low|Medium
    (default)>
    ```
- RA (under nd subcommand):
  - Removes the RA parameters from database:
    ```
    # no ipv6 nd ra
    ```
  - Suppresses IPv6 RA (default):
    ```
    # ipv6 nd ra suppress
    ```
  - Enables IPv6 RA:
    ```
    # no ipv6 nd ra suppress
    ```
  - Sets advertised “Router Lifetime” value:

```
# ipv6 nd ra lifetime <0-9000 sec (default 1800)>
```

- Sets IPv6 RA maximum interval:

```
# ipv6 nd ra interval <4-1800 sec>
```

Note: The minimum interval is set to 0.33 x maximum interval.

- Sets IPv6 RA minimum and maximum intervals:

```
# ipv6 nd ra interval <4-1800 sec> <[3-(0.75*MaxRAInterval) sec]>
```

- IPv6 Routing Prefix Advertisement:
  - Sets IPv6 prefix with defaults:

```
# ipv6 nd prefix <prefix>
```

  - Sets IPv6 prefix:

```
# ipv6 nd prefix <prefix> <valid lifetime> <preferred lifetime> <no-advertise> <on-link|off-link> <no-autoconfig|autonomous>
```

    - *valid lifetime*: 0-4294967295 sec (default 86400). Can have the symbolic value 'infinity'.
    - *preferred lifetime*: 0-4294967295 sec (default 14400). Can have the symbolic value 'infinity'.
    - *off-link*: Do not use prefix for on-link determination.
    - *no-autoconfig*: Do not use prefix for auto-configuration.

    Notes:
    - The IPv6 prefix must be /64.
    - The parameter off-link and no-autoconfig can appear in any combination. Both parameters can have the symbolic value 'infinity'.
  - Removes the prefix from database:

```
# no ipv6 nd prefix
```

  - Saves this prefix, but does not advertise it - [no] option means the device advertises the prefix (default):

```
# [no] ipv6 nd prefix <X:X:X:X::> no-advertise
```

Note: For this feature, the installed Software License Key must contain the IPv6 Feature Key (i.e., enabled).

Applicable Products: Mediant MSBR.

4.1.1.13.6 IPv6 for DNS

This feature provides support for the device's Domain Name System (DNS) proxy to operate over IPv6 interfaces. In addition to supporting IPv6 clients, DNS name-servers may now be configured with IPv6 addresses. Mixing of IPv4 and IPv6 is supported, such that an IPv4 client may query the DNS server for a name which will be resolved by an IPv6 name-server on another interface, and vice versa.

Applicable Products: Mediant MSBR.

4.1.1.13.7 IPv6 for Automatic Updates

This feature provides support for using IPv6 addresses for the Automatic Update mechanism. This applies to the remote server (e.g., HTTP server) on which the software files are located and from where the device downloads them (or HTTP Redirect server). The URL of the server can include an IPv6 address or a host name (FQDN) which is resolved into an IPv6 address by a DNS server.

The configured IPv6 URL must be enclosed in square brackets:

- URL with host name (FQDN) for DNS resolution into an IPv6 address:

```
http://[FQDN]:<port>/<filename>
```

- URL with IPv6 address:

```
http://[IPv6 address]:<port>/<filename>
```

Below is a configuration example for Automatic Update using IPv6:

```
(automatic-update)# firmware
http://[2000::1]:80/F6.80A.222.0070.cmp
```

Note: IPv6 for FTP servers is not supported.

Applicable Products: Mediant MSBR.

4.1.1.13.8 IPv6 for Syslog Server

This feature provides support for configuring the Syslog server with an IPv6 address. This is applicable only when communicating with the Syslog server through the device's WAN interface (not LAN).

Applicable Products: Mediant MSBR.

4.1.1.13.9 IPv6 Ping Support

This feature provides support for performing a ping from an IPv6 data-router interface to an IPv6 destination address in order, for example, to test network connectivity. This support also extends to Virtual Routing and Forwarding (VRF) interfaces. Up until this release, ping was supported only for IPv4 addresses.

To support this feature, the `ipv6` subcommand has been added to the existing `ping` command:

```
# ping ipv6 <IPv6 address or host name> source data [vrf | source-
address interface| interface] [size <max. IP packet size>] [repeat
<1-300>]
```

For example:

```
# ping ipv6 2001:15::300 source data vrf VOIP
```

Note: IPv6 ping is currently only supported on Ethernet and Fiber interfaces.

Applicable Products: Mediant MSBR.

4.1.1.13.10 IPv6 for Traceroutes

This feature provides support for performing a traceroute. Traceroute is a diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network.

The command supports both IPv4 and IPv6 addresses. In IPv4, it supports hostname resolution as well. The command sends three requests to each hop on the way to the destination.

To support this feature, the following new CLI command (run from the root level) has been added:

```
# traceroute ipv6 <X:X::X:X> [vrf <vrf name>]
# traceroute <A.B.C.D or hostname> [vrf <vrf name>]
```

Examples:

- IPv6:

```
# traceroute ipv6 2014:6666::dddd
1  2014:7777::aa55 (2014:7777::aa55)  2.421 ms  2.022 ms
2.155 ms
2  2014:6666::dddd (2014:6666::dddd)  2.633 ms  2.481 ms
2.568 ms
Traceroute: Destination reached
```

- IPv4:

```
# traceroute 10.3.0.2
```

```
1   1 (10.4.0.1)   2.037 ms   3.665 ms   1.267 ms
2   1 (10.3.0.2)   1.068 ms   0.796 ms   1.070 ms
Traceroute: Destination reached
```

Applicable Products: Mediant MSBR.

4.1.1.13.11 IPv6 VRF

This feature provides support for IPv6 VRF, supporting static routes in IPv6 VRF, extending providers' VRF technology to the device. IPv6 VRF supports multiple, intersecting, independent routing and forwarding tables per enterprise customer.

The VRF new feature also supports the following:

- Packet forwarding between IPv6 interfaces within the same VRF
- Configuration of IPv6 static routes within each VRF
- IPV6 dynamic routing
- IPv6 ping
- IPv6 traceroute
- IPv6 static route

New CLI commands:

```
(config-data)# ipv6 route [vrf <vrf name>] <destination prefix>
[<gw address>] <interface name> [metric] [track <id>]
```

IPv6 static routes in VRFs can be viewed using the following command:

```
# sh run
```

IPv6 VRF routing tables can be viewed using the following command:

```
# show data ipv6 route [vrf <vrf name>] [connected|static|…]
```

Applicable Products: Mediant MSBR.

4.1.1.13.12 Dynamic Routing Protocols (BGP, OSPF, and RIP) over IPv6

This feature provides support for dynamic routing protocols over IPv6. Dynamic routing protocols include Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

The following new CLI commands were added for this IPv6 support:

- RIP:
  - Show commands:

    ```
    # show data debugging ripng
    # show data ipv6 ripng
    # show data ipv6 ripng status
    # show data ipv6 route
    ```

  - Debug commands:

    ```
    # debug ripng events
    # debug ripng packet
    # debug ripng zebra
    ```

  - General configuration commands:

    ```
    (config-data)# router ripng
    (conf-router)# redistribute [bgp | connected | kernel |
    ospf6 | static] metric <0-16> route-map <string>
    aggregate-address [X:X::X:X/M]
    route-map [rmap_name] [in|out] [interface]
    ```

- OSPF:

- Debugs commands:

```
# debug [vrf <vrf name>] ospf6 lsa [as-external | inter-
prefix | inter-router | intra-prefix | link | network |
router | unknown] [examin| flooding | originate]
# debug [vrf <vrf name>] ospf6 abr
# debug [vrf <vrf name>] ospf6 asbr
# debug [vrf <vrf name>] ospf6 border-routers
# debug [vrf <vrf name>] ospf6 flooding
# debug [vrf <vrf name>] ospf6 interface
# debug [vrf <vrf name>] ospf6 message
# debug [vrf <vrf name>] ospf6 neighbor
# debug [vrf <vrf name>] ospf6 route
# debug [vrf <vrf name>] ospf6 spf
# debug [vrf <vrf name>] ospf6 zebra
```

- Show commands:

```
# show data debugging [vrf <vrf name>] ospf6
# show data ipv6 ospf6 [vrf <vrf name>] [area | border-#
routers | database | interface | linkstate | neighbor |
redistribute | route | simulate | spf | vrf]
# show data ipv6 route [vrf <vrf name>] ospf6
```

- General configuration commands:

```
(config-data)# router ospf6
(conf-router)# area <Area-ID> filter-list prefix <prefix-
name> [in|out]
(conf-router)# area < Area-ID> range <X:X::X:X/M>
[advertise | not-advertise]
(conf-router)# interface <interface> area <area-ID>
redistribute [bgp | connected | kernel | ripng | static]
route-map <route-map>
```

Applicable Products: Mediant MSBR.

4.1.1.13.13 Display of IPv6 Neighbor Discovery (ND) Cache Table

This feature provides support for displaying IPv6 neighbor discovery (ND) cache information. To support this feature, the following new CLI command has been added:

```
# show data ipv6 neighbors
```

For example:

```
IPv6 Address                 Age Link-layer Addr State Interface
FE80::290:8FFF:FE4A:230D           0 0090.8f4a.230d  STALE Gi0/0
FE80::4637:E6FF:FE32:9D1           0 4437.e632.09d1  REACH Gi0/0
2010:3::90:52                      0 4437.e632.09d1  REACH Gi0/0
2010:3::40:81                      0 0090.8f4a.230d  STALE Gi0/0
```

Applicable Products: Mediant MSBR.

4.1.1.13.14 Display of IPv6 Addresses

This feature provides support for displaying IPv6 addresses.

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

- Displays IPv6 prefixes:

```
# show data ipv6 prefix-list <name> [vrf <VRF name>]
```

- Clears IPv6 information:

```
# clear ipv6 prefix-list
```

Applicable Products: Mediant MSBR.

4.1.1.14 Security Features

This section describes the new data-router security features.

4.1.1.14.1 802.1X LAN Port-based Authentication

This feature provides support for functioning as an IEEE 802.1X authenticator. IEEE 802.1X (EAP-over-LAN, or EAPOL) is a standard for port-level security on secure Ethernet switches (wired or wireless); when equipment is connected to a secure port, no traffic is allowed until the identity of the equipment is authenticated.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server (e.g., supporting RADIUS and EAP protocols). The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The AudioCodes device is the authenticator, acting as a secure Ethernet switch and wireless access point.

The authenticator acts like a security guard to a protected network. The supplicant is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. The supplicant provides credentials such as username / password or digital certificate to the authenticator, and the authenticator forwards the credentials (encapsulated in RADIUS Access-Request packets) to the authentication server for verification. The authenticator communicates with the supplicant using EAP-over-LAN frames (containing protocols such as EAP-MD5, Protected EAP, or EAP-TLS). If the authentication server determines the credentials are valid, it instructs the AudioCodes device to allow the supplicant full access to the protected side of the network.

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

- Enables 802.1X LAN port authentication:

```
(config-data)# [no] dot1x lan-authentication
```

- Defines the RADIUS server for 802.1X authentication:
  - External RADIUS server:

```
(config-data)# dot1x radius-server host 10.3.4.250 auth-
port 1812 key 123456
```

  - On-board RADIUS server:

```
(config-data)# dot1x radius-server local
```

- Following a successful authentication, each port is re-authenticated after a user-defined interval (in seconds):

```
(config-data) # dot1x reauth-time 3600
```

- Determines which client (based on MAC address) is allowed through a specific port after 802.1X authentication succeeds:

```
(config-data)# interface GigabitEthernet 4/2
(conf-if-GE 4/2)# [no] authentication dot1x <single-host |
multi-host>
```

  Where:
  - single-host = Only the MAC address that successfully passed the 802.1x authentication is allowed
  - multi-host = Any MAC address is allowed after 802.1x authentication succeeds

  An alternative to the above option is to manually enter the MAC addresses that are permitted access to the port.

- Displays 802.1X port status:

```
# show data dot1x-status
```

  For example:

```
Port    Auth      State         Timeout Username
----    ----      -----         ------- --------
  1     Disabled  Idle                0
  2     Enabled   Forwarding         75 John
  3     Disabled  Idle                0
  4     Disabled  Idle                0
```

Note: The RADIUS server must be configured for EAP.

Applicable Products: Mediant MSBR.

4.1.1.14.2 On-board RADIUS Server for 802.1X Authentication

This feature provides support for an on-board RADIUS server that can be used for 802.1X wired (LAN) and wireless (Wi-Fi Protected Access II / WPA2 Enterprise) authentication. This supports both password-based authentication and certificate-based authentication.

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

- Defines username and password:

```
(config-data)# dot1x local-user <username> password <password>
```

- Wireless:
  - Defines Wi-Fi interface:

```
(config-data)# interface dot11radio 1
```

  - Enables on-board RADIUS server for 802.1X security:

```
(config-if-dot11radio 1)# security 802.1x radius server
local
```

  - Enables Wi-Fi security mode

```
(config-if-dot11radio 1)# security wpa mode 802.1x
```

  - Defines Wi-Fi security mode to WPA2:

```
(config-if-dot11radio 1)# security mode wpa2
```

  - Enables the interface:

```
(config-if-dot11radio 1)# no shutdown
```

- 802.1X LAN port authentication (wired):
  - Enables local RADIUS server:

```
(config-data)# dot1x radius-server local
```

  - See Section 3.1.1.99 for the full configuration.

Applicable Products: Mediant MSBR.

4.1.1.14.3 Port Security based on MAC Address

This feature provides support for port access security based on MAC address. Only clients whose MAC addresses are defined for the device's port interface are allowed access to the port.

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

```
# [no] authentication static [mac <MAC address as
xx:xx:xx:xx:xx:xx>|auto]
```

In auto mode, the device authorizes the first MAC address to access the Ethernet port. Once this address is learned, the administrator should use the `write` command to save it to the configuration. If the device restarts at any later stage, the interface does not need to relearn these addresses. If you do not save the configuration, the device will repeat the learning process after restarting.

The example below defines a MAC address to allow access to one of the device's interfaces:

```
(config-data)# interface GigabitEthernet 4/4
```

```
(config-if-GE 4/4)# authentication static mac 01:23:45:67:89:ab
```

Applicable Products: Mediant MSBR.

4.1.1.14.4 Numbering of IP Access List Rules

This feature provides support for assigning a sequence number (ID) to an IP Access List rule and re-sorting the order of rules within an Access List. The resorting of rules includes defining the number assigned to the first rule (starting sequence number) and then defining the numbers assigned to the subsequent rules. The numbering assigned to the subsequent rules is defined by an incremental step size from the starting number. By default, the first rule created is assigned the number 10 and each additional rule is incremented by 10.

As the device reads the access rules sequentially according to sequence number, this feature allows the administrator to re-assign priority of rules within an Access Lists. Once a rule is matched, the other rules belonging to the Access List are ignored.

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

- Defines an Access List with an access list number ID:

  ```
  (config-data)# ip access-list standard <Access List ID>
  ```

- Defines a rule with a rule number for the Access List:

  ```
  (config-std-nacl)# <Rule ID> [permit|deny] <rule options …>
  ```

  Where *Rule ID* is 1 to 2147483647.

- Re-sequences rule numbering of a specific Access List:

  ```
  (config-data)# ip access-list resequence <Access List ID>
  <starting rule number> <step increment>
  ```

For example, below shows a configuration of Access List ID 1 with two rules (numbers 10 and 20):

```
(config-data)# ip access-list standard 1
(config-std-nacl)# 10 permit any
(config-std-nacl)# 20 permit host 3.3.3.3
```

To change the order of the rules so that the first rule is assigned number 100 and subsequent rules are assigned numbers incremented by 50:

```
(config-data)# ip access-list resequence 1 100 50
```

To view the rules and their changed sequence numbers:

```
(config-data)# do show data access-lists
…
Standard IP access list 1
1 100 permit  any   (0 matches)
1 150 permit  host 3.3.3.3   (0 matches)
```

Applicable Products: Mediant MSBR.

4.1.1.14.5 TACACS+ through WAN Interface

This feature provides support for communicating with a TACACS+ server through the device's WAN interface. Up until this release, communication with the server could only be done through the device's LAN interface.

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

```
(config-data)# tacacs-server source data source-address interface
<interface name>
```

For example:

```
(config-data)# tacacs-server source data source-address interface
GigabitEthernet 0/0
```

Applicable Products: Mediant MSBR.

4.1.1.14.6 RADIUS through WAN Interface

This feature provides support for specifying a WAN interface as the source for RADIUS messages. Up until this release, RADIUS messages were sent from the OAMP interface (default).

To support this feature, the following CLI commands were added under `config-system > radius`:

```
# source data interface <interface name>
# source data source-address interface <IP address of interface>
```

For example:

```
(radius)# source data interface gigabitethernet 0/0
```

The `show run` CLI command can be used to verify that data packets for RADIUS are being sent from the specified WAN interface.

To return to the OAMP interface, the following `no` command is used:

```
(radius)# no source data interface <interface name>
```

The new feature provides:

- Support for RADIUS server's source interface data
- NAS-IP-Address sent in RADIUS packets adjusts and updates according to the address of the selected source interface

Applicable Products: Mediant MSBR.

4.1.1.15 Performance Monitoring and Status Features

This section describes the new data-router performance monitoring (PM) features.

4.1.1.15.1 Configurable Sample Intervals for Performance Statistics

This feature provides support for configuring sample intervals for performance monitoring statistics in the CLI. Up until this release, the CLI command `show data interface` displayed the performance statistics (counters) for intervals of the last 15 seconds and of the last 5 minutes. These intervals are now configurable.

To support this feature, the following new CLI commands have been added under the configure data mode:

```
(config-data)# pm sample-interval seconds <first sample interval
in seconds, e.g., 20>
(config-data)# pm sample-interval minutes <second sample interval
in minutes, e.g., 1>
```

Applicable Products: Mediant MSBR.

4.1.1.15.2 Performance Monitoring MIBs for VDSL Interface

This feature provides support for performance monitoring of traffic on the VDSL interface through SNMP MIBs. This is provided by the WAN VDSL entry in the SNMP IfTable MIB, providing the following packet counters:

- ifInOctets
- ifInUcastPkts
- ifInDiscards
- ifInErrors
- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutDiscards

- ifOutErrors

Applicable Products: Mediant 500 MSBR; Mediant 800/B MSBR.

4.1.1.15.3 MAC Table Display Enhancements in CLI

This feature provides support for an enhanced MAC table display in the CLI. This feature can display the MAC table per a specified VLAN, as well as display the VLAN and physical port through which a specified MAC address was acquired.

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

- Displays MAC address per VLAN:

```
# show data mac-address-table vlan <VLAN ID>
```

For example:

```
# show data mac-address-table vlan 1
MAC Address                 port
-------------------------------------------------------
1    00:00:e2:91:3c:f5      4/1
2    00:01:6c:59:ab:32      4/1
3    00:01:6c:59:f1:4e      4/1
```

- Displays the VLAN and physical port through which a specific MAC address was acquired:

```
# show data mac-address-table address <MAC address>
```

For example:

```
# show data mac-address-table address 00:0c:29:76:a8:eb
MAC Address             VLAN    Port
---------------------------------------
00:0C:29:76:A8:EB       1       4/1
```

Notes:

- The CLI command, `show data mac-address-table print` is now obsolete.
- The CLI command, `show data mac-address-table count` has been modified to `show data mac-address-table count vlan <VLAN ID>`.

Note: The following related CLI command from previous releases is now obsolete: `show data mac-address-table print`

Applicable Products: Mediant MSBR.

4.1.1.15.4 Display of Data-Router VLAN Interfaces Status in SNMP

This feature provides support for displaying the status of data-router VLAN interfaces in SNMP. The status is displayed in the IfTable.

Applicable Products: Mediant MSBR.

4.1.1.15.5 Display of Data-Router IP Network Connections in CLI

This feature provides support for displaying the data-router IP network connections in the CLI. To support this feature, the following new CLI commands have been added:

- Displays all IP connections (including a summary of the connections):

```
# show data ip connections all
```

For example:

```
IP  connections summary: 28 TCP, 39 UDP, 0 ICMP. Total 115
connections.
NAT connections summary: 0 TCP, 0 UDP, 0 ICMP. Total 0 NAT
connections.
```

```
Fastpath packets: 687102, Fullpath packets: 1104728

1 UDP in 0.0.0.0:68 out 0.0.0.0:68 other 0.0.0.0:67 inf
local_dev Route Outgoing
2 UDP in 10.13.2.15:68 out 10.13.2.15:68 other
255.255.255.255:67 inf local_dev
Route Outgoing
3 UDP in 224.0.0.252:5355 out 224.0.0.252:5355 other
10.13.22.78:64164 inf VLAN
1 Route Incoming
…
```

- Displays a brief summary of all the current IP network connections:

```
# show data ip connections brief
```

For example:

```
IP  connections summary: 28 TCP, 53 UDP, 0 ICMP. Total 129
connections.
NAT connections summary: 0 TCP, 0 UDP, 0 ICMP. Total 0 NAT
connections.
Fastpath packets: 696322, Fullpath packets: 1119176
```

- Displays the IP network connections for a specific interface:

```
# show data ip connections interface <interface type> all
```

For example:

```
# show data ip connections interface gigabitethernet 0/0 all
```

- Displays IP network connections for a specific port:

```
# show data ip connections port <port number> detail
```

- Displays IP network connections for a specific QoS queue, configured in the QOS service map menu, e.g., (conf-s-map)# queue Data1:

```
# show data ip connections queue <QoS queue name>
```

- Displays a summary of IP network connections for a specific port or all ports:

```
# show data ip connections summary port [<port number>|all-
ports]
```

For example:

```
# show data ip connections summary port all-ports
port    68: Pkt 0/0 Kb 0.0/0.0 pps 0/0 kbps 0.0/0.0
port    67: Pkt 0/0 Kb 0.0/0.0 pps 0/0 kbps 0.0/0.0
port   137: Pkt 680/0 Kb 51.7/0.0 pps 0/0 kbps 0.0/0.0
```

Where:

- *Pkt 0/0*: received/sent packets
- *Kb 0.0/0.0*: received/sent kilobytes
- *pps 0/0*: number of received/sent packets per second
- *kbps*: number of received/sent kilobytes per second

- Displays the most recent number (1 – 100) of connections:

```
# show data ip connections top <last number of connections>
```

Applicable Products: Mediant MSBR.

4.1.1.16 Diagnostics and Troubleshooting

This section describes the new data-router diagnostics and troubleshooting features.

4.1.1.16.1 Loopback on WAN Interface for Debugging

This feature provides support for performing loopback testing on specific WAN interfaces for monitoring and troubleshooting (debugging). Loopback debugging can be activated on any WAN interface (name or type) and allows the remote side to loopback traffic through the device's WAN interface (typically used to check traffic flow). This is to comply with the IEEE 802.3ah standard for Operation, Administration, and Management (OAM) for link-fault management by remote loopback (on the Ethernet WAN interface).

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

```
# debug ethernet loopback interface <interface name / type>
```

For example:

```
# debug ethernet loopback interface GigabitEthernet 0/0
```

The `no debug` command is used to disable the feature.

Note: All communication through the loopback WAN interface stops when this feature is enabled.

Applicable Products: Mediant 5xx MSBR; Mediant 800/B MSBR.

4.1.1.16.2 Dying Gasp for SHDSL upon Power Outage

The feature provides support for the Dying Gasp through the power status bit, as defined in in ITU-T standard G.991.2, section 7.1.2.5.3. This is relevant for SHDSL interfaces. The Dying Gasp allows a customer premises equipment (CPE) to automatically notify the digital subscriber line access multiplexer (DSLAM) of a power failure in the CPE. Based on this indication, the server provider can conclude that the connectivity loss was due to a loss of power in the CPE, rather than a disconnected cable.

For information on the relevant hardware versions for which this feature is supported, please contact your AudioCodes sales representative.

Applicable Products: Mediant 800/B MSBR.

4.1.1.16.3 Automatic Stopping of Debug Captures

This feature provides support for starting a debug-traffic capture on the device's physical network interfaces and allowing it to run until a user-defined event. This event can be a Syslog message or an interface state-change.

This feature supports all physical targets (TFTP, FTP, and USB), and SSH retrieval. This feature supports regular and cyclic-buffer modes. When combined with cyclic-buffer mode, this feature makes diagnosis of network problems easier.

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

- Defines the Syslog message event, upon which the device stops the debug capture:

  ```
  # debug capture data physical auto-stop event syslog
  "<message>"
  ```

- Defines the state change on a specific interface, upon which the device stops the debug capture:

  ```
  # debug capture data physical auto-stop event state-change
  <interface, e.g., GigabitEthernet 0/0>
  ```

- Defines a state change on any interface, upon which the device stops the debug capture:

  ```
  # debug capture data physical auto-stop event state-change any
  ```

- Defines what to do with the debug capture when it is automatically stopped:

  ```
  # debug capture data physical auto-stop [send <IP
  address>|keep]
  ```

  Where:

- *send* sends the capture to the defined IP address
- *keep* saves the capture on the device for later retrieval

- Disables the automatic stopping feature for debug captures:

```
# no debug capture data physical auto-stop
```

Applicable Products: Mediant MSBR.

4.1.1.16.4 Debug Capture of ATM Packets over ADSL on PHY

This feature provides support for debug capturing of Asynchronous Transfer Mode (ATM) packets over ADSL through the ADSL/VDSL PHY (physical layer) chipset. This functionality supports ATM AAL5 (ATM Adaptation Layer 5) and ATM OAMP cells. Up until this release, debug capturing of ATM packets was supported for the WAN interface (debug capture data physical dsl-wan) on a routing CPU. However, as the PHY based on the ADSL/VDSL chipset exists between the routing CPU and DSLAM, it may also be important to capture ATM packets from the PHY.

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

```
# debug capture data physical dsl-wan phy
```

The debug capture is activated and de-activated using the following existing commands:

```
# debug capture data physical start
# debug capture data physical stop <server IP address>
```

Applicable Products: Mediant 800B MSBR.

4.1.1.16.5 Enhanced Q.931 ISDN Traces

This feature provides support for enhanced Q.931 traces for debugging. In previous releases, when ISDN traces were done, in addition to the desired trace messages, other non-related messages were also shown in the trace. From this release, non-related messages are not included in the ISDN trace.

Applicable Products: Mediant 5xx; Mediant 8xx; Mediant 1000B; Mediant 3000.

4.2 Patch Version 6.80A.308.003

This patch version includes new features, known constraints and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.306.006 (see Section 3.7 on page 159).
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
  - √ OAM-EFM (802.3ah)
- If the MSBR device is running a software version that is **earlier than 6.80A.286.002**, to upgrade the device to the latest software version, the device must **first** be upgraded to Version **6.80A.286.002** and only then upgraded to the latest software version.

4.2.1 New Features

New features introduced in this version include the following:

- BGP neighbor authentication using MD5 (IPv4 only).
- VRF route leaking to allow replication of a static route from one VRF to another.
- The `show data interface` command now displays QoS bandwidth for each interface configured with QoS.
- Configuration of IGMP Proxy through CLI.
- Removing given IP addresses or ranges from a DHCP address allocation pool, using the new command `ip dhcp-server network exclude`.
- The `track` command can now be used with the automatic default route received from the DHCP server as well as for static routes.
- VRRP protocol support, which enables two device (MSBR) routers to share a virtual IP address for redundancy for the default gateway on a LAN.
- Enhancement of the A/VDSL LED indication.
- Configuration of tcp mss on tunnel interfaces, using the command `ip tcp adjust-mss`.
- New SNMP trap which indicates Track up/down events.

- New troubleshooting option that tracks DSL line state changes, using the new command `debug adsl-connection`.
- Accelerating AH traffic traversing the device.
- Accelerating ESP traffic traversing the device.
- The device can now forward its' DNS servers to its' DHCP clients. The clients query the DNS servers directly and not through the device. DNS requests to the device are ignored. To activate the feature (off by default), use the command `no ip dns proxy`.
- Measuring voice statistics using PacketSmart.

4.2.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-1: Known Constraints for Patch Version 6.80A.308.003

Incident	Description
134785	Software upgrade and configuration file load/download through TR-069 fails. **Note:** This constraint has been resolved in patch release **6.80A.308.504** (see Section 4.3).
131611	Sometimes some pairs do not synchronize after a device reset when working with SHDSL 4-Pairs EFM configuration. This can result in random traffic loss and the inability to establish reliable connectivity. A workaround is to use the interop reset configuration under `interface shdsl`. The recommended values are `interop reset 120 30`.
130070	The WAN-to-LAN mirroring utility for troubleshooting is not functioning properly on DSL interfaces. A workaround is to use other debug utilities such as debug capture physical / interface.
131537	TR-069 does not function when the ACS is located on the LAN side of the device.
131198	On some occasions, the device fails to successfully complete a software upgrade process through TR-069, and the process has to be repeated.
130626	Multilink is torn down when changing the NAPT parameter.
134510	When working in the VDSL-first mode, L2 sometimes remains on EFM even though the actual connectivity is ADSL. A workaround is to reset the device.

4.2.3 Resolved Constraints

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

Table 4-2: Resolved Constraints for Patch Version 6.80A.308.003

Incident	Description
127583	When using T1-WAN in HDLC encapsulation, SLARP keep-alive does not function properly and cannot be used on the device side or on the link partner side.
133104	DNS Proxy default configuration is not shown in the configuration.
133115	Erroneous display of the OUI of the remote peer for the OAM interface.
133194	In certain scenarios, configuring the VoIP application to "WAN" does not function properly.

Incident	Description
133210	The MTU value changes for the EFM interface upon a device reset.
133271	Erroneous reporting of the Ethernet OAM protocol capabilities in the OAM frame sent to the remote router.
133282	OAM Loopback mode fails when remote-loopback is initiated by the remote peer.
133426	Configuration issues when setting TX power values between 51-100% on the radio interface.
133566	The use of a single pair of an SHDSL interface cannot be used if it is not the first pair (Master Pair).
133573	The EFM OAM interface erroneously retrieves its status (up or down) from the Gigabit Ethernet 0/0 interface.
133651	Support for Novatel Wireless HSUPA modem cellular dongle is being blocked.
133676	The MSS value in `show run` is not identical to the actual value after the device resets.
133047	IP fragmentation bug when multiple fragments are received simultaneously.
117565	The `show dhcp binding` command truncates the full list of configured DHCP clients.
125747	Issues concerning QoS on SHDSL in auto mode.
126385	LAN Physical interfaces Data counter sample intervals configuration cannot be applied.
127612	DSL autoswitch configuration cannot be pasted from `show run` because the content is erroneous.
127613	DSL autoswitch mechanism fails to synchronize between ADSL and VDSL.
127651	Under certain circumstances, IPsec traffic is not forwarded to the remote host peer via the WAN.
128282	The `show data qos service-map` command cannot be applied on an SHDSL ATM interface.
128423	Configuring a new Media Realm through CLI fails and a message is displayed informing the user that the Default Media Realm was already defined.
128521	The `show run data interface` command does not show LAN ports configuration.
128921	After restoring the device to factory defaults, IGMP proxy configuration remains.
129092	The port-security violation shutdown cannot be applied after the `shut` and `no shut` operations are performed on the device.
129384	In certain scenarios, `ip nat inside source list` configuration causes the device to fail during reset following a length recovery process.
129935	MAC address configuration cannot be removed from the physical WAN.
129761	The DHCP relay agent does not functioning correctly in VRF mode.
129785	The WAN fiber port is not blocked when the device's License Key does not include the Fiber interface feature.
129808	When the CLI script is copied, the RADIUS password disappears.
129485	"Leaking" of resources when 802.11 radio (Wi-Fi) is configured with the auto rescan feature, and the dot11radio interface is administratively booted up and shut down hundreds of times.

Incident	Description
130564	Unable to configure `ip dhcp-client default-route track` on the ATM interface under DSL and SHDSL.
130834	When the device is configured to VDSL-V43 and the automatic DSL detection feature detects ADSL, the automatic process for creating the ATM interface on top of the ADSL fails.
130915	RTCP-XR cannot be configured offline through CLI if the RTCP-XR feature key is not enabled on the device.
131019	The device fails when the command `show run > (HTTP address)` is run.
131287	The device does not display data track brief when the interface is physically disconnected.
131485	IPv6 DHCP loads faster when the GE interface's connection is established.
131814	The device fails after the NAT rule `nat inside destination` is configured.
132846	When configuring the SHDSL EFM interface and the master pair in the group is not pair 0, incorrect show output is displayed.
132663	A new CLI command `debug serial-port` enables the changing of the serial cable mode yellow connector to RMX (default), DSL or DSL2. When the `keep` option is used, the device configuration is maintained after reset.
132777	Errors are generated when trying to configure serial interfaces after transition from E1-WAN to T1-WAN.
123245	The device fails when there is an existing E1-WAN configuration and an attempt is made to overwrite it with a T1-WAN configuration.

4.3 Minor Patch Version 6.80A.308.504

This patch version is identical to its major patch version (6.80A.308.003), except for resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.306.006 (see Section 3.7 on page 159).
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
  - √ OAM-EFM (802.3ah)
- If the MSBR device is running a software version that is **earlier than 6.80A.286.002**, to upgrade the device to the latest software version, the device must **first** be upgraded to Version **6.80A.286.002** and only then upgraded to the latest software version.

4.3.1 Resolved Constraints

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

Table 4-3: Resolved Constraints for Patch Version 6.80A.308.504

Incident	Description
134785	Software upgrade and configuration file load/download through TR-069 fails.

4.4 Patch Version 6.80A.311.003

This patch version includes new features, known constraints and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.310.002 (see Section 3.7 on page 159).
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
  - √ OAM-EFM (802.3ah)
- If the MSBR device is running a software version **earlier than 6.80A.286.002**, to upgrade the device to the latest software version, the device must **first** be upgraded to Version **6.80A.286.002** and only then upgraded to the latest software version.

4.4.1 New Features

New features introduced in this version include the following:

- New CLI commands for monitoring the device's CPU and memory utilization:
  - Displays CPU utilization in the last minute, last hour (average minute utilization), and last 72 hours (average utilization per hour):

```
show system cpu-util history data ;
show system cpu-util history voice
```

  - To clear CPU utilization history:

```
clear system cpu-util history
```

  - Display memory utilization in last hour and last 72 hours:

```
show system utilization history data
show system utilization history voice
```

- A/VDSL modem recovery support: If the device detects a failure in its' A/VDSL modem, it reloads the ADSL software from its' flash memory and re-initializes the modem. Note that to enable the feature, this patch version must be loaded **twice** to the device. For more information, refer to the document *Mediant MSBR Access CLI Configuration Guide*.

4.4.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-4: Known Constraints for Patch Version 6.80A.311.003

Incident	Description
131611	Sometimes some of the pairs don't synchronize after a device reset when operating on SHDSL 4-Pairs EFM configuration. This sometimes results in random traffic loss and inability to establish reliable connectivity. A workaround is to use the `interop reset` command under `interface shdsl`. The recommended configuration is: `interop reset 120 30`
130070	The WAN-to-LAN mirroring utility for troubleshooting does not function properly on DSL interfaces. A workaround is to use other debug utilities such as `debug capture physical / interface`.
133713	Configuring and un-configuring the 3G interface repeatedly may cause the device to crash.

4.4.3 Resolved Constraints

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

Table 4-5: Resolved Constraints for Patch Version 6.80A.311.003

Incident	Description
131537	TR-069 does not function when the ACS is located on the LAN side of the device.
130626	Multilink failure occurs when NAPT configuration (`napt` command) is changed.
134510	Layer-2 sometimes stays on EFM even though the actual connectivity is ADSL, while working on VDSL-first mode.
134063	The Monitor Interface and Network Interface parameters appear in the Web interface for PacketSmart configuration, even though they are not relevant to MSBR devices. (They have now been removed.)
134306	The CLI output of the `show data vrrp` command does not display information for tracked objects.
134784	TR-069 port configuration does not take effect unless the device is reset. (Now, a prompt has been added whenever the port is changed.)
134931	When the default Media Realm is configured to the maximum available ports, the available ports for routing through the WAN interface is affected adversely.

4.5 Patch Version 6.80A.317.001

This patch version includes new features, known constraints and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.316.005 (see Section 3.9 3.7on page 163).
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
  - √ OAM-EFM (802.3ah)
- If the MSBR device is running a software version **earlier than 6.80A.286.002**, to upgrade the device to the latest software version, the device must **first** be upgraded to Version **6.80A.286.002** and only then upgraded to the latest software version.

4.5.1 New Features

New features introduced in this version include the following:

- A new CLI command, `show data interface dsl brief` has been added, which displays downstream and upstream information for DSL interfaces.
- A new CLI command, `ip max connection` has been added, which limits the maximum number of sessions per PPPoE interface.
- Support for the DHCP message FORCERENEW. When the device acts as a DHCP client and receives this message from the DHCP server, it will re-acquire an IP address.
- Multi-authentication on PPP and Cellular interfaces. Up to eight users with passwords can be configured, which are arranged in eight lists.

4.5.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-6: Known Constraints for Patch Version 6.80A.317.001

Incident	Description
131611	When the MSBR device is configured for SHDSL 4-Pairs EFM, sometimes some of the pairs do not synchronize after a device reset. As a result, random traffic loss and inability to establish reliable connectivity can occur. A workaround is to use the `interop reset` command under the SHDSL interface (recommended values are `interop reset 120 30`).
130070	WAN-to-LAN mirroring utility for troubleshooting does not function properly on DSL interfaces. A workaround is to use other debug utilities such as `debug capture physical / interface`.
133713	Configuring and un-configuring 3G interfaces repeatedly may cause the device to crash (reset).

4.5.3 Resolved Constraints

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

Table 4-7: Resolved Constraints for Patch Version 6.80A.317.001

Incident	Description
135196	Loading new configuration that includes a new ACS URL to the device through the ACS causes the device to reply to the new ACS with the messages “TRANSFER COMPLETE” and “M Download”, instead of replying to the old ACS.
135320	Incorrect representation of TR-098 parameters. The bug was resolved by removing the dashes.
135323	Escaping characters missing from TR-069 command output. The bug was resolved by support for XML characters.
136364	Unable to connect to the device through SSH over WAN with IPv6.
136658	Enhanced SAR (Segmentation and reassembly) ATM implementation for slow ATM-SHDSL lines (less than 2 Mbps).
135319	When the device requests information from a DNS server using Recursive DNS queries and the DNS server responds with a non-Recursive query, the device is unable to process the response correctly.

4.6 Patch Version 6.80M.584.002

This patch version includes only resolved constraints.

Note:

- This patch version is a derivative of Version 6.80A.317.001.
- This patch version is applicable **only to TR-181 customers** (coordinated with AudioCodes).
- This patch version is applicable only to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interface:
  - √ A/VDSL ISDN

4.6.1 Resolved Constraints

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

Table 4-8: Resolved Constraints for Patch Version 6.80M.584.002

Incident	Description
136189	The serial ID of the MSBR device is not sent to the ACS when using DDNS.
135551	When updating the TR-181 database (tree) upon removal of the object “IP.Interface” or upon updating a DNS entry, the tree is not updated accordingly.
134940	In some cases with DNS relay, the client does not receive the DNS IP address.
135464	An empty value appears under the object “Device.IP.Interface.{i}.Router”.
135943	For port forwarding, when an incorrect name or WAN IP address is configured, NAT rules sometimes result in a disconnection.
135524	When configuring an empty ACS_URL through TR-069, the device crashes (resets).
135538	The "Service On " / "Service Off" TR service through the Web causes the device to crash (reset).

4.7 Patch Version 6.80AR.317.001

This patch version includes new features, known constraints and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.316.005 (see Section 3.9 on page 163).
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
  - √ OAM-EFM (802.3ah)
- The "R" in this patch version stands for "reduced". This version is reduced in size and does not include the PacketSmart feature and A/VDSL firmware.
- The A/VDSL firmware needs to be loaded after this firmware is loaded to the MSBR device.
- The update to this version can be performed from any previous firmware.

4.7.1 New Features

New features introduced in this version include the following:

- A new CLI command, `show data interface dsl brief` has been added, which displays downstream and upstream information for DSL interfaces.
- A new CLI command, `ip max connection` has been added, which limits the maximum number of sessions per PPPoE interface.
- Support for the DHCP message FORCERENEW. When the device acts as a DHCP client and receives this message from the DHCP server, it will re-acquire an IP address.
- Multi-authentication on PPP and Cellular interfaces. Up to eight users with passwords can be configured, which are arranged in eight lists.

4.7.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-9: Known Constraints for Patch Version 6.80AR.317.001

Incident	Description
131611	When the MSBR device is configured for SHDSL 4-Pairs EFM, sometimes some of the pairs do not synchronize after a device reset. As a result, random traffic loss and inability to establish reliable connectivity can occur. A workaround is to use the `interop reset` command under the SHDSL interface (recommended values are `interop reset 120 30`).
130070	WAN-to-LAN mirroring utility for troubleshooting does not function properly on DSL interfaces. A workaround is to use other debug utilities such as `debug capture physical / interface`.
133713	Configuring and un-configuring 3G interfaces repeatedly may cause the device to crash (reset).

4.7.3 Resolved Constraints

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

Table 4-10: Resolved Constraints for Patch Version 6.80AR.317.001

Incident	Description
135196	Loading new configuration that includes a new ACS URL to the device through the ACS causes the device to reply to the new ACS with the messages “TRANSFER COMPLETE” and “M Download”, instead of replying to the old ACS.
135320	Incorrect representation of TR-098 parameters. The bug was resolved by removing the dashes.
135323	Escaping characters missing from TR-069 command output. The bug was resolved by support for XML characters.
136364	Unable to connect to the device through SSH over WAN with IPv6.
136658	Enhanced SAR (Segmentation and reassembly) ATM implementation for slow ATM-SHDSL lines (less than 2 Mbps).
135319	When the device requests information from a DNS server using Recursive DNS queries and the DNS server responds with a non-Recursive query, the device is unable to process the response correctly.

4.8 Patch Version 6.80A.323.002

This patch version includes new features, known constraints and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.323.002 (see Section 3.10 on page 165).
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
  - √ OAM-EFM (802.3ah)
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.8.1 New Features

New features introduced in this version include the following:

- Dual image (.cmp) support, whereby if the software upgrade process is interrupted by a power outage, the device runs the previously installed software version when it is powered up again. Note that the feature is currently supported only for MSBR models with 128-MByte flash.
- Retransmission (per G.998.4) at the VDSL upstream.
- New page in the device's Web interface titled "IP Interface Status" (under Data Status), which displays the status of WAN IP interfaces.
- Authentication for BGP peer group (router bgp > **neighbor** <bgp peer> **password** <string>).
- Binding Track to local source address, using the following new command: **track** <track ID> <track protocol type - icmpecho/icmpv6echo> <destination IPv4 address> <source interface> [**source-ip-interface**] [id] [interval between probes] [number of retries before track goes down]

4.8.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-11: Known Constraints for Patch Version 6.80A.323.002

Incident	Description
131611	Sometimes some of the pairs don't sync after a reboot when working on SHDSL 4-Pairs EFM configuration. This can result in random traffic loss and the inability to establish reliable connectivity. A workaround is to use the **interop reset** configuration under **interface shdsl**. The recommended values are **interop reset 120 30**.
130070	The WAN-to-LAN mirroring utility for troubleshooting is not functioning properly on DSL interfaces. A workaround is to use other debug utilities such as **debug capture physical** / **interface**.
133713	Configuring and un-configuring 3G interface repeatedly may cause the device to crash.
138272	BRI configuration downloaded to the device through a CLI script is processed and applied **only** after a reset. This issue does not exist for BRI configuration through the Web interface.

4.8.3 Resolved Constraints

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

Table 4-12: Resolved Constraints for Patch Version 6.80A.323.002

Incident	Description
129053	The **clear ipv6 dhcp bind** command doesn't clear binds relating to DHCPv6.
132103	Stateful DHCPv6 server does not record lease of single address in lease table.
136838	No maximum number of users is enforced for PPP multi-authentication. Now, up to eight ppp-user-lists are allowed to be configured.
138024	When deleting an IPv6 static route rule from configuration, the rule still exists in the route table.
137582	Issue resolved concerning upgrading software through HTTP/HTTPS (HTTP redirect code 301 302).
136574	When obtaining the ACS URL through DHCP for TR-069, a problem exists in connecting to the ACS.
136689	The device crashes (and and reset) when running the Speed Test (**debug speedtest select country** < country >).

4.9 Patch Version 6.80A.330

This patch version includes new features, known constraints and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.328.004 (see Section 3.11 on page 167).
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
  - √ OAM-EFM (802.3ah)
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.9.1 New Features

New features introduced in this version include the following:

- For the Virtual Router Redundancy Protocol (VRRP) feature, a new command allows you to change the VRRP priority according to whether the Track is up or down: **vrrp** [VRRP ID] **track** [Tracked Object] **decrement** [Decrement Value]
- Deleting debug capture files from the device's RAM, using the new command **debug capture data physical clear**.
- Support for the Cellular USB dongle (PPP), ZTE 0x19d2 MF710M 0x1589.
- Bypassing TACACS+ server.
- Maximum connection statistic per hour or per 72 hours, using the following commands:
  - **show data ip firewall max-conn-statistics last-hour**
  - **show data ip firewall max-conn-statistics last-72-hours**
- Changing ProductClass value through TR-098.
- Configuring WPA2 with 11i parameters (Default BeaconType set to basic) through TR-98.

- Display of Inventory Information according to ITU-T G.997.1, using the new command **show data interface dsl 0/x inventoryinfo**.
- When downloading files to the device over a secured channel (TLS), the cipher suite can now be configured using the ini file parameter, AupdCipherString. Standard OpenSSL syntax is used for configuration (see https://wiki.openssl.org/index.php/Manual:Ciphers(1)). For example, to enable only ciphers using AES variants: AupdCipherString = AES

4.9.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-13: Known Constraints for Patch Version 6.80A.330

Incident	Description
130070	WAN-to-LAN mirroring utility for troubleshooting does not function properly on DSL interfaces. A workaround is to use other debug utilities such as **debug capture physical / interface**.
131611	Sometimes some pairs do not synchronize after a device reset when working with SHDSL 4-Pairs EFM configuration. This can result in random traffic loss and the inability to establish reliable connectivity. A workaround is to use the interop reset configuration under `interface shdsl`. The recommended values are `interop reset 120 30`.
138370	DynDNS does not function.
139656	The device crashes (resets) when deleting the ATM interface that is assigned as a source to the GRE interface. A workaround is to change the source interface or delete the GRE tunnel before deleting the interface or modifying encapsulation.

4.9.3 Resolved Constraints

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

Table 4-14: Resolved Constraints for Patch Version 6.80A.330

Incident	Description
132475	Incorrect counting of the total number of IPv6 addresses shown in the DHCPv6 pool.
137393	Bug when loading a Startup script file that includes TR-069 parameters from a USB device.
138028	The SNMP MIB, acSysStateVoIpCpuUtilization always shows 0.
138058	No IPv6 Link-Local address on the PPPoE interface.
138093	Various bugs when using static routes for source-based routing.
138124	When a loopback interface is configured as WAN using the **network wan** command, the NAT on the WAN interface changes the IP address from the loopback IP address to the WAN interface IP address. In normal operation, the loopback IP address should be changed by NAT to the WAN interface IP address only if the loopback is configured as LAN using the **network lan** command.
138251	No option for prefix delegation when WAN (IPv6) is PPPoE.
138271	IPv6 on PPPoE doesn't work when IPv4 isn't enabled.

Incident	Description
138274	No option to choose DHCPv6 work mode for PPPoE interface (stateful/stateless).
138446	Policy-Based Routing bug: to prevent accidental route leaking, there is a need to configure an output interface in a VRF that is different from the input interface.
138470	No option to configure SNTP IP address (IPv6) for DHCPv6 server.
138612	Policy-Based Routing bug: configuring a PBR rule where the output interface is in VRF may cause a crash when disabling and enabling the output interface.
138619	When configuring a management ACL to block a specific host (IPv6), it also denies other hosts on different networks.
138624	When using management ACL, the command **override-telnet-acl-for-lan** (IPv6) doesn't override the ACL definition and blocks Telnet.
138709	Source-based routes are not prioritized over regular routes with the same destination.
138883	Device resets when a hub device is connected to the USB port.
139020	IPv6 interfaces fail to load after changing the MTU.
139039	When configuring an IPv6 DHCP client and autoconfig on Copper WAN, the device crashes (reset).
139105	The **copy to** command fails with the error message "Address already in use".
139352	The **show data ipv6 interface gigabitethernet** command causes the device to crash (reset).
139658	ADSL does not function if **encapsulation pppoa-mux** (PPP encapsulation) is configured under the ATM interface.
139870	For TR-098, DSL data rates report incorrect values to the ACS.

4.10 Patch Version 6.80M.588.002

This patch version includes only resolved constraints.

Note:

- This patch version is a derivative of Version 6.80A.330 (see Section 4.9).
- This patch version is applicable **only to TR-181 customers** (coordinated with AudioCodes).
- This patch version is applicable only to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interface:
  - √ A/VDSL ISDN

4.10.1 Resolved Constraints

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

Table 4-15: Resolved Constraints for Patch Version 6.80M.588.002

Incident	Description
140405	Implement DTAG configuration hardcoded.
139027	DNS on interface VLAN cannot be configured through the TR-069 ACS.
136311	The device (client) receives two DNS server IP addresses instead of one.

4.11 Patch Version 6.80A.335.005

This patch version includes new features, known constraints and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.333.004.
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.11.1 New Features

New features introduced in this version include the following:

- Configuration of a customized serial number (S/N) for the device. This is supported by the new ini file parameter, CustomerSN. Note that the device's original S/N is automatically added at the end of the configured S/N. For example, if the original S/N is 8906721 and the configured S/N is "abc123", the resultant S/N will be "abc1238906721".
- Redundant messages displayed upon device boot time are no longer shown.
- Running speed tests through TR-069.
- The physical port to which a specific LAN host (DHCP) is connected can be determined using the following new settings:
  - CLI: **show data ip dhcp bindings**
  - CWMP: InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}.Layer2Interface.

4.11.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-16: Known Constraints for Patch Version 6.80A.335.005

Incident	Description
130070	The WAN-to-LAN mirroring utility for troubleshooting does not function properly on DSL interfaces. A workaround is to use other debug utilities such as **debug capture physical / interface**.
131611	Sometimes some of the pairs aren't synchronizing after a device reset when operating on SHDSL 4-Pairs EFM configuration. This can result in random traffic loss and the inability to establish reliable connectivity. A workaround is to use the **interop reset** command under the **interface shdsl**. The recommended value is **interop reset 120 30**.
140954	When the command **copy cli to** fails, the device indicates that the command was successful.

4.11.3 Resolved Constraints

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

Table 4-17: Resolved Constraints for Patch Version 6.80A.335.005

Incident	Description
134328	Reset-is-required indication asterisk (*) in the CLI session is not displayed during configuration of the **wan-snmp-allow** command.
134656	Frames are forwarded only LAN-to-WAN on CFM interfaces in BVI configuration.
134891	MAC error displays in **show data ethernet cfm**.
139083	PBR with output interface from a different VRF is displayed in the **show data ip route** main VRF routing table as active.
139977	DSCP filtering doesn't function when working in PBR configuration with ACL rule **dscp**.
139536	Deleting an interface configured as a tunnel source may cause the device to fail.
140079	Test call to an IPv6 group doesn't function.
140085	Device crashes when deleting a VTI interface.
140155	By default, the DSL modem attempts twice instead of three times to connect with VDSL and if not successful, it attempts to use ADSL.
141164	Route leak between L2TP clients and interfaces in other VRFs does not function.
140654	IPv6 prefix delegation does not function on WAN interfaces (the device does not send Identity Association requests).
140657	The device crashes when removing a PPPoE interface while vlan IPv6 prefix delegation config points to it.
140660	NQM does not get bind to the WAN interface on dynamic IP interfaces (DHCP,PPP).
140694	Access List configuration lacks the option to configure the DSCP field for IPv6 packets.
140886	The command **clear IPv6 neighbor all** does not function correctly on interfaces that use SLAAC.

Incident	Description
140892	Mediant 800 MSBR fails to burn configuration using write/burn in some rare cases.
141090	DNS query fails when using a hostname in the Proxy Sets table.
141091	The file transfer time of copy files from HTTP/TFTP is slow.
141111	The **qos** command fails to modify the DSCP value in egress packets.
141135	Traffic does not get NATed when fragmenting according to the configured MTU.
141372	The **show data ip interface** command is available only in privileged mode.
141539	IPv6 address for PPPoE interface received from BRAS doesn't save after a device reset.
139695	Improper PPPoE behavior in which the device sends PADO messages mistakenly.
141331	The device doesn’t update its IP address correctly in VoIP packets even though the address was changed.
140527	After a device reset, MTU of EFM interface becomes **auto**, even though it was set to **static**.
141250	Incoherent SNMP configuration done from the CLI, preventing restoring configuration at new device.
141753	Port forwarding rules cause memory leaks in the device.
141551	When a CLI Script file is copied from an HTTP server that does not respond with an HTTP 304, the device resets even if the CLI script did not change.

4.12 Patch Version 6.80M.589.007

This patch version includes only resolved constraints.

Note:

- This patch version is a derivative of Version 6.80A.335.005 (see Section 4.11).
- This patch version is applicable **only to TR-181 customers** (coordinated with AudioCodes).
- This patch version is applicable only to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interface:
  - √ A/VDSL ISDN

4.12.1 Resolved Constraints

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

Table 4-18: Resolved Constraints for Patch Version 6.80M.589.007

Incident	Description
131321	Incorrect values for the TR-181 Device.ATM.Link.1.Stats.HECErrors parameter.
132467	Incorrect values for the TR-181 Device.DSL.Line.1.Stats parameters.
131319	Incorrect values for the TR-181 Device.ATM.Link.1.Stats.CRCErrors parameters.

4.13 Patch Version 6.80A.339.001

This patch version includes new features, known constraints, and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.338.003.
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL (Only EFM)
  - √ VDSL ISDN
  - √ VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.13.1 New Features

New features introduced in this version include the following:

- Bidirectional Forwarding Detection (BFD) support for Open Shortest Path First (OSPF). The new command to enable BFD for an OSPF interface is as follows:

```
(config-if)# ip ospf bfd interval <Value> min_rx <Value>
multiplier <Value>
```

  where:

  - *interval*: Interval (in msec) for outgoing BFD messages. The interval is increased if required by remote system.
  - *min_rx*: Minimal interval (in msec) between BFD messages in milliseconds. The remote system uses this interval for sending messages if its interval is lower.
  - *multiplier*: Maximum number of packets that can be missed before the session status is considered down.

- Bidirectional Forwarding Detection (BFD) support for static routes. The new command to enable BFD for a static route is as follows:

```
(config-data)# bfd neighbor <Neighbor ID> <IP Address>
<Interface ID> interval <Value> min_rx <Value> multiplier
<Value> [multihop]
```

  where:

  - *neighbor id:* (1-20) Neighbor identifier.
  - *ip address:* Address of the remote BFD device.
  - *interface id:* Name and number of the outgoing interface.

- *interval*: Interval (in msec) for outgoing BFD messages. The interval is increased if required by remote system.
- *min_rx*: Minimal interval (in msec) between BFD messages in milliseconds. The remote system uses this interval for sending messages if its interval is lower.
- *multiplier*: Maximum number of packets that can be missed before the session status is considered down.
- *multihop:* Set the neighbor to multihop mode in case the remote device is not on the local LAN
  The parameter **bfd-neighbor <neighbor ID>** was added to the **ip route** command:

```
(config-data)# ip route <Ip Address> <Ip Destination Mask>
[next-hop IP address] <Interface> <Interface ID> [<Metric
Value>] [track <Track Id>] [bfd-neighbor <Neighbor ID>]
[output-vrf <VRF ID>] [description <String>]
```

where:

- *bfd-neighbor:* Defines the ID of a BFD neighbor to attach the route to.

4.13.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-19: Known Constraints for Patch Version 6.80A.339.001

Incident	Description
142836	LAN-based host feature doesn't function on Ethernet ports 1/5-1/8.
130070	The WAN-to-LAN mirroring utility for troubleshooting does not function properly on DSL interfaces. A workaround is to use other debug utilities such as **debug capture physical** / **interface**.
131611	Sometimes some of the pairs aren't synchronizing after a device reset when operating on SHDSL 4-Pairs EFM configuration. This can result in random traffic loss and the inability to establish reliable connectivity. A workaround is to use the **interop reset** command under the interface shdsl. The recommended value is **interop reset 120 30**.
140954	When the command **copy cli to** fails, the device erroneously indicates that the command was successful.
142952	IPv6 default gateway does not function in single-networking mode. A workaround is to configure a "dummy" IPv6 address on the WAN interface.

4.13.3 Resolved Constraints

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

Table 4-20: Resolved Constraints for Patch Version 6.80A.339.001

Incident	Description
139561	New command has been added to view DDNS status (**show data ddns**).
140189	Configuration of GRE tunnel without a source interface is not allowed in order to prevent a mismatch with the other side of the tunnel.
141810	InternetGatewayDevice.LANDevice.1.LANEthernetInterfaceConfig.4 is not displayed in the TR-069 ACS.

Incident	Description
142444	The configuration **qos match-map** input "NAME" VLAN 4001 appears as **qos match-map** input "NAME" internal-LAN when the **show** command is run.
138399	The RTP port is different than that advertised in the SDP body of the SIP 200 OK.
142237	The OSPF **max-metric router-lsa** command has no effect when the OSPF process is closed.

4.14 Patch Version 6.80A.347.001

This patch version includes new features and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.346.005.
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL (Only EFM)
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.14.1 New Features

New features introduced in this version include the following:

- Management ACL for TR-069 can now be configured, using the new command:

```
(config-system)# cwmp
(cwmp-tr069)# cwmp-acl <ACL name>
```

- Auto-detect mode (ADSL or VDSL) feature has been added for A/VDSL. For more information, refer to *Mediant MSBR LAN-WAN Access CLI Configuration Guide*.
- Triggering DNS entries of all types (A, AAAA, NAPTR, etc.) is now supported. For more information, refer to *Mediant MSBR IP Networking CLI Configuration Guide*.
- The License Key can now be loaded through CLI, using the new command:

```
# copy feature-key from <URL>
```

- Hostnames can now be configured for the management ACL.
- The CLI terminal window height can now be locked. The feature can be configured through CLI using the command **default-window-height <value>** or through the Web interface using the new parameter 'Default terminal window height' (System > Management > Telnet/SSH Settings > General).
- ACL can now be applied to NAT port forwarding rules, by using the new option "match" for the **ip nat inside source** command. For example:
  - Access list rule called “PF-ACL”:

```
(config-data)# access-list PF-ACL permit ip host 4.4.4.4 any
```

  - Access list “PF-ACL” used in NAT port forwarding:

```
(config-data)# ip nat inside source static tcp 192.168.0.16
same gigabitethernet 0/0 8080 match PF-ACL
```

- Vendor-specific TR-069 log string can now be configured, using the DeviceLog parameter (InternetGatewayDevice.DeviceInfo.DeviceLog).
- Sending TR-069 connection request (send-connection-request) is now also available in unprivileged CLI mode, using the new command **debug cwmp send-connection-request**.
- Auto assign self IPv6 address has been added to **ipv6 dhcp-server dns-server address** when using a DHCP server.
- The status of all interfaces (**show data interfaces atm/bvi** ...) is now also available in unprivileged CLI mode.

4.14.2 Resolved Constraints

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

Table 4-21: Resolved Constraints for Patch Version 6.80A.347.001

Incident	Description
138223	The cellular, dynamic option driver is not saved after a device reset.
138373	In some cases, the Huawei 4G USB stick does not receive an IP address after a device reset.
141709	TR-069 provisioning code is lost after device reset and reverts to default ("VOIP.DATA").
142256	No option to configure dynamic learning of IPv6 NTP addresses on a PPPoE interface.
142642	QoS calibration on VDSL/EFM lines.
142821	Unable to display L2 hosts in the TR hosts table (but now possible (InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i}).
142836	LAN-based host feature doesn't show all hosts.
142952	Statically configured IPv6 route does not function when a dynamic IP address is configured.
143500	PPPoE interface cannot be underlying to an ATM interface.
143774	Single Network Mode - no RTP between local extensions (FXS and IP Phone) when using VRF.
143806	Single Network Mode – ringback tone from PRT file is not played.
143892	Single Network Mode - no RTP between local extensions (FXS and IP Phone / FXS and FXS) when using the loopback interface.
143969	Upload of files through TR-069 via HTTPS fails.
144096	TR-069 change of PPPoE credentials terminates too early and causes transaction error.
144197	Configuring "cellular-backup" in the backup-group when IPSec crypto map is configured, causes the cellular interface to remain in non-operational mode.
144870	The **show run** command does not display IPSec, PFS or metric parameters under the crypto map if the crypto map is not associated with the interface.
144927	IPv6 addresses on the PPPoE interface does not function with IPv4 addresses.
145396	For DHCPv6 NTP, the **ipv6 dhcp-client ntp-server** command is not displayed by the **show run** command under the PPPoE interface.

4.15 Patch Version 6.80M.591.004

This patch version includes new features and resolved constraints.

Note:

- This patch version is a derivative of Version 6.80A.347.001 (see Section 4.14).
- This patch version is applicable **only to TR-181 customers** (coordinated with AudioCodes).
- This patch version is applicable only to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interface:
  - √ A/VDSL ISDN

4.15.1 New Features

New features introduced in this version include the following:

- A new TR-069 command has been added to activate/deactivate a BRI trunk. The new command is VoiceService.{i}.PhyInterface.{i}.ISDN.state, where "false" stops (de-activates) the trunk and "true" activates the trunk.

4.15.2 Resolved Constraints

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

Table 4-22: Resolved Constraints for Patch Version 6.80M.591.004

Incident	Description
142794	Running the CLI command **display-device-log** causes the device to crash (reset).
146100	On rare occasions when loading a .cmp file to the device through TR-069, a BOOT event is not sent to the ACS server after the device resets.

4.16 Patch Version 6.80A.352

This patch version includes new features and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.346.005.
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL (Only EFM)
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.16.1 New Features

New features introduced in this version include the following:

- Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED) support on the Gigabit Ethernet WAN port (0/0), allowing the device to function as an LLDP client.
- Configuration of rapid-commit for PPPoE interfaces.
- Support for DMZ host.
- Copying DSL firmware using HTTP or HTTPS server.
- Clearing statistics of the maximum round-trip time (RTT) of packets for all tracks or optionally, per track ID
- Support for Gratuitous ARP per interface with timer.

4.16.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-23: Known Constraints for Patch Version 6.80A.352

Incident	Description
147299	For Y.1731 configuration, the device crashes when you start the LCK signal and then try to stop it.
147416	The VLAN interface flaps if it is configured under the Ethernet CFM process.

4.16.3 Resolved Constraints

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

Table 4-24: Resolved Constraints for Patch Version 6.80A.352

Incident	Description
142255	DNS static IP host configuration issues (IPv4 and IPv6).
145144	Traffic is not encrypted when the destination in IPsec ACL is 'any to any'.
145360	OSPF does not function when a static BFD and OSPF neighbor are configured.
145361	BFD configuration is not displayed in the output of the **show run data interface** command.
145396	The **ipv6 dhcp-client ntp-server** command is not displayed in the output of the **show run** command for the PPP interface.
145440	IPv6 mechanism doesn’t function if the IPv4 server operates slowly or doesn’t function at all.
145514	Track starting state for IPv6 is incorrect (INIT instead of DOWN).
145787	Track IPv6 displays garbage value for "max rtt" after a device reload.
145980	FQDN (host name) is missing in the access-list menu.
146088	The output of the ? symbol entered for ipsec lifetime is incorrect; the maximum lifetime of ISAKMP is 86400 seconds and not 28800.
146165	OSPF configuration is not removed properly.
146777	CDC dongle doesn't acquire an IP address when ACL is set on the VoIP side.
146213	For the Single Network Mode (SNM), the override acl feature does not function under VRF.
146615	Encrypted data over IPsec together with unencrypted voice traffic doesn't function correctly; the voice traffic gets encrypted.
146776	For Single Network Mode (SNM), encrypted data over IPsec together with unencrypted voice traffic doesn't operate correctly; the voice traffic gets encrypted

4.17 Patch Version 6.80A.358.003

This patch version includes new features and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.346.005.
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL (Only EFM)
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.17.1 New Features

New features introduced in this version include the following:

- Configuration of a secondary DHCP relay agent.
- The device is now aware of DSCP markings in IPsec tunneling when in NAT-T mode.
- Configuration of a specific bind per management server (snmp|http|https|telnet|ssh).

4.17.2 Resolved Constraints

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

Table 4-25: Resolved Constraints for Patch Version 6.80A.358.003

Incident	Description
145343	The **no shutdown** command does not appear in the running configuration under the ATM interface.
147164	Gratuitous ARP is sent even if there is no IP address configuration for the interface.
147209	QoS calibration on VDSL/EFM lines.
147243	More than 100 DHCP clients are not visible in the **show data hosts** command output.
147299	On Y.1731 interface, the device crashes when starting and then stopping the LCK signal.
147640	The access-list does not deny IPv6 traffic on PPPoE interface after the **shut** or **no shut** command is run.

Incident	Description
147788	The value of the TR069PERIODICINFORMINTERVAL is not saved to configuration.
147979	The **aaa authentication login tacacs+ allow-console-bypass authentication authorization** command does not survive after device reboot.
148324	For TR-069, the digest authentication message is sent in the wrong format.
148394	When the WAN interface is configured on VRF, the autoupdate and copy features do not function if DNS resolution is required.
148587	Wi-Fi "krack" vulnerability has been resolved.
149079	The cellular dongle E3372h-153 signal strength displays -1dBm for the status of the cellular interface.
149742	For TR-069, manual URL doesn't function as accepted when using ACS DownloadDiagnostics.
149650	No capability to configure tunnel authentication key for L2TP interface.
149430	In IPSec, during quick negotiation, when the peer presents a transform set that includes the SHA-512 authentication algorithm, this algorithm ID is interpreted as a syntax error and not as a non-supported transform set. As a result, the syntax errors result in the rejection of the entire transaction without considering other possible proposals.
149478	For DHCP server functionality, the distribution of IP addresses is done only to authorized hosts (static hosts).

4.18 Patch Version 6.80A.365.002

This patch version includes new features and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.346.005.
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL (Only EFM)
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.18.1 New Features

New features introduced in this version include the following:

- RFC 2833 DTMF to SIP INFO (and vice versa) on RTP forwarding sessions without consuming DSP resources.
- Hostname resolving on IPv6 access list, supported by the following new command:

```
ipv6 access-list [Number or Word] deny ipv6 host [Host IPv6 Address]
```

- DNS lookup queries per specific VRF, supported by the following new command:

```
nslookup [Hostname] source data vrf [VRF Name]
```

- SHA-256 support for the following IPSec operations:
  1. IKEv1 main mode hashing
  2. IKEv1 main mode certificate signature handling when hashed with SHA-256
  3. IPSec HMAC-SHA-256

```
(config-data)# crypto isakmp policy 19
(config-isakmp)# hash
```

- RSA to IPSec is now supported, using the following new command:

```
crypto isakmp policy 10
encr aes 128
authentication rsa-sig
```

- When enabling the DHCPv4 auto NTP feature, the device sends the NTP IP addresses or hostname it used for the clients on the interface on which the feature is

configured. To support this feature, the following new command has been added:

```
(conf-if-VLAN 1)# ip dhcp-server ntp-server auto
```

- Diffie-Hellman (DH) groups 14,15 and 16 in IPSec is now supported.
- SNMP support for the IPSec table.
- Improved user management experience upon heavy traffic.

4.18.2 Resolved Constraints

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

Table 4-26: Resolved Constraints for Patch Version 6.80A.365.002

Incident	Description
145311	The Access List (**access-list**) with host name resolution does not function with VRF.
148394	When the WAN interface is configured on a VRF, the Automatic Update and copy features do not operate if DNS resolution is required.
148648	Under some conditions, the INI file cannot be loaded using the Automatic Update mechanism (IniFileURL parameter).
149093	Loading autorun file via USB fails.
149571	The device does not issue a new DHCP discover after the DHCP server goes down. Only non-multiple WAN platforms are affected.
151347	CWMP packets are sent with the "dont fragment" flag even for packets that require fragmentation. To resolve this constraint, a new command has been added to enable fragmentation (default is off): (cwmp-tr069)# **tcp-fragment on/off**
130468	ACL FQDN has been added to support multiple IP address.
150691	In some scenarios, DNS resolution uses a port that is intended for VoIP traffic.
151441	Old IPV6-PD prefixes that are being delegated cannot be cleared.
150378	L2TP server using loopback is not functioning properly.
151442	IPv6PD Lifetime advertised by the device is different than that advertised by the server.
149319	When the IPSec tunnel is down, encrypted traffic is still being routed (even though it should not be).

4.19 Patch Version 6.80M.597

This patch version includes new features and resolved constraints.

Note:

- This patch version is a derivative of Version 6.80A.365.002 (see Section 4.18).
- This patch version is applicable **only to TR-181 customers** (coordinated with AudioCodes).
- This patch version is applicable only to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interface:
  - √ A/VDSL ISDN

4.19.1 New Features

New features introduced in this version include the following:

- Support for the following new TR-104 V2.5 parameters:
  - Device.Services.VoiceService.{i}.NetworkProfile.{i}.Line [Subtree]
  - Device.Services.VoiceService.{i}.NetworkProfile.{i}.SIPLine [Subtree]
  - Device.VoiceService.{i}.NetworkProfile.{i}.SIP [Subtree]
  - Device.VoiceService.{i}.NetworkProfile.{i}.STUNServer.

  For more information, refer to the *TR-069 for DTAG Reference Guide Ver. 6.8*.
- Read-write (RW) permissions are now allowed for the following parameters:
  - Device.Services.VoiceService.{i}.NetworkProfile.{i}.Enable
  - Device.Services.VoiceService.{i}.NetworkProfile.{i}.Name
  - Device.Services.VoiceService.{i}.NetworkProfile.{i}.SignalingProtocol
- New access control mechanism has been added (TR-069 Provisioning code).

4.19.2 Resolved Constraints

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

Table 4-27: Resolved Constraints for Patch Version 6.80M.597

Incident	Description
151647	For TR-069, the GetValueResponse of Device.ManagementServer.ConnectionRequestPassword should return an empty string.

4.20 Patch Version 6.80A.369.004

This patch version includes new features and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.346.005.
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL (Only EFM)
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.20.1 New Features

New features introduced in this version include the following:

- New SNMP objects - acSysIdProductClass and acSysIdModelName.
- Support for QoS to Layer-2 Tunneling Protocol (L2TP) clients.

4.20.2 Resolved Constraints

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

Table 4-28: Resolved Constraints for Patch Version 6.80A.369.004

Incident	Description
152855	Loading the Startup Script file from the Axiros ACS takes a long time.
152998	DTMF transcoding does not function without DSP resources for RTP forwarding sessions (RFC 2833 DTMF to SIP INFO, and vice versa). (No DSPs should be used.)
153185	BGP doesn't redistribute network permitted by route-map with prefix-list.
153484	Minor errors during startup.
153652	NATPR resolve-method type doesn't operate correctly.

4.21 Patch Version 6.80A.371.003

This patch version includes new features and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.346.005.
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL (Only EFM)
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.21.1 New Features

New features introduced in this version include the following:

- Improved L2TP performance.

4.21.2 Known Constraints

Additional constraints discovered in this patch version include the following:

Table 4-29: Known Constraints for Patch Version 6.80A.371.003

Incident	Description
-	In some scenarios, the device may not have sufficient DSP resources to process the number of SBC transcoding sessions as configured by the MediaChannels parameter. The parameter must be configured to 8 (i.e., maximum 4 transcoding sessions) and not more to allow SBC transcoding by Mediant 500L.

4.21.3 Resolved Constraints

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

Table 4-30: Resolved Constraints for Patch Version 6.80A.371.003

Incident	Description
154045	When configuring a rule for match address local-voip in dns-view (**conf data** > **dns-view 2** > **match source address local-voip**), the output of the **show run** command is incorrect.
155231	If an upgrade process is initiated during another upgrade process, the device crashes.
155368	During the Automatic Update process, the commands **write factory** and **reload** do not function.

4.22 Patch Version 6.80A.375.004

This patch version includes new features and resolved constraints.

Note:

- This patch version corresponds to the SBC/Gateway patch version 6.80A.346.005.
- This patch version is applicable **only** to the following MSBR devices:
  - √ Mediant 500 MSBR
  - √ Mediant 500L MSBR
  - √ Mediant 800 MSBR
- This patch version is applicable only to the following physical WAN interfaces:
  - √ Copper
  - √ Cellular
  - √ Fiber
  - √ SHDSL (Only EFM)
  - √ A/VDSL ISDN
  - √ A/VDSL POTS
  - √ T1-WAN
- The following software features are not supported in this patch version:
  - √ Auto VPN
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to the latest software version, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to the latest software version.

4.22.1 New Features

New features introduced in this version include the following:

- If the TLS Context at Index 0 uses a self-signed certificate and the certificate is about to expire per local time on the device (less than 1 day), or has expired already, then the device will generate a new self-signed certificate that will be valid per local time on device.

4.22.2 Resolved Constraints

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

Table 4-31: Resolved Constraints for Patch Version 6.80A.375.004

Incident	Description
155857	The Welcome message in the management interfaces is not displayed correctly.
156153	In certain configuration scenarios, no data transmission is possible due to memory allocation failure.
153947	The BRI line doesn't synchronize in certain scenarios.
155828	The **debug reset-history** command displays the "– More –" prompt even if the window height configuration (**default-window-height**) is changed.
156154	An unexpected device restart occurred due to an exception in some cases with overlap dialing.

This page is intentionally left blank.

5 SBC Session and DSP Channel Capacities

This chapter provides capacity figures per product supported in Release 6.8.

5.1 Signaling, Media and User Registration Capacity

The table below lists the maximum SIP signaling sessions, call (media) sessions, and registered users per product.

Table 5-1: Maximum Signaling, Call Sessions and Registered Users

Product	Signaling Sessions	Media Sessions			Registered Users
		RTP-to-RTP	SRTP-RTP or SRTP-TDM	Codec Transcoding	
Mediant 500 E-SBC	250	250	180	-	0
	250	100	60	-	800
Mediant 500 MSBR	180	100	100	-	600
Mediant 500L MSBR	60	60	60	-	200
Mediant 800 Gateway & E-SBC	60	60	60	See Table 5-7	200
Mediant 800B Gateway & E-SBC	250	250	180	See Table 5-7	0
	250	100	60	See Table 5-7	800
Mediant 800 MSBR	60	60	60	See Table 5-8	200
Mediant 800B MSBR	180	100	100	See Table 5-8	600
Mediant 1000B Gateway & E-SBC	150	150	120	96	600
Mediant 3000 Gateway & E-SBC	1008	1,008	1,008	1,008	3,000 (5,000 Depop.)
Mediant 2600 E-SBC	600	600	600	See Table 5-17	8,000
Mediant 4000 SBC	5000	5000	3000	See Table 5-18	20,000
Mediant 4000B SBC	5000	5000	3000	See Table 5-19	20,000
Mediant 9000 SBC	6,000	4,000	4,000	-	36,000

Product		Signaling Sessions	Media Sessions			Registered Users
			RTP-to-RTP	SRTP-RTP or SRTP-TDM	Codec Transcoding	
		16,000	16,000	12,000	-	0
Mediant SE SBC	Low Capacity	5,000	5,000	4,500	-	25,000
	High Capacity	6,000	4,000	4,000	-	36,000
		16,000	16,000	12,000	-	0
Mediant VE SBC	Low Capacity ESXi VMware or Hyper-V	250	250	250	-	1,000
	High Capacity ESXi VMware only	2,000	2,000	1,500	-	6,000

Notes:

- The 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 sales representative.
- *Registered Users* is the maximum number of users that can be registered with the device. Depending on product, this applies to the supported application (SBC, CRP, and/or IP-to-IP Gateway).
- Regarding signaling, media, and transcoding session resources:
  - √ A signaling session is a SIP dialog session between two SIP entities, traversing the SBC and using one signaling session resource.
  - √ A media session is an audio (RTP or SRTP), fax (T.38), or video session between two SIP entities, traversing the SBC and using one media session resource.
  - √ A gateway session (i.e. TDM-RTP or TDM-SRTP) is also considered as a media session for the calculation of media sessions. In other words, the maximum Media Sessions specified in the table refer to the sum of gateway sessions and SBC sessions.
  - √ In case of direct media (i.e., Anti-tromboning / Non-Media Anchoring), where only SIP signaling traverses the SBC and media flows directly between the SIP entities, only a signaling session resource is used. Thus, for products with a greater signaling session capacity than media, even when media session resources have been exhausted, additional signaling sessions can still be handled for direct-media calls.
  - √ For call sessions requiring transcoding, one transcoding session resource is also used. For example, for a non-direct media call in which one leg uses G.711 and the other leg uses G.729, one signaling resource, one media session resource, and one transcoding session resource is used.
- The capacity figures for Mediant VE are for running on the recommended platforms only, when there are no other virtual machines (VM) running on these platforms.

5.2 Mediant 500 E-SBC

The SBC session capacity and DSP channel capacity for Mediant 500 E-SBC are shown in the tables below.

Table 5-2: Mediant 500 E-SBC (Non Hybrid) SBC Session Capacity

Hardware Configuration	DSP Channels Allocated for PSTN	Wideband Coders			Max. SBC Sessions (RTP to RTP)
		G.722	AMR WB	SILK WB	
SBC	N/A	N/A	N/A	N/A	250

Table 5-3: Mediant 500 Hybrid E-SBC (with Gateway) Media Capacity

Hardware Configuration	DSP Channels Allocated for PSTN	Wideband Coders			Max. SBC Sessions (RTP to RTP)
		G.722	AMR WB	SILK WB	
1 x E1/T1	30/24	√	-	-	220/226
	26/24	-	√	-	224/226
	24/24	-	-	√	226/226

5.3 Mediant 500 MSBR

The channel capacity and SBC session capacity for Mediant 500 MSBR are shown in the table below.

Table 5-4: Mediant 500 MSBR Capacity per PSTN Assembly and Capabilities

Telephony Interface Assembly	DSP Channels Allocated for PSTN	Max. SBC Sessions
1 x E1/T1	30/24	150/156
4 x BRI	8	172
1/2/3 x BRI	2/4/6	178/176/174
4 x FXS or 4 x FXO	4	176
FXS, FXO, and/or BRI, but none in use	0	180

Notes:

- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- Three-way conferencing is supported by the analog ports.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

5.4 Mediant 500L MSBR

The channel capacity and SBC session capacity for Mediant 500L MSBR are shown in the table below.

Table 5-5: Mediant 500L MSBR Capacity per PSTN Assembly and Capabilities

Telephony Interface Assembly	DSP Channels Allocated for PSTN	Max. SBC Sessions
4 x FXS & 4 x FXO	8	52
2 x BRI & 2 x FXS	6	54
2 x BRI	4	56
4 x FXS	4	56
FXS, FXO, and/or BRI, but not in use	0	60

Notes:

- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- Three-way conferencing is supported by the analog ports.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

5.5 Mediant 800/B Gateway & E-SBC

The DSP channel capacity and SBC session capacity for Mediant 800 Gateway & E-SBC and Mediant 800B Gateway & E-SBC are shown in the tables below.

Table 5-6: Mediant 800/B Gateway & E-SBC SBC Session Capacity per Capabilities (Only SBC)

Hardware Configuration	DSP Channels Allocated for PSTN	SBC Transcoding Sessions									Conf. Participants	Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities							To Profile 1	To Profile 2		Mediant 800	Mediant 800B
		SBC Enhancements	IPM Detectors	G.722	AMR WB	SILK NB / iLBC	SILK WB	V.150.1					
SBC	N/A	-	-	-	-	-	-	-	45	42	-	60	250
	N/A	-	-	√	-	-	-	-	45	39	-	60	250
	N/A	√	-	-	-	-	-	-	45	36	-	60	250
	N/A	√	-	√	-	-	-	-	39	33	-	60	250
	N/A	-	-	-	-	√	-	-	36	30	-	60	250
	N/A	-	-	-	√	√	√	-	27	21	-	60	250
	N/A	√	-	-	-	√	-	-	30	24	-	60	250
	N/A	√	-	-	√	√	√	-	24	21	-	60	250

Table 5-7: Mediant 800/B Gateway & E-SBC Channel Capacity per Capabilities (Only Gateway)

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions									Conf. Participants	Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities							To Profile 1	To Profile 2		Mediant 800	Mediant 800B
		SBC Enhancements	IPM Detectors	G.722	AMR WB	SILK NB / iLBC	SILK WB	V.150.1					
2 x E1/T1	60/48	-	-	-	-	-	-	-	4/12	3/11	-	0/12	190/202
2 x T1	48	-	√	-	-	-	-	√	9	7	-	12	202
1 x E1/T1 & FXS/FXO Mix x 8	38/32	-	√	-	-	-	-	-	16/21	14/18	-	22/28	212/218
	38/32	-	√	-	-	√	-	-	3/7	2/6	-	22/28	212/218
1 x E1/T1	30/24	-	√	-	-	√	-	√	9/14	7/11	-	30/36	220/226
1 x E1 & 4 x BRI	38	-	√	-	-	-	-	-	16	14	-	22	215
1 x E1 & 4 x FXS	34	-	√	-	-	-	-	-	19	16	-	26	216
2 x E1 & 4 x FXS	64	-	-	-	-	-	-	-	0	0	-	0	186
4 x BRI & 4 x FXS & 4 x FXO	16	-	√	-	-	-	-	-	3	2	-	44	234
8 x BRI & 4 x FXS	20	-	√	-	-	-	-	-	1	1	-	40	230
8 x BRI	16	-	√	-	-	-	-	-	3	2	-	44	234
12 x FXS	12	-	√	-	-	√	-	√	1	1	-	48	238
4 x FXS & 8 x FXO	12	-	√	-	-	√	-	-	1	1	-	48	238
8 x FXS & 4 x FXO	12	-	√	-	-	√	-	-	1	1	-	48	238
4 x BRI & 4 x FXS	12	-	√	-	-	√	-	-	1	1	-	48	238
4 x FXS & 4 x FXO	8	-	-	-	-	-	-	-	9	8	6	52	242
	8	-	√	-	-	√	-	-	4	3	-	52	242
4 x BRI	8	-	-	-	-	-	-	-	9	8	6	52	242
	8	-	√	-	-	√	-	-	4	3	-	52	242
1/2/3 x BRI	2/4/6	-	-	-	-	-	-	-	13/12/10	12/11/10	-	58/56/54	248/246/244
	2/4/8	-	√	-	-	√	-	-	7/4/1	6/3/1	-	58/56/54	248/246/244
4 x FXS	4	-	-	-	-	√	-	√	7	6	-	56	246

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions									Conf. Participants	Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities							To Profile 1	To Profile 2		Mediant 800	Mediant 800B
		SBC Enhancements	IPM Detectors	G.722	AMR WB	SILK NB / iLBC	SILK WB	V.150.1					
or 4 x FXO	4	-	-	√	-	-	-	-	12	10	8	56	246
	4	-	-	-	-	√	-	-	8	7	7	56	246
	4	-	√	-	√	√	-	-	7	6	4	56	246
	4	-	√	-	√	√	√	-	5	4	4	56	246
FXS, FXO, and/or BRI, but not in use	0	-	-	-	-	-	-	-	15	14	-	60	250

Notes:

- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729, G.723.1, and AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- *SBC Enhancements* includes the network Acoustic Echo Suppressor.
- *IPM Detectors* includes Automatic Gain Control (AGC) and Answer Detector (AD).
- V.150.1 is supported only for the US Department of Defense (DoD).
- *Transcoding Sessions* represents part of the total SBC Sessions.
- *Conference Participants* represents the number of participants in one or more conference (bridge), where each conference may include three or more participants. Conferences are supported on all above configurations. For figures on the maximum number of participants per configuration, please contact your AudioCodes sales representative.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

5.6 Mediant 800/B MSBR

The DSP channel capacity and SBC session capacity for Mediant 800 MSBR and Mediant 800B MSBR are shown in the table below.

Table 5-8: Mediant 800/B MSBR Channel Capacity per PSTN and Capabilities

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions								Conf. Participants	Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities						To Profile 1	To Profile 2		Mediant 800	Mediant 800B
		IPM Detectors	G.722	AMR WB	SILK NB / iLBC	SILK WB	V.150.1					
2 x E1/T1	60/48	-	-	-	-	-	-	4/12	3/11	-	0/12	120/132
2 x T1	48	√	-	-	-	-	√	9	7	-	12	132
1 x E1/T1 & 8 x FXS/FXO Mix	38/32	√	-	-	-	-	-	16/21	14/18	-	22/28	142/148
	38/32	√	-	-	√	-	-	3/7	2/6	-	22/28	142/148
1 x E1/T1	30/24	√	-	-	√	-	√	9/14	7/11	-	30/36	150/156
1 x E1 & 4 x BRI	38	√	-	-	-	-	-	16	14	-	22	145
1 x E1 & 4 x FXS	34	√	-	-	-	-	-	19	16	-	26	146
2 x E1 & 4 x FXS	64	-	-	-	-	-	-	0	0	-	0	116
4 x BRI & 4 x FXS & 4 x FXO	16	√	-	-	-	-	-	3	2	-	44	164
8 x BRI & 4 x FXS	20	√	-	-	-	-	-	1	1	-	40	160
8 x BRI	16	√	-	-	-	-	-	3	2	-	44	164
12 x FXS	12	√	-	-	√	-	√	1	1	-	48	168
4 x FXS & 8 x FXO	12	√	-	-	√	-	-	1	1	-	48	168
8 x FXS & 4 x FXO	12	√	-	-	√	-	-	1	1	-	48	168
4 x BRI & 4 x FXS	12	√	-	-	√	-	-	1	1	-	48	168
4 x FXS & 4 x FXO	8	-	-	-	-	-	-	9	8	6	52	172
	8	√	-	-	√	-	-	4	3	-	52	172
4 x BRI	8	-	-	-	-	-	-	9	8	6	52	172
	8	√	-	-	√	-	-	4	3	-	52	172
1/2/3 x BRI	2/4/6	-	-	-	-	-	-	13/12/10	12/11/10	-	56/52/48	176/172/168
	2/4/6	√	-	-	√	-	-	9/7/6	7/6/5	-	56/52/48	176/172

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions								Conf. Participants	Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities						To Profile 1	To Profile 2		Mediant 800	Mediant 800B
		IPM Detectors	G.722	AMR WB	SILK NB / iLBC	SILK WB	V.150.1					
												/168
4 x FXS or 4 x FXO	4	-	-	-	√	-	√	7	6	-	56	176
	4	-	√	-	-	-	-	12	10	8	56	176
	4	-	-	-	√	-	-	8	7	7	56	176
	4	√	-	√	√	-	-	7	6	4	56	176
	4	√	-	√	√	√	-	5	4	4	56	176
FXS, FXO, and/or BRI, but not in use	0	-	-	-	-	-	-	15	14	-	60	180

Notes:

- *Profile 1*: G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2*: G.711, G.726, G.729, G.723.1, and AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- *IPM Detectors* includes Automatic Gain Control (AGC) and Answer Detector (AD).
- V.150.1 is supported only for the US Department of Defense (DoD).
- *Transcoding Sessions* represents part of the total SBC Sessions.
- *Conference Participants* represents the number of participants in one or more conference (bridge), where each conference may include three or more participants. Conferences are supported on all above configurations. For figures on the maximum number of participants per configuration, please contact your AudioCodes sales representative.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

5.7 Mediant 1000B Gateway & E-SBC

This section lists the channel capacity and DSP templates for Mediant 1000B Gateway & E-SBC DSP, for the following interfaces:

- Analog (FXS/FXO) – see Section 5.7.1 on page 243
- Digital interfaces – see Section 5.7.2 on page 244
- Media processing interfaces (MPM module) – see Section 5.7.4 on page 246

Notes:

- The maximum number of channels on any form of analog, digital, and MPM module assembly is 192. When the device handles both SBC and Gateway call sessions, the maximum number of total sessions is 150.
- Installation and use of voice coders is subject to obtaining the appropriate license and royalty payments.
- For additional DSP templates, contact your AudioCodes sales representative.

5.7.1 Analog (FXS/FXO) Interfaces

The channel capacity per DSP firmware template for analog interfaces is shown in the table below.

Table 5-9: Channel Capacity per DSP Firmware Template for Mediant 1000B Analog Series

	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.726 ADPCM	√	√
G.723.1	√	√
G.729 A, B	√	√
G.722	-	√

5.7.2 BRI Interfaces

The channel capacity per DSP firmware template for BRI interfaces is shown in the table below.

Table 5-10: Channel Capacity per DSP Firmware Template for Mediant 1000B BRI Series

	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.726 ADPCM	√			√		
G.723.1	√			√		
G.729 A, B	√			√		
G.722	-			√		

5.7.3 E1/T1 Interfaces

The channel capacity per DSP firmware template for E1/T1 interfaces is shown in the table below.

Table 5-11: Channel Capacity per DSP Firmware Templates for Mediant 1000B E1/T1 Series

	DSP Template																			
	0 or 10				1 or 11				2 or 12				5 or 15				6 or 16			
	Number of Spans																			
	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8
	Number of Channels																			
Default settings	31	62	120	192	31	48	80	160	24	36	60	120	24	36	60	120	31	60	100	192
With 128 ms EC	31	60	100	192	31	48	80	160	24	36	60	120	24	36	60	120	31	60	100	192
With SRTP	31	62	120	192	31	48	80	160	24	36	60	120	24	36	60	120	31	60	100	192
With IPM Features[1]	31	60	100	192	-	-	-	-	-	-	-	-	-	-	-	-	31	60	100	192
With IPM Features & SRTP	31	60	100	192	-	-	-	-	-	-	-	-	-	-	-	-	31	60	100	192
Voice Coder																				
G.711 A-law/Mμ-law PCM	✓				✓				✓				✓				✓			
G.726 ADPCM	✓				✓				✓				✓				-			
G.723.1	✓				-				-				-				-			
G.729 A, B	✓				✓				✓				✓				✓			
GSM FR	✓				✓				-				-				-			
MS GSM	✓				✓				-				-				-			
iLBC	-				-				-				✓				-			
EVRC	-				-				✓				-				-			
QCELP	-				-				✓				-				-			
AMR	-				✓				-				-				-			
GSM EFR	-				✓				-				-				-			
G.722	-				-				-				-				✓			
Transparent	✓				✓				✓				✓				✓			

[1] 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.

5.7.4 Media Processing Interfaces

The channel capacity per DSP firmware template for media processing (provided by the MPM module) is shown in the table below

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 5-12: Channel Capacity per DSP Firmware Template for Mediant 1000B MPM Series

			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.726 ADPCM			✓		✓		✓		✓		-	
G.723.1			✓		-		-		-		-	
G.729 A, B			✓		✓		✓		✓		✓	
GSM FR			✓		✓		-		-		-	
MS GSM			✓		✓		-		-		-	
iLBC			-		-		-		✓		-	
EVRC			-		-		✓		-		-	
QCELP			-		-		✓		-		-	
AMR			-		✓		-		-		-	
GSM EFR			-		✓		-		-		-	
G.722			-		-		-		-		✓	
Transparent			✓		✓		✓		✓		✓	

5.8 Mediant 3000

This section lists the supported channel capacity per DSP template of Mediant 3000 for the following:

- Mediant 3000 full chassis – see Section 5.8.1 on page 248
- Mediant 3000 with 16 E1 / 21 T1 – see Section 5.8.2 on page 249
- Mediant 3000 with single T3 – see Section 5.8.3 on page 251
- DSP template mix feature – see Section 5.8.4 on page 252

Notes:

- Installation and use of voice coders is subject to obtaining the appropriate license and royalty payments.
- For additional DSP templates, contact your AudioCodes sales representative.

5.8.1 Mediant 3000 Full Chassis

The channel capacity per DSP firmware template is shown in the table below.

Table 5-13: Channel Capacity per DSP Firmware Template for Mediant 3000

					DSP Template										
					0	1	2	4	5	7	9	10	11	12	13
Supplementary Capabilities					Number of Channels										
SRTP	ARIA	RTCP XR	IPM Detectors	Acoustic Echo Suppressor											
-	-	-	-	-	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.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					-	-	-	-	-	-	-	✓	-	-	-

5.8.2 Mediant 3000 16 E1 / 21 T1

The channel capacity per DSP firmware template for Mediant 3000 with 16 E1 / 21 T1 is 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 5-14: Channel Capacity per DSP Firmware Templates for Mediant 3000 16 E1 / 21 T1

					DSP Template								
					0	1	2	4	5	7	9	10	11
Supplementary Capabilities					Number of Channels								
SRTP	ARIA	RTCP XR	IPM Detectors	Acoustic Echo Suppressor									
-	-	-	-	-	504	504	504	360	360	468	288	432	180
-	-	✓	✓	-	504	504	468	324	324	468	288	432	180
-	-	-	-	✓	324	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.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					-	-	-	-	-	-	-	✓	-

5.8.3 Mediant 3000 with Single T3

The channel capacity per DSP firmware template for Mediant 3000 with a single T3 interface is shown in the table below.

Table 5-15: Channel Capacity per DSP Firmware Templates for Mediant 3000 with Single T3

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								
-	-	-	-	-	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.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					-	-	-	-	-	-	-	✓	-

5.8.4 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 5-16: Channel Capacity of DSP Template Mix Feature for Mediant 3000

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

5.9 Mediant 2600 E-SBC

The maximum number of supported SBC sessions is shown in Section 5.1 on page 235. 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 5-17: Channel Capacity per Coder-Capability Profile for Mediant 2600 E-SBC

Session Coders		Number of Sessions	
From Coder Profile	To Coder	Without MPM4	With MPM4
1	Profile 1	375	600
2	Profile 1	275	600
2	Profile 2	225	600
1	Profile 2 + G.722	225	600
2	Profile 2 + G.722	175	575
1	Profile 2 + AMR-WB or SILK-NB or iLBC	175	525
2	Profile 2 + AMR-WB or SILK-NB or iLBC	150	450
1	Profile 2 + SILK-WB	100	350
2	Profile 2 + SILK-WB	100	300

Notes:

- *Profile 1:* G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729, G.723.1, AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance by about 30%. For more information, contact your AudioCodes sales representative.
- MPM is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

5.10 Mediant 4000 SBC

The maximum number of supported SBC sessions is listed in Section 5.1 on page 235. 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 5-18: Channel Capacity per Coder-Capability Profile for Mediant 4000 SBC

Session Coders		Number of Sessions	
From Coder Profile	To Coder	Without MPM8	With MPM8
1	Profile 1	750	2300
2	Profile 1	550	1650
2	Profile 2	450	1350
1	Profile 2 + G.722	450	1350
2	Profile 2 + G.722	350	1150
1	Profile 2 + AMR-WB or SILK-NB or iLBC	350	1050
2	Profile 2 + AMR-WB or SILK-NB or iLBC	300	900
1	Profile 2 + SILK-WB	200	700
2	Profile 2 + SILK-WB	200	600

Notes:

- *Profile 1:* G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729, G.723.1, AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance by about 30%. For more information, contact your AudioCodes sales representative.
- MPM is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

5.11 Mediant 4000B SBC

The maximum number of supported SBC sessions is listed in Section 5.1 on page 235. 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 5-19: Channel Capacity per Coder-Capability Profile for Mediant 4000B SBC

Session Coders		Number of Sessions			
From Coder	To Coder	Without MPM	1 x MPM8B	1 x MPM12B	2 x MPM12B
Profile 1	Profile 1	750	2300	2300	2300
Profile 2	Profile 1	550	1700	2300	2300
Profile 2	Profile 2	450	1350	1800	2300
Profile 1	Profile 2 + G.722	450	1350	1800	2300
Profile 2	Profile 2 + G.722	350	1150	1500	2300
Profile 1	Profile 2 + AMR-WB or SILK-NB or iLBC	350	1050	1400	2300
Profile 2	Profile 2 + AMR-WB or SILK-NB or iLBC	300	900	1200	2150
Profile 1	Profile 2 + SILK-WB	200	700	950	1650
Profile 2	Profile 2 + SILK-WB	200	600	850	1500

Notes:

- *Profile 1:* G.711 at 20ms only, with In-band signaling (in voice channel) and Silence Suppression (no fax detection or T.38 support).
- *Profile 2:* G.711, G.726, G.729, G.723.1, AMR-NB, T.38 with fax detection, In-band signaling (in voice channel), and Silence Compression.
- Acoustic Echo Suppressor reduces performance by about 30%. For more information, contact your AudioCodes sales representative.
- MPMB is the optional, Media Processing Module that provides additional DSPs, allowing greater capacity.

5.12 Mediant 9000 SBC

Note: Mediant 9000 SBC does not implement digital signal processing (DSP). Therefore, it supports only SBC functionalities that do not require media signal processing.

5.13 Mediant Server Edition SBC

Note: Mediant Server Edition SBC does not implement digital signal processing (DSP). Therefore, it supports only SBC functionalities that do not require media signal processing.

5.14 Mediant Virtual Edition SBC

Note: Mediant Virtual Edition SBC does not implement digital signal processing (DSP). Therefore, it supports only SBC functionalities that do not require media signal processing.

6 Supported SIP Standards

6.1 Supported SIP RFCs

The table below lists the supported RFCs.

Table 6-1: Supported RFCs

RFC	Description	Gateway	SBC
RFC 6341	Use Cases and Requirements for SIP-Based Media Recording (Session Recording Protocol - draft-ietf-siprec-protocol-02, and Architecture - draft-ietf-siprec-architecture-03)	Yes	Yes
RFC 6140	Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)	Yes	Yes
RFC 5853	Requirements from SIP / SBC Deployments	-	Yes
RFC 4566	Session Description Protocol	Yes	Yes
RFC 2976	SIP INFO Method	Yes	Yes
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 -

RFC	Description	Gateway	SBC
			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 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 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	Yes	Yes -

RFC	Description	Gateway	SBC
	transparent call - Clearmode		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 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	Description	Gateway	SBC
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	Yes
ECMA-355, ISO/IEC 22535	QSIG tunneling	Yes	Yes - forwarded transparently
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

6.2 SIP Message Compliancy

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

6.2.1 SIP Functions

The device supports the following SIP Functions:

Table 6-2: 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

6.2.2 SIP Methods

The device supports the following SIP Methods:

Table 6-3: 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	-

6.2.3 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

6.2.4 SDP Fields

The device supports the following SDP fields:

Table 6-4: 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

SDP Field	Name
e=	Email address header
i=	Session info header
p=	Phone number header
y=	Year

6.2.5 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

6.2.5.1 1xx Response – Information Responses

Table 6-5: 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

6.2.5.2 2xx Response – Successful Responses

Table 6-6: Supported 2xx SIP Responses

2xx Response	
200	OK
202	Accepted

6.2.5.3 3xx Response – Redirection Responses

Table 6-7: 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.

6.2.5.4 4xx Response – Client Failure Responses

Table 6-8: 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.

4xx Response		Comments
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.
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.

4xx Response		Comments
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.

6.2.5.5 5xx Response – Server Failure Responses

Table 6-9: 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	

6.2.5.6 6xx Response – Global Responses

Table 6-10: 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	

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
200 Cottontail Lane
Suite A101E
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

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

Document #: LTRT-27389