

# MSBR Series and MediaPack™ 5xx Series

Version 7.2

---

## Table of Contents

---

<b>Notice.....</b>	<b>vii</b>
Security Vulnerabilities.....	vii
WEEE EU Directive.....	vii
Customer Support.....	vii
Stay in the Loop with AudioCodes.....	vii
Abbreviations and Terminology.....	vii
Related Documentation.....	vii
Document Revision Record.....	viii
Documentation Feedback.....	ix
<b>1 Introduction.....</b>	<b>10</b>
1.1 Software Revision Record.....	10
1.2 Supported Products.....	12
1.2.1 MSBR Series.....	12
1.2.2 MediaPack 5xx Series.....	12
1.3 Product Naming Convention.....	13
<b>2 Released Versions.....</b>	<b>14</b>
2.1 Version 7.28A.356.286.....	14
2.1.1 Resolved Constraints.....	14
2.2 Version 7.28A.356.277.....	15
2.2.1 New Features.....	15
2.2.2 Resolved Constraints.....	19
2.3 Version 7.28A.356.189.....	22
2.3.1 Resolved Constraints.....	22
2.4 Version 7.28A.356.187.....	23
2.4.1 New Features.....	23
2.4.2 Resolved Constraints.....	26
2.5 Version 7.28A.356.070.....	27
2.5.1 New Features.....	27
2.5.2 Resolved Constraints.....	28
2.6 Version 7.28A.356.043.....	29
2.6.1 New Features.....	29
2.6.2 Known Constraints.....	34
2.6.3 Resolved Constraints.....	34
2.7 Version 7.26A.356.899.....	36
2.7.1 Resolved Constraints.....	36
2.8 Version 7.26A.356.888.....	37
2.8.1 New Features.....	37
2.8.2 Resolved Constraints.....	41

---

2.9	Version 7.26A.356.773 .....	42
2.9.1	New Features .....	42
2.9.2	Known Constraints .....	47
2.9.3	Resolved Constraints.....	47
2.10	Version 7.26A.356.630 .....	49
2.10.1	New Features .....	49
2.10.2	Known Constraints .....	53
2.10.3	Resolved Constraints.....	53
2.11	Version 7.26A.356.459 .....	55
2.11.1	New Features .....	55
2.11.2	Known Constraints .....	59
2.11.3	Resolved Constraints.....	59
2.12	Version 7.26A.356.180 .....	61
2.12.1	Known Constraints .....	61
2.13	Version 7.26A.356.174 .....	62
2.13.1	New Features .....	62
2.13.2	Known Constraints .....	64
2.13.3	Resolved Constraints.....	65
2.14	Versions 7.26A.356.070 / 7.26A.356.074 / 7.26A.356.075 .....	67
2.14.1	New Features .....	67
2.14.2	Resolved Constraints.....	73
2.15	Version 7.24A.356.914 .....	77
2.15.1	New Features .....	77
2.15.2	Resolved Constraints.....	78
2.16	Versions 7.24A.356.854 / 7.24A.356.867 .....	79
2.16.1	New Features .....	79
2.16.2	Resolved Constraints.....	82
2.17	Versions 7.24A.356.706 / 7.24A.356.747 .....	85
2.17.1	New Features .....	85
2.17.2	Resolved Constraints.....	87
2.18	Version 7.24A.356.508 .....	90
2.18.1	Resolved Constraints.....	90
2.19	Version 7.24A.356.481 .....	91
2.19.1	New Features .....	91
2.20	Version 7.24A.356.468 .....	91
2.20.1	New Features .....	91
2.20.2	Known Constraints .....	95
2.20.3	Resolved Constraints.....	96
2.21	Version 7.24A.356.263 .....	98
2.21.1	New Features .....	98
2.21.2	Known Constraints .....	99

---

2.21.3	Resolved Constraints .....	99
2.22	Version 7.24A.356.248 .....	100
2.22.1	New Features .....	100
2.22.2	Known Constraints .....	102
2.22.3	Resolved Constraints .....	102
2.23	Version 7.24A.356.069 .....	104
2.23.1	New Features .....	104
2.23.2	Resolved Constraints .....	107
2.24	Version 7.24A.256.329 .....	109
2.24.1	New Features .....	109
2.24.2	Resolved Constraints .....	112
2.25	Version 7.24A.256.219 .....	113
2.25.1	New Features .....	113
2.25.2	Resolved Constraints .....	116
2.26	Version 7.24A.256.105 .....	118
2.26.1	New Features .....	118
2.26.2	Resolved Constraints .....	122
2.27	Version 7.20A.256.125 .....	123
2.27.1	Resolved Constraints .....	123
2.28	Version 7.20A.256.107 .....	123
2.28.1	New Features .....	124
2.28.2	Resolved Constraints .....	126
2.29	Version 7.20A.254.733 .....	126
2.29.1	New Features .....	126
2.30	Version 7.20A.254.026 .....	127
2.30.1	Resolved Constraints .....	128
2.31	Version 7.20A.252.192 .....	129
2.31.1	Resolved Constraints .....	129
2.32	Version 7.20A.252.183 .....	130
2.32.1	New Features .....	130
2.32.2	Resolved Constraints .....	131
2.33	Version 7.20A.252.144 .....	132
2.33.1	New Features .....	132
2.33.2	Resolved Constraints .....	132
2.34	Version 7.20A.252.078 .....	134
2.34.1	Resolved Constraints .....	134
2.35	Version 7.20A.252.062 .....	135
2.35.1	New Features .....	136
2.35.2	Resolved Constraints .....	137
2.36	Version 7.20A.250.028 .....	138
2.36.1	New Features .....	138

---

2.36.2	Resolved Constraints .....	140
2.37	Version 7.20A.202.307 .....	141
2.37.1	New Features .....	141
2.37.2	Resolved Constraints .....	142
2.38	Version 7.20A.202.112 .....	143
2.38.1	New Features .....	143
2.38.2	Resolved Constraints .....	144
2.39	Version 7.20A.200.038 .....	145
2.39.1	New Features .....	145
2.39.2	Resolved Constraints .....	146
2.40	Version 7.20A.154.078 .....	147
2.40.1	New Features .....	147
2.40.2	Resolved Constraints .....	147
2.41	Version 7.20A.154.061 .....	148
2.41.1	Resolved Constraints .....	148
2.42	Version 7.20A.154.025 .....	149
2.42.1	New Features .....	149
2.42.2	Resolved Constraints .....	151
2.43	Version 7.20A.150.004 .....	152
2.43.1	Known Constraints .....	152
<b>3</b>	<b>Capacity .....</b>	<b>154</b>
3.1	SIP Signaling and Media Capacity .....	154
3.2	Detailed Capacity .....	156
3.2.1	Mediant 500 MSBR .....	156
3.2.2	Mediant 500L MSBR .....	156
3.2.3	Mediant 500Li MSBR .....	157
3.2.4	Mediant 800 MSBR .....	158
3.2.5	MediaPack 5xx .....	161
3.3	Session Capacity per Feature .....	163
<b>4</b>	<b>Supported SIP Standards .....</b>	<b>164</b>
4.1	Supported SIP RFCs .....	164
4.2	SIP Message Compliancy .....	169
4.2.1	SIP Functions .....	169
4.2.2	SIP Methods .....	169
4.2.3	SIP Headers .....	170
4.2.4	SDP Fields .....	171
4.2.5	SIP Responses .....	171



## 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: March-30-2026

## Security Vulnerabilities

All security vulnerabilities should be reported to [vulnerability@audiocodes.com](mailto:vulnerability@audiocodes.com).

## WEEE EU Directive

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

## Customer Support

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

## Stay in the Loop with AudioCodes



## Abbreviations and Terminology

The term *MSBR* refers to all the products belonging to the Multi-Service Business Router family.

## Related Documentation

Document Name
<a href="#">MSBR and MediaPack 5xx Series CLI Reference Guide</a>
<b>Hardware</b>
<a href="#">MediaPack 504-508 Hardware Installation Manual</a>
<a href="#">MediaPack 516, 524 &amp; 532 Hardware Installation Manual</a>
<a href="#">Mediant 500 MSBR Hardware Installation Manual</a>
<a href="#">Mediant 500L MSBR Hardware Installation Manual</a>

Document Name
<a href="#">Mediant 500Li MSBR Hardware Installation Manual</a>
<a href="#">Mediant 800 MSBR Hardware Installation Manual</a>
<b>User's Manual</b>
<a href="#">MediaPack 5xx User's Manual</a>
<a href="#">Mediant 500 MSBR User's Manual</a>
<a href="#">Mediant 500L MSBR User's Manual</a>
<a href="#">Mediant 500Li MSBR User's Manual</a>
<a href="#">Mediant 800 MSBR User's Manual</a>
<b>Configuration Note</b>
<a href="#">M5G-EA Cellular Module Hardware Installation and Configuration Guide</a>
<a href="#">Mediant MSBR IP Networking CLI Configuration Guide</a>
<a href="#">Mediant MSBR Layer-2 Bridging CLI Configuration Guide</a>
<a href="#">Mediant MSBR LAN-WAN Access CLI Configuration Guide</a>
<a href="#">Mediant MSBR Security Setup CLI Configuration Guide</a>
<a href="#">Mediant MSBR Basic System Setup CLI Configuration Guide</a>
<a href="#">Troubleshooting the MSBR Configuration Note</a>
<a href="#">Configuring Mediant MSBR Wireless Access Configuration Guide</a>
<a href="#">Recover from Rescue Mode Configuration Note</a>

## Document Revision Record

LTRT	Description
27394	Ver. 7.20A.252.144; initial dedicated document for MSBR
27399	MSBR-8673 added to resolved constraints for Ver. 7.20A.252.144
27442	Ver. 7.20A.254.733
27447	Ver. 7.20A.252.183
27457	Ver. 7.20A.256.107
27463	Ver. 7.20A.252.192
27465	Ver. 7.20A.256.125
27475	Ver. 7.20M1.256.029
27489	Ver. 7.24A.256.105 (replaced version number 7.20M1.256.029)
27495	Ver. 7.24A.256.219
27502	MSBR-9894 added to resolved constraints
27525	Ver. 7.24A.256.329
27544	Ver. 7.24A.356.069

LTRT	Description
27557	Ver. 7.24A.356.248
27563	Ver. 7.24A.356.263
27578	Ver. 7.24A.356.468
27579	Mediant 800 hybrid capacity updated
27585	Ver. 7.24A.356.481
27593	Ver. 7.24A.356.508
27623	Ver. 7.24A.356.706
27626	Ver. 7.24A.356.706 and Ver. 7.24A.356.747
27628	Ver. 7.24A.356.854
27630	Ver. 7.24A.356.867
27643	Ver. 7.24A.356.914; max. TLS connections added
27648	Ver. 7.26A.356.070
27653	Ver. 7.26A.356.074 / 7.26A.356.075 (replaced 7.26A.356.070) and resolved constraints added
27656	Ver. 7.26A.356.070 added to 7.26A.356.074 / 7.26A.356.075
27672	Ver. 7.26A.356.174
27680	Ver. 7.26A.356.180
27683	Ver. 7.26A.356.459
27706	Ver. 7.26A.356.630
27719	Ver. 7.26A.356.773
27733	Ver. 7.26A.356.888
27735	Typo in resolved constraints Ver. 7.26A.356.888
27740	Ver. 7.26A.356.899; capacity for MediaPack 5xx updated
27749	Ver. 7.28A.356.043; Opus capacity for Mediant 800C MSBR
27759	Ver. 7.28A.356.070
27764	Resolved constraints MSBR-19979 and MSBR-19997 added to Ver. 7.28A.356.070
27771	Ver. 7.28A.356.187
27776	Ver. 7.28A.356.189
27782	Ver. 7.28A.356.277
27787	Ver. 7.28A.356.286; RFC 5246 added to RFC list
27790	Capacity updated for Mediant 800C MSBR

## 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 7.2. This includes new products, new hardware features, new software features, known constraints, and resolved constraints.



- Some of the features mentioned in this document are available only if the relevant software License Key has been purchased from AudioCodes and is installed on the device. For a list of available License Keys that can be purchased, please contact your AudioCodes sales representative.
- Open-source software may have been added and/or amended. For further information, contact your AudioCodes sales representative.
- Updates to this document may be made due to significant information discovered after the release or too late in the release cycle to be otherwise included in this release documentation. You can check for an updated version on AudioCodes website at <https://www.audiocodes.com/library/technical-documents>.

## 1.1 Software Revision Record

The following table lists the MSBR software versions released in Version 7.2.



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

**Table 1: MSBR Software Revision Record**

Software Version	Date Released
7.28A.356.286 (M16.1)	March 22, 2026
7.28A.356.277 (M16)	February 3, 2026
7.28A.356.189 (M15.1)	November 12, 2025
7.28A.356.187 (M15)	August 19, 2025
7.28A.356.070 (M14.1)	May 20, 2025
7.28A.356.043 (M14)	February 23, 2025
7.26A.356.899 (M13.1)	December 23, 2024
7.26A.356.888 (M13)	August 22, 2024
7.26A.356.773 (M12)	April 3, 2024
7.26A.356.630 (M11)	January 15, 2024
7.26A.356.459 (M10)	August 15, 2023
7.26A.356.180 (M9.1)	July 24, 2023
7.26A.356.174 (M9.1)	June 12, 2023
7.26A.356.070 / 7.26A.356.074 / 7.26A.356.075 (M9)	February 16, 2023
7.24A.356.914 (M8.1)	December 11, 2022
7.24A.356.867 (M8)	September 25, 2022
7.24A.356.854 (M8)	September 4, 2022

Software Version	Date Released
7.24A.356.747 (M7)	August 8, 2022
7.24A.356.706 (M7)	August 8, 2022
7.24A.356.508 (M6.2)	March 23, 2022
7.24A.356.481 (M6.1)	February 7, 2022
7.24A.356.468 (M6)	January 5, 2022
7.24A.356.263 (M5-2)	September 5, 2021
7.24A.356.248 (M5)	August 1, 2021
7.24A.356.069 (M4)	April 19, 2021
7.24A.256.329 (M3)	January 4, 2021
7.24A.256.219 (M2)	October 29, 2020
7.24A.256.105	June 21, 2020
7.20A.256.125	April 19, 2020
7.20A.252.192	April 2, 2020
7.20A.256.107	March 15, 2020
7.20A.252.183	December 25, 2019
7.20A.254.733	November 5, 2019
7.20A.252.144	October 7, 2019
7.20A.254.026	September 9, 2019
7.20A.252.078	July 1, 2019
7.20A.252.062	April 30, 2019
7.20A.250.028	January 24, 2019
7.20A.202.307	October 2018
7.20A.202.112	June 2018
7.20A.200.038	March 2018
7.20A.154.078	February 2018
7.20A.154.061	November 2017
7.20A.154.025	August 2017
7.20A.150.004	May 2017

## 1.2 Supported Products

The following table lists the MSBR products supported in this release.



- 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.
- Figures shown in the table below are maximum values per interface. For available hardware configurations including combinations of supported interfaces, contact your AudioCodes sales representative.
- For Mediant 500L MSBR, the USB port is not provided when the device is ordered with LTE cellular support.

### 1.2.1 MSBR Series

The following table lists the MSBR products, and their interfaces supported in Version 7.2.

**Table 2: MSBR Products Supported in Release 7.2**

Product	Telephony Interfaces				Ethernet Interfaces	Wi-Fi	USB	OSN	WAN				
	FXS	FXO	BRI	E1/T1					Copper GbE	Fiber	ADSL2+ / VDSL2	SHDSL	4G LTE / LTE Advanced
Mediant 500Li	8	-	4	-	4 GE	√	1	-	√	√	√	-	√
Mediant 800Ci	4	-	4	-	4 GE	√	1	√	√	√	√	-	√
Mediant 500L MSBR	8	4	4	-	4 GE	-	1	-	√	√	√	-	√
Mediant 500 MSBR	3	1	2	1	4 GE	-	1	-	√	√	√	√	-
Mediant 500C MSBR	2	-	2	1	4 GE	-	1	-	√	√	√	-	-
Mediant 800B MSBR	12	12	8	2	4 GE / 8 FE	-	2	√	√	√	√	√	-
Mediant 800C MSBR	12	12	8	4	4 GE / 8 FE	-	2	√	√	√	√	-	√

### 1.2.2 MediaPack 5xx Series

The following table lists the MediaPack 5xx products, and their interfaces supported in Version 7.2.

**Table 3: MediaPack 5xx Products Supported in Release 7.2**

Model	Telephony Interfaces FXS / FXO	LAN Ethernet (GE)	WAN (Copper GbE)	USB
MP-502	2 / 0	1	1	-
MP-504	4 / 0	1	1	1
MP-508	8 / 0 or 4 / 4	1	1	1
MP-516	16 / 0	1	2	1
MP-524	24 / 0	1	2	1

Model	Telephony Interfaces FXS / FXO	LAN Ethernet (GE)	WAN (Copper GbE)	USB
MP-532	32 / 0	1	2	1

### 1.3 Product Naming Convention

For simplicity, this document uses the following terms to represent groups of products. Where content in this document is applicable to only a specific product(s), the full name of the product(s) is stated.

**Table 4: Product Naming Convention**

Term	Products
<i>Mediant 500</i>	<ul style="list-style-type: none"> <li>■ Mediant 500 MSBR</li> <li>■ Mediant 500C MSBR</li> <li>■ Mediant 500L MSBR</li> </ul>
<i>Mediant 800</i>	<ul style="list-style-type: none"> <li>■ Mediant 800B MSBR</li> <li>■ Mediant 800C MSBR</li> </ul>
<i>Mediant 500Li</i>	Mediant 500Li MSBR
<i>Mediant 800Ci</i>	Mediant 800Ci MSBR
<i>MP-5xx</i>	<ul style="list-style-type: none"> <li>■ MediaPack 502 (MP-502)</li> <li>■ MediaPack 504 (MP-504)</li> <li>■ MediaPack 508 (MP-508)</li> <li>■ MediaPack 516 (MP-516)</li> <li>■ MediaPack 524 (MP-524)</li> <li>■ MediaPack 532 (MP-532)</li> </ul>

## 2 Released Versions

This chapter describes new features, known constraints and resolved constraints.

### 2.1 Version 7.28A.356.286

This version includes resolved constraints only.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS



For Mediant 500L, Mediant 500/C, and Mediant 800B/C MSBRs, the Web interface's Access List (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Access List**) is no longer supported. Instead, use the management access list in the CLI (`configure data > access-list`). For more information on configuration, see [Mediant MSBR Security Setup CLI Configuration Guide](#).

#### 2.1.1 Resolved Constraints

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

**Table 5: Resolved Constraints for Version 7.28A.356.286**

Incident	Description
MSBR-20457	Configured VPN user isn't saved. <b>Applicable Products:</b> Mediant 500Li
MSBR-20606	Auto-Update mechanism fails to download Configuration and Firewall files. <b>Applicable Products:</b> Mediant 500Li
MSBR-20633	Factory reset triggered by a SIP NOTIFY message fails. <b>Applicable Products:</b> Mediant 500Li
MSBR-20709	The device doesn't respond (as a DHCP server) to DHCP requests received from the C470HD IP Phone. <b>Applicable Products:</b> Mediant 500Li
MSBR-20755	Debug Capture doesn't function. <b>Applicable Products:</b> Mediant 500Li

## 2.2 Version 7.28A.356.277

This version includes new features and resolved constraint.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS



For Mediant 500L, Mediant 500/C, and Mediant 800B/C MSBRs, the Web interface's Access List (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Access List**) is no longer supported. Instead, use the management access list in the CLI (`configure data > access-list`). For more information on configuration, see [Mediant MSBR Security Setup CLI Configuration Guide](#).

### 2.2.1 New Features

This section describes the new features introduced in this version.

#### 2.2.1.1 New Product Launch – MediaPack 502 Analog Gateway

AudioCodes is pleased to announce the release of the MediaPack 502 (MP-502) Analog VoIP Gateway, a new addition to our MediaPack 5xx Series of Analog VoIP Gateways, offering flexible configurations from 2 to 32 analog ports to meet a wide range of customer deployment needs.

The MP-502 features two FXS (Foreign Exchange Subscriber) ports, allowing seamless connection to analog equipment such as fax machines and standard analog telephones.

**Applicable Products:** MP-502

#### 2.2.1.2 Restricting Cellular Technology for External Cellular Module

The cellular technology used by AudioCodes external cellular modules Mediant 5G-EA or Mediant 5G-EA-G can now be specified. When configured, the module operates only on the specified cellular technology. Previously, the module automatically selected any available cellular technology (this behavior remains the default if no restriction is configured).

The feature is supported by the new CLI command `cellular-network tech`:

```
# configure data
(config-data)# interface cellular 0/0
M500Li(conf-cellular-0/0)# cellular-network tech {e-utran|ng-
ran|ng-ran_e-utran|ng-ran_e-utran_utran|ng-
ran_utran|utran|utran_e-utran}
```

Where, *E-UTRAN* is LTE (4G), *UTRAN* is 3G, and *NG-RAN* is 5G.

**Applicable Products:** Mediant 5G-EA; Mediant 5G-EA-G

#### 2.2.1.3 L2TP over IPv6 Support with PPP

The device now supports IPv6 address configuration through PPP IPv6 Control Protocol (IPv6CP), enabling IPv6 connectivity for L2TP sessions.

The feature is supported by the new CLI command `ipv6 enable` within the L2TP interface, for example:

```
(config-data)# interface l2tp 8
(conf-if-L2TP 8)# ipv6 enable
```

**Applicable Products:** All

### 2.2.1.4 L2TP Unnumbered IP Configuration

The device now supports Unnumbered IP configuration for Layer 2 Tunneling Protocol (L2TP), allowing an L2TP interface to borrow an IP address from another interface (usually a Loopback) to save IP address space on point-to-point connections.

The feature is supported by the new CLI command `ip unnumbered` within the L2TP interface:

```
(config-data)# interface l2tp 0
(conf-if-L2TP 0)# ip unnumbered <interface type> <interface ID>
```

For example:

```
(conf-if-L2TP 0)# ip unnumbered Loopback 1
```

Below shows the L2TP sharing the same address as the Loopback interface:

```
(conf-if-L2TP 0)# do sh d ip in b
```

Interface	IP Address	Status	Protocol
Loopback	1.1.1.1	Connected	Up
L2TP	1.1.1.1	Disconnected	Up

**Applicable Products:** Mediant 500Li; Mediant 800Ci

### 2.2.1.5 Increased Maximum SIP SUBSCRIBE Sessions

The device now supports up to 460 concurrent SIP SUBSCRIBE sessions. Previously, the maximum was 200.

**Applicable Products:** MSBR

### 2.2.1.6 Classification by Users Registration Database per SIP Interface

Classification to IP Groups of incoming SIP dialog-initiating requests (e.g., INVITE) by the device's users registration database can now be enabled or disabled per SIP Interface for SBC calls. Previously, classification by the users registration database was enabled for all SIP Interfaces (and couldn't be disabled).

This feature is configured by the new SIP Interfaces table parameter, 'Classify by Registration DB' parameter. By default, classification by users registration database is enabled.

**Applicable Products:** All

### 2.2.1.7 Parameters Changed to Online

The following parameters no longer require a device reset for their settings to take effect:

- [HTTPport]
- [HTTPSPort]
- [HTTPSOnly]

**Note:** This functionality is already supported by the MP-5xx, Mediant 500Li, and Mediant 800Ci devices.

**Applicable Products:** MSBR

### 2.2.1.8 Enhanced Control of Debug Recording

The device's debug recording feature has been enhanced to provide the user with more control of the process:

- Starting and stopping debug recording is now done explicitly by the user. Previously, as soon as a rule was added to the Logging Filters table, the device automatically started debug recording (if the 'Mode' parameter was set to **Enable**). Debug recording continued until the user deleted the rule or changed the rule's 'Mode' to **Disable**.
- The debug recording process now has a maximum duration (configurable), after which it automatically stops.

This feature is supported by the following new parameters on the Debug Recording page (Troubleshoot menu > Troubleshoot tab > Logging folder > Debug Recording):

- 'Status' field: Displays if debug recording is currently running (started) or not (stopped).
- Start and Stop buttons: Starts and stops debug recording.
- 'Maximum Duration': Configures the maximum duration (in minutes) of the debug recording process (by default, 60 minutes).
- 'End Time': Displays the date and time when debug recording will stop.

This is also supported in the CLI by the following new commands under `configure troubleshoot > logging settings`:

- `dbg-rec-timeout`: Configures the maximum debug recording duration.
- `dbg-rec-status {start|stop|timer-restart}`: Displays the current debug recording status, starts or stops debug recording, and resets the maximum duration.

**Note:**

- This feature affects only rules in the Logging Filters table whose 'Mode' is **Enable**.
- The maximum debug recording timer is reset to the configured duration upon the following:
  - Configuration (new or modified rule) of Logging Filters table
  - Device restart

**Applicable Products:** All

### 2.2.1.9 Enhanced Password Obfuscation in INI and CLI Script Files

Passwords in the device's downloaded INI and CLI Script files can now be securely obfuscated using a strong encryption algorithm. The encryption is performed using the AES-256 algorithm with a 16-bit random CFB initialization vector (IV) cipher, ensuring robust protection of sensitive data.

The obfuscated passwords appear as follows:

- **INI File:** Prefixed with "\$2\$", for example:  

```
WSTunPassword = $2$8EGYm+FG+JJT/p8ZOytU64uplPMKcw==
```
- **CLI Script file:** Suffixed with "encrypted", for example:  

```
password B55osyLT1t7+oorwkaNB3bxEX4B18g== encrypted
```

The encryption key can be configured in one of the following ways:

- **Manually through CLI:**  

```
configure network > security-settings > encryption-key assign  
<string>
```
- **Device-Generated through CLI:**

```
configure network > security-settings > encryption-key
generate
```

- **Manually using Configuration Package File:** This is done by uploading a Configuration Package file with a newly created *encryption.key* file that contains the key. (For detailed instructions, refer to the User's Manual.)

The encryption key must be at least 32 characters long and can contain a combination of the following characters: A-Z, a-z, 0-9, !, #, \$, %, &, (, ), \*, +, ,, -, ., /, <, =, >, ?, @, [, ], ^, \_ ` , { }, ~. A-Z, a-z, 0-9, !, #, \$, %, &, (, ), \*, +, ,, -, ., /, <, =, >, ?, @, [, ], ^, \_ ` , { }, and ~.

The CLI displays only part of the encryption key for security (first four characters followed by three asterisks, for example, %3[-\*\*\*]). This is displayed using the following new CLI command:

```
configure network > security-settings > encryption-key display
```

This command can be used to check if an encryption key has been configured.

The full encryption key is included in a downloaded, encrypted Configuration Package file. The key is shown in a separate file called *encryption.key* inside the archive. This allows complete backup-and-restore, if needed.

The encryption key can be deleted, using the following new CLI command:

```
configure network > security-settings > encryption-key clear
```

**Note:**

- If you plan to downgrade the device to an earlier version that doesn't support this feature, you must first clear the encryption key; otherwise, the downgrade will fail.
- The encryption key remains unaffected during a restore to factory defaults (*write factory*).

**Applicable Products:** All

### 2.2.1.10 Azure Blob Storage for Debug Recording Files

The device now supports automatic upload of debug recording files to a customer's Microsoft Azure Blob Storage container. When a debug recording file is generated, it is immediately transferred to the configured Azure Blob container for centralized storage and retrieval.

To configure this functionality, the following new parameters have been added to the Debug Recording page:

- 'File Storage' – Enables the storage of debug recording files.
- 'Recording' – Starts the creation of debug recording files.
- 'File Size' – Defines the maximum size of each debug recording file.
- 'Rotation Period' – Defines how frequently (in minutes) new debug files are created, or earlier if the maximum file size is reached.
- 'Filename Prefix' – Defines a custom prefix for generated debug recording filenames.
- 'Storage Location' – Selects the storage destination; in this case, the Azure Blob Storage container.
- 'Storage URL' – Defines the URL of the Azure Blob container.

- 'Container' – Defines the name of the Azure Blob container used for storing the files.
- 'Account Key' – Provides the Shared Access Signature (SAS) token required to securely authenticate and access the Blob storage.

**Note:** Previously, this capability was available only for the Mediant 90xx and Mediant Software platforms. It is now supported on additional models as listed in Applicable Products below.

**Applicable Products:** All

## 2.2.2 Resolved Constraints

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

**Table 6: Resolved Constraints for Version 7.28A.356.277**

Incident	Description
MSBR-19974	Noise experienced during call. <b>Applicable Products:</b> Mediant 500Li
MSBR-20009	Remote disconnect on CAMA 911 line locks port. <b>Applicable Products:</b> Mediant 500Li
MSBR-20165	SNMP alarm-customized-severity is not aligned with the Web interface. <b>Applicable Products:</b> MP-504
MSBR-20185	Parameters are not set correctly when uploading a CLI-Script file. <b>Applicable Products:</b> MP-5xx
MSBR-20210	Do Not Disturb (KeyCFDoNotDisturb) parameter can't be configured. <b>Applicable Products:</b> MP-5xx
MSBR-20254	Configuration is lost after device downgrade. <b>Applicable Products:</b> Mediant 500
MSBR-20255	RTP fails after DTMF detected by device. <b>Applicable Products:</b> MP-5xx
MSBR-20272	Device doesn't respond to SNMP requests. <b>Applicable Products:</b> MP-504
MSBR-20274	Timeout SNMP monitoring delay experienced on device. <b>Applicable Products:</b> MP-5xx
MSBR-20286	Uploading configuration file (copy startup-script from) to device fails because of space in network source name. <b>Applicable Products:</b> Mediant 500Li
MSBR-20288	The device is sending acBoardOverloadAlarm alarms. <b>Applicable Products:</b> MP-5xx
MSBR-20289	The device fails to authenticate the peer certificate when the AUPDVerifyCertificates parameter is enabled. <b>Applicable Products:</b> MP-508
MSBR-20290	IP address isn't populated in the SIP X-Channel header (XChannelHeader parameter). <b>Applicable Products:</b> MP-5xx
MSBR-20293	Access through WebSocket tunnel to device's Web interface fails. <b>Applicable Products:</b> MSBR

Incident	Description
MSBR-20354	FXS port doesn't play a ringback dial tone when phone is off hooked and user can't dial a phone number. <b>Applicable Products:</b> Mediant 800
MSBR-20360	IPv6 received from DHCP server is removed after a few hours. <b>Applicable Products:</b> Mediant 500Li
MSBR-20363	The device doesn't show traces of the automatic update. <b>Applicable Products:</b> MP-5xx
MSBR-20368	The device doesn't perform DNS resolution. <b>Applicable Products:</b> Mediant 500Li
MSBR-20371	The device resets when configuring a Trunk Group. <b>Applicable Products:</b> MP-5xx
MSBR-20379	Issues experienced on the first PRI port after a software upgrade to 7.28A.356.187. <b>Applicable Products:</b> Mediant 800 MSBR
MSBR-20380	One-way voice on FXS port. <b>Applicable Products:</b> MP-5xx
MSBR-20432	DHCP via IPSec tunnel fails when connected via DSL. <b>Applicable Products:</b> Mediant 500Li
MSBR-20434	Hotline Autodial feature doesn't function. <b>Applicable Products:</b> Mediant 500Li; MP-5xx
MSBR-20435	Downgrade deletes IP Group and Trunk Group configuration. <b>Applicable Products:</b> MSBR
MSBR-20440	Unable to activate DND without a configured destination. <b>Applicable Products:</b> MP-524
MSBR-20441	Unable to connect to device through HTTPS. <b>Applicable Products:</b> Mediant 500L
MSBR-20442	SNMP community strings return to default password. <b>Applicable Products:</b> Mediant 500L
MSBR-20443	Digits missing from Caller ID. <b>Applicable Products:</b> MP-5xx
MSBR-20446	The device loses connection with OVOC after a network interruption. <b>Applicable Products:</b> Mediant 500; Mediant 500L
MSBR-20453	IPSec over the internal LTE doesn't function. <b>Applicable Products:</b> Mediant 500Li
MSBR-20456	Device monitoring through SNMP isn't functioning properly because of SNMP OID issues. <b>Applicable Products:</b> MP-5xx
MSBR-20458	The device doesn't connect to Live Platform. <b>Applicable Products:</b> MP-5xx

Incident	Description
MSBR-20462	When uploading a CLI-Script file to the device, SNMP settings don't get applied correctly if the auth-key and priv-key are obscured. <b>Applicable Products:</b> MSBR
MSBR-20466	TLS Context configuration is deleted when upgrading device from 6.8 to 7.28. <b>Applicable Products:</b> MSBR
MSBR-20471	Device fails to establish WebSocket connection with OVOC. <b>Applicable Products:</b> MSBR
MSBR-20494	FXS line testing fails for ports 10 and higher. <b>Applicable Products:</b> MP-5xx
MSBR-20495	Device fails to be managed using SNMPv3. <b>Applicable Products:</b> MP-5xx
MSBR-20505	The device stops responding to SNMP requests after a few hours. <b>Applicable Products:</b> Mediant 800 MSBR
MSBR-20512	FXS CAMA 911 calling issue with Answer Supervision and/or Disconnect Supervision. <b>Applicable Products:</b> MP-516
MSBR-20529	The device randomly resets. <b>Applicable Products:</b> MSBR

## 2.3 Version 7.28A.356.189

This version includes resolved constraints only.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.3.1 Resolved Constraints

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

**Table 7: Resolved Constraints for Version 7.28A.356.189**

Incident	Description
MSBR-20284	MP-524 can't establish connection to OVOC management platform. <b>Applicable Products:</b> MP-524
MSBR-20423	MP-508 fails to be managed through SNMPv3. <b>Applicable Products:</b> MP-508
MSBR-20393	SNMP displays product type for MP-504 as "acMediaPack500". <b>Applicable Products:</b> MP-504

## 2.4 Version 7.28A.356.187

This version includes new features and resolved constraints.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.4.1 New Features

This section describes the new features introduced in this version.

#### 2.4.1.1 New SNMP MIBs for Cellular Interface of 5G Cellular Module

The following cellular-related SNMP MIB objects have been added for monitoring the Mediant 5G-EA and Mediant 5G-EA-G cellular modules:

- **acSysNetworkCellOperatorName** – Name of the connected cellular operator.
- **acSysNetworkCellSignalLevel** – Cellular signal level strength (“none”, “poor”, “moderate”, “good”, “great”).
- **acSysNetworkCellIMEI** - International Mobile Equipment Identity (IMEI) of the cellular module.
- **acSysNetworkCellICCIDofFirstSim** –Integrated Circuit Card Identifier (ICCID) of the first SIM card.
- **acSysNetworkCellICCIDofSecondSim** - ICCID of the second SIM card.

**Applicable Products:** All

#### 2.4.1.2 Remote Restore to Factory Defaults using SIP NOTIFY Message

The device supports remote restore to factory default settings—including all configuration and network parameters—through a SIP NOTIFY message. To trigger this, the NOTIFY message must contain an Event header with the value ‘factory-restore-sync’, as 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: factory-restore-sync
```

Upon receipt of such a message, the device restores its factory defaults and then automatically reboots to complete the process. This feature is enabled by configuring the existing parameter 'Remote Management by SIP Notify' (EnableSIPRemoteReset) to the new optional value **Enable Including Factory Restore**.

**Applicable Products:** All

### 2.4.1.3 Interworking ISDN CUG Supplementary Service and SIP

The device now supports interworking between the ISDN Closed User Group (CUG) supplementary service and SIP, for Tel-to-IP calls. CUG supplementary service enables users to form groups, where members of a specific closed user group can communicate among themselves but not, in general, with users outside the group.

The feature is enabled by the new parameter, 'Cug Data Mode' (CugDataMode / cug-data-mode). By default (disabled), the device doesn't add the CUG body. If this feature is enabled and the device receives an ISDN Setup message whose Facility IE indicates CUG (cUGCall invoke), it adds an XML body containing CUG information (CUG index and outgoing access) to the outgoing SIP INVITE message, as shown in the following example:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/xcap"
elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:annotation>
<xs:documentation>XML Schema Definition for the closed user group
parameter</xs:documentation>
</xs:annotation>
<xs:include schemaLocation="xcap.xsd"/>
<!--Definition of simple types-->
<xs:simpleType name="twobitType">
<xs:restriction base="xs:string">
<xs:pattern value="[0-1][0-1]"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="networkIdentityType">
<xs:restriction base="xs:hexBinary">
<xs:length value="2"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="sixteenbitType">
<xs:restriction base="xs:hexBinary">
<xs:length value="2"/>
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="cugIndexType">
<xs:restriction base="xs:integer">
<xs:minInclusive value="0"/>
<xs:maxInclusive value="32767"/>
</xs:restriction>
</xs:simpleType>
<!--Definition of complex types-->
<xs:complexType name="cugRequestType">
<xs:sequence>
<xs:element name="outgoingAccessRequest" type="xs:boolean"/>
<xs:element name="cugIndex" type="cugIndexType" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
<!--Definition of document structure-->
```

```

<xs:element name="cug" substitutionGroup="ss:absService">
  <xs:complexType>
    <xs:complexContent>
      <xs:extension base="ss:simservType">
        <xs:sequence>
          <xs:element name="cugCallOperation" type="cugRequestType"
            minOccurs="0">
            <xs:complexType>
              <xs:sequence>
                <xs:element name="outgoingAccessRequest" type="xs:boolean"
                  value="True"/>
                <xs:element name="cugIndex" type="xs:integer" value="32767"/>
              </xs:sequence>
            </xs:complexType>
          </xs:element>
          <xs:element name="networkIndicator" type="networkIdentityType"
            minOccurs="0"/>
          <xs:element name="cugInterlockBinaryCode" type="sixteenbitType"
            minOccurs="0"/>
          <xs:element name="cugCommunicationIndicator" type="twobitType"
            minOccurs="0"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
</xs:element>
</xs:schema>

```

**Applicable Products:** All

#### 2.4.1.4 Sending Syslog to Apache Kafka

The device's embedded syslog (Rsyslog) client can now send event logs (syslog messages) to Apache Kafka, an open-source platform for event streaming.

The device, as a Kafka producer, transmits syslog messages to the remote Kafka broker. The broker can be on a local server or hosted on the cloud.

The broker manages one or more topics, which act like categories for classifying syslog messages. For example, the device can be configured to send syslog messages to specific topics based on severity level. Multiple applications or services (Kafka consumers) can subscribe to these topics and receive syslog messages.

The existing Syslog Servers table is used to configure this functionality. Kafka-specific configuration includes the following:

- 'Address' (existing) - defines the address (FQDN) of the Kafka broker.
- 'Kafka Topic' (new) - defines the Kafka topic (Event Hub name in Azure).
- 'Kafka Connection String' (new) - defines the authentication/encryption string (password) for connecting to the Kafka broker (topic).
- 'Transport Protocol' (existing) –set to the new optional value KAFKA.
- 'Port' (existing) – defines the listening port for Kafka (9093 for Azure Event Hub).

In addition to the above configuration, a TLS Context must be selected (using the global 'Syslog TLS Context' parameter).

**Applicable Products:** All

## 2.4.2 Resolved Constraints

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

**Table 8: Resolved Constraints for Version 7.28A.356.187**

Incident	Description
MSBR-20256	Device sends the incorrect calling name Facility IE in ISDN SETUP messages during call initiation. <b>Applicable Products:</b> All
MSBR-19538	Increasing memory utilization and memory leak. <b>Applicable Products:</b> All
MSBR-19687	Security vulnerability CVE-1999-0524 identified. <b>Applicable Products:</b> All
MSBR-19725	The "local" acl doesn't include VRRP floating address and therefore, doesn't block the incoming traffic toward the IP address. <b>Applicable Products:</b> All
MSBR-19833	The Web interface's Network View for interfaces is displayed incorrectly. <b>Applicable Products:</b> Mediant 500Li
MSBR-19900	Restoring factory defaults through the Web interface fails. <b>Applicable Products:</b> Mediant 500Li
MSBR-19954	Device fails to connect to OVOC via tunnel. <b>Applicable Products:</b> All
MSBR-20008	The Web interface access list ( <code>mgmt-access-list</code> ) blocks access to the Web interface after a firmware upgrade. <b>Applicable Products:</b> MSBR
MSBR-20063	Users defined in the Supplementary Services table don't register. <b>Applicable Products:</b> Mediant 500Li
MSBR-20068	Packet length changes for some calls. <b>Applicable Products:</b> MSBR
MSBR-20070	UDP port spacing ( <code>udp-port-spacing</code> ) supports only the value 10 (other values removed - 2, 4, and 5). <b>Applicable Products:</b> MP-504
MSBR-20141	BVI (Bridge Virtual Interface) for RIP (Routing Information Protocol) is not usable. <b>Applicable Products:</b> MSBR
MSBR-20162	The device crashes when using TR-069 with incorrect XML configuration. <b>Applicable Products:</b> MSBR

## 2.5 Version 7.28A.356.070

This version includes new features and resolved constraints.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.5.1 New Features

This section describes the new features introduced in this version.

#### 2.5.1.1 IPv6 BFD for IPv6 Static Routes

The device now supports IPv6 Bidirectional Forwarding Detection (BFD) for IPv6 static routes. Previously, this was supported only for IPv4.

This feature uses the existing CLI commands for BFD. Below shows a configuration example of an IPv6 BFD entry that is associated with an IPv6 static route:

- BFD entry with IPv6 neighbor address:

```
(config-data)# bfd neighbor 1 2027:db9:a::2 GigabitEthernet  
0/0.41 interval 2000 min_rx 2000 multiplier 3 multihop
```

- IPv6 static route associated with the BFD:

```
(config-data)# ipv6 route 3000::/64 2023:a::1 GigabitEthernet  
0/0.41 1 bfd-neighbor 1
```

**Applicable Products:** Mediant 800Ci; Mediant 500Li; MediaPack 5xx

#### 2.5.1.2 SNMP Performance Monitoring for Memory and CPU Utilization

The device provides new SNMP performance monitoring for memory and CPU utilization. Low and high thresholds can be defined for these performance monitoring parameters that if crossed, the existing acPerformanceMonitoringThresholdCrossing trap is sent by the device.

The new performance monitoring parameters (gauge) include the following:

- **CPU utilization** - acPMSysVoipCPUUtilization
- **Memory utilization** - acPMSysVoipMemoryUtilization

**Applicable Products:** Mediant 800Ci; Mediant 500Li; MediaPack 5xx

## 2.5.2 Resolved Constraints

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

**Table 9: Resolved Constraints for Version 7.28A.356.070**

Incident	Description
MSBR-19979	The device isn't provisioned correctly through TR-069. <b>Applicable Products:</b> MP-508
MSBR-19997	No voice is experienced when using the AES-256 encryption algorithm. <b>Applicable Products:</b> MP-532
MSBR-19464	The device changes RTP packet length during a call. <b>Applicable Products:</b> Mediant 800C
MSBR-19773	The device crashes due to a "TPApp Linux Signal". <b>Applicable Products:</b> All
MSBR-19782	When using SNMPv3 and a WebSocket is used with OVOC, OVOC can't communicate with the device. <b>Applicable Products:</b> MP-5xx
MSBR-19790	The device resets when an LDAP service runs. <b>Applicable Products:</b> MP-5xx
MSBR-19837	The device crashes (resets) when using a specific setting. <b>Applicable Products:</b> MSBR
MSBR-19850	The device repeatedly resets after being upgraded to 7.28A.356.043. <b>Applicable Products:</b> MSBR
MSBR-19856	BFD configuration is deleted after a device reset. <b>Applicable Products:</b> Mediant 500Li
MSBR-19864	The device resets daily. <b>Applicable Products:</b> MSBR
MSBR-19942	Version 7.28A.356.043 causes an audio issue (cracking sounds). <b>Applicable Products:</b> MP-5xx
MSBR-19956	When the 5G module is configured as second route, the route is lost for about 1 second, every 30 to 60 seconds. <b>Applicable Products:</b> Mediant 500Li

## 2.6 Version 7.28A.356.043

This version includes new features, known constraints and resolved constraints.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.6.1 New Features

This section describes the new features introduced in this version.

#### 2.6.1.1 Power Management of AudioCodes PoE Injector and Cellular Module via USB

When using AudioCodes PoE injector for AudioCodes external cellular module (e.g., Mediant 5G-EA or Mediant 5G-EA-G), the device can now control power (on or off) to the Power-over-Ethernet (PoE) injector and thus, to the cellular module. Previously, PoE was always on.

This is achieved by connecting the PoE injector's USB port to the device's USB port, using a special USB cable (purchased from AudioCodes), and then running the following new CLI command, which functions together with the status of the cellular interface (`shutdown` or `no shutdown`):

```
(conf-cellular-0/0)# remote usb-controlled-poe
```

The following example powers off the PoE injector (and thus, cellular module):

```
interface Cellular 0/0
  desc "WAN Cellular"
  remote mode m5g-ea-g
  remote underlying GigabitEthernet 0/0
  sim slot 1
  remote usb-controlled-poe
  remote mgmt-vlan 4051 data-vlan 4052 4053
  obscured-pin RXR3dnk=
  shutdown
exit
```

**Applicable Products:** Mediant 5G-EA / 5G-EA-G

### 2.6.1.2 BGP Multipath Routing

The device now supports BGP multipath, which allows multiple BGP routes to be used simultaneously to reach the same destination. The BGP routing protocol learns and adds multiple routing rules for the same destination, from several BGP neighbors. The benefits of BGP multipath include traffic load-balancing between multiple paths and redundancy in case of path failure.

This feature is configured using existing CLI commands, including the `maximum-paths` and `maximum-paths ibgp` commands. The following is an example of BGP multipath configuration for learning two paths to the same destination:

```
configure data
router bgp 1
  maximum-paths 2
  maximum-paths ibgp 2
  neighbor 10.31.4.61 remote-as 1
  neighbor 100.100.100.2 remote-as 1
exit
exit
```

If BGP learns the same route (in this example, with destination 11.11.0.0) from both BGP neighbors, it adds both to the routing table, which is displayed like this:

```
CLI# show data ip route
B 11.11.0.0/16 [20/0] via 10.31.4.61, GigabitEthernet 0/0,
00:00:15
                                     via 100.100.100.2,
GigabitEthernet 0/0.1000, 00:00:15
```

**Applicable Products:** All

### 2.6.1.3 RADIUS Binding to VRF Source Interface

The RADIUS application can now be bound to a source network interface associated with a specific Virtual Routing and Forwarding (VRF) instance.

This feature is configured using the new `vrf` command option:

```
configure system > radius settings > source data vrf <VRF name>
```

If the VRF name is not specified, the device uses the default VRF (*main-vrf*).

**Applicable Products:** All

### 2.6.1.4 LAN Source Address Included in DHCP Relay Packets

The device (DHCP relay agent) can now be configured to include the LAN interface's (DHCP client) address as the source address in DHCP relay unicast packets sent to the DHCP server from the WAN.

To configure this feature, the following new CLI command has been added for the LAN interface where the relay is configured:

```
ip dhcp-source-address interface
```

**Note:** This feature is already supported by the other products (Mediant 500Li, Mediant 800Ci, and MP-5xx).

**Applicable Products:** MSBR

### 2.6.1.5 UA-Profile Events Subscription

The device can now be configured to subscribe to UA-Profile events with a UA-Profile server. The subscription process is initiated by sending a SIP SUBSCRIBE request that includes an Event header, which specifies the desired app or service, for example:

```
Event: ua-profile;profile-type=application;appids="myapp"
```

This feature is configured by the following new parameters:

- 'Subscribe to UA-Profile' / [EnableUaProfileSubscription] / `subscribe-to-ua-profile`: Enables UA-Profile subscription (by default, disabled).
- 'UA-Profile Subscribe Expiration Time' / [UaProfileExpirationTime] / `ua-profile-subscribe-time`: Defines the UA-Profile service subscription expiration time in seconds (10 to 15,500,000; default 7200 or 2 hours).
- 'UA-Profile Server IP Address' / [UaProfileServerIP] / `ua-profile-srvr-ip-addr`: Defines the address (IP or FQDN) of the UA-Profile server.
- 'UA-Profile Subscribe IP Group' / [UaProfileSubscribeIPGroupID] / `ua-profile-subscribe-ipgroupid`: Defines the IP Group to subscribe to the UA-Profile events.
- 'UA-Profile Server Transport Type' / [UaProfileServerTransportType] / `ua-profile-srvr-transport-type`: Defines the transport type used for sending the SIP SUBSCRIBE requests to the UA-Profile server (UDP,TCP, TLS; default is Not Configured).

**Applicable Products:** All

### 2.6.1.6 New SNMP Alarm for Registration Failure

A new SNMP alarm has been introduced in this release that is raised when a registration failure occurs per Account (configured in the Accounts table), per endpoint, or for the whole device (*Gateway*). The registration mode is configured by the 'Registration Mode' parameter in the Trunk Group Settings table.

The new alarm is called `acAccountRegistrationAlarm` (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.164).

**Note:** This feature is applicable only to the Gateway application (not SBC).

**Applicable Products:** All

### 2.6.1.7 New SNMP Alarm for IP Group Connectivity

A new SNMP alarm has been introduced that is raised when the device has no connection (based on keep-alive messages) with an IP Group.

The new alarm is called `acIpGroupKeepAliveAlarm` (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.163).

**Applicable Products:** All

### 2.6.1.8 Enhanced SNMP Features for Mediant 5G-EA Cellular Modules

The following SNMP features are now supported by the Mediant 5G-EA and Mediant 5G-EA-G cellular modules:

- **Active SIM Slot Identification:** You can now identify the active SIM card slot via an SNMP Get request using the new SNMP MIB `acSysNetworkCellCurrentSimSlot`. The active slot is enabled through the CLI command: `configure data > interface cellular 0/0 > sim slot [slot number]`.
- **5G Support in SNMP Trap Event:** The existing SNMP trap event `acWirelessCellularModemStatusChanged` now includes support for 5G. This event notifies you when there is a change in cellular technology (e.g., switching from 4G to 5G).

- **Current Cellular Network Type Description:** The SNMP MIB `acSysNetworkCellCurrentNetworkTypeDescription` has been enhanced to support 5G and provide a description of the current cellular technology in use (e.g., 3G, 4G, or 5G).

**Applicable Products:** Mediant 5G-EA; Mediant 5G-EA-G

### 2.6.1.9 SNMP View-based Access Control Model for SNMP

The device offers an advanced SNMP configuration mode called View-based access control (VACM) that enables fine-grained access control over SNMP MIB objects. Users can define customized read, write, and notification privileges for SNMPv2/v3 users and community strings, specifically targeting MIB objects (subtrees/OIDs). This feature enhances security and flexibility by allowing precise control over which users have access to different parts of the MIB tree.

Additionally, an intuitive and improved user interface has been introduced to streamline the SNMP configuration process, ensuring a more efficient and user-friendly experience when managing SNMP.

The key points and updates of this feature (basic and advanced) are summarized below:

- The SNMP Community Settings page has been renamed **SNMP Settings**, and includes the following changes:
  - The 'Read-Only' and 'Read-Write' community string fields have been removed and are now configured in the new SNMP Community Strings table (see below).
  - The 'Trap Manager Host Name' field (`SNMPTrapManagerHostName`) is now obsolete. Hostname can now be configured in the SNMP Trap Destinations table (see below).
  - The page now includes the 'Allow WAN access to SNMP' parameter, which was only configurable through CLI or Ini file.
- The advanced SNMP mode is enabled by the new command / ini file parameter, `configure system > snmp settings > enable-advanced-mode / [EnableSnpAdvancedMode]`.
- The advanced SNMP mode introduces the following new tables:
  - **SNMP Access Table:** Configures SNMP access groups, controlling write, read and notification privileges for specific SNMP users over MIB object information, as configured in the View Tree Family table (see below).
  - **View Tree Family Table:** Configures SNMP Views, which sets read view and write view privileges for specified MIB subtrees (OIDs).
- A new table called **SNMP Community Strings** now configures the SNMP community strings (passwords). These were previously configured in the 'Read-Only' and 'Read-Write' fields on the SNMP Community Settings page.
  - In basic mode, the 'Group' drop-down list selects either the Read-Only or Read-Write value.
  - In advanced mode, the 'Access Group' drop-down list selects the access group from the new SNMP Access table.
- In the **SNMPv3 Users** table, the name of the existing 'Group' field depends on the SNMP mode:
  - In basic mode, the 'Group' drop-down list selects the Read-Only, Read-Write, or Trap value (same as previous version).
  - In advanced mode, the 'Access Group' drop-down list (row pointer) selects an access group from the new SNMP Access table.

- The **SNMP Trap Destinations** page has been redesigned into the standard table format (i.e., rows added using the New button). This table also includes the following new fields:
  - 'SNMP Version' - selects the SNMP user type (SNMPv2 or SNMPv3).
  - 'SNMPv3 User' - row pointer to the SNMPv3 Users table.
- The **SNMP Trusted Managers** page has been redesigned into the standard table format (i.e., rows added using the New button).

**Note:** Once in advanced SNMP mode, it's not recommended to return to basic mode. If returned, all advanced settings are deleted. However, if you want to return to basic mode, you must do a device reset.

**Applicable Products:** All

### 2.6.1.10 Enhanced SSH Cipher String Configuration

Secure access to the device's CLI through SSH has been enhanced with the addition of the following new configuration parameters:

- 'Kex Algorithms String' / `configure system > cli-settings > sshkex-algorithms-string / [SSHKexAlgorithmsString]`: Defines the SSH Key Exchange Algorithms. (diffie-hellman-group-exchange-sha256, diffie-hellman-group14-sha1, or diffie-hellman-group1-sha1).
- 'Ciphers String' / `configure system > cli-settings > sshciphers-string / [SSHCiphersString]`: Defines the SSH cipher string (aes128-ctr, aes128-cbc, aes256-ctr, or aes256-cbc).
- 'MACs String' / `configure system > cli-settings > sshmacs-string / [SSHMACsString]`: Defines the SSH MAC algorithms (hmac-sha1 or hmac-sha2-256).

**Applicable Products:** All

## 2.6.2 Known Constraints

This section lists known constraints.

**Table 10: Known Constraints in Version 7.28A.356.043**

Incident	Description
MSBR-19725	<p>"local" in the ACL doesn't include VRRP floating addresses and therefore, it doesn't block incoming traffic toward this IP address.</p> <p>As a work around, explicitly add an ACL rule for this IP address.</p> <pre>access-list [Number or Word] deny ip [Network IP Address] [Network Wildcard] [VRRP Floating Address] [Network Wildcard]</pre> <p><b>Applicable Products:</b> All</p>

## 2.6.3 Resolved Constraints

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

**Table 11: Resolved Constraints for Version 7.28A.356.043**

Incident	Description
MSBR-19763	<p>Device restarts when configuring the external 5G cellular module (Mediant 5G-EA).</p> <p><b>Applicable Products:</b> All</p>
MSBR-18028	<p>No response via ping, SSH, and Web interface.</p> <p><b>Applicable Products:</b> MSBR</p>
MSBR-18639	<p>Device restarts after software upgrade, caused by a bug in custom DDNS without a name (dynamic-dns &gt; service custom).</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-19032	<p>The device sends SIP OPTIONS messages from port 1024.</p> <p><b>Applicable Products:</b> MSBR</p>
MSBR-19057	<p>The SIP From header for an SBC test call shows "Anonymous" even though the Endpoint URI parameter is configured.</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-19153	<p>DTMF transcoding fails because of no DSP resources even though the device has an SBC session license.</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-19173	<p>After a certain duration, connectivity is lost to the HTTPS Web interface.</p> <p><b>Applicable Products:</b> MSBR</p>
MSBR-19265	<p>Device is unable to detect all DTMF digits when loud alarm.</p> <p><b>Applicable Products:</b> MP-5XX</p>
MSBR-19269	<p>Device crashes and freezes.</p> <p><b>Applicable Products:</b> MSBR</p>
MSBR-19320	<p>Irrelevant error message generated for dev name wlan0.</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-19351	<p>Only up to two LDAP Server Groups can be configured.</p>

Incident	Description
	<b>Applicable Products:</b> MP-524
MSBR-19357	The device fails to download the CLI configuration file from the remote provisioning server using the Auto Update feature. <b>Applicable Products:</b> Mediant 500Li
MSBR-19360	The device restarts when all available SDP bodies are allocated. <b>Applicable Products:</b> Mediant 500L
MSBR-19361	LDAP-based login intermittently triggers a device reset. <b>Applicable Products:</b> MSBR
MSBR-19385	Alias for PPOE is lost after a device upgrade. <b>Applicable Products:</b> Mediant 500Li
MSBR-19400	The device fails to download the firmware file from the provisioning server when using the Redirect Service (Zero Conf). <b>Applicable Products:</b> MSBR
MSBR-19441	Copying client default configuration file to the device from USB fails. <b>Applicable Products:</b> Mediant 800Li
MSBR-19481	REST API PUT request for incremental ini file fails. <b>Applicable Products:</b> MSBR
MSBR-19505	The setting of the 'Secured Web Connection (HTTPS)' parameter to <b>HTTPS only</b> is not preserved after a device reset. <b>Applicable Products:</b> Mediant 500Li
MSBR-19625	The device sends a SIP 500 response when attempting call transfer from FXS port 1 to FXS port 2. <b>Applicable Products:</b> MP-504
MSBR-19641	No CLI command for EnableEarlyMedia. <b>Applicable Products:</b> MSBR

## 2.7 Version 7.26A.356.899

This version includes only resolved constraints.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS



From this version, the device no longer undergoes a reset after loading a CLI Script file through the Web interface (unless the script contains the `reload now` command).

### 2.7.1 Resolved Constraints

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

**Table 12: Resolved Constraints for Version 7.26A.356.899**

Incident	Description
MSBR-19193	The device is longer manageable by OVOC after a device reset. <b>Applicable Products:</b> MSBR
MSBR-19201	The device is no longer manageable by OVOC after a software update. <b>Applicable Products:</b> MSBR
MSBR-19266	Floating License failure. <b>Applicable Products:</b> Mediant 500Li
MSBR-19273	Failure accessing the device from OVOC using SSO. <b>Applicable Products:</b> Mediant 500Li
MSBR-19284	The device is not getting updated in OVOC. <b>Applicable Products:</b> Mediant 500Li
MSBR-19316	The Floating license no longer functions after a device upgrade. <b>Applicable Products:</b> Mediant 500Li
MSBR-19440	Kernel panic experienced. <b>Applicable Products:</b> Mediant 500C; Mediant 800C
MSBR-19517	Device resets when trying to upgrade from version 7.24A.256.331 to 7.26A.356.896. <b>Applicable Products:</b> MSBR
MSBR-19562	BGP routing is not learned after device reset. <b>Applicable Products:</b> MSBR

## 2.8 Version 7.26A.356.888

This version includes new features and resolved constraints.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
  - This version is applicable only to the following physical WAN interfaces:
    - Copper
    - Cellular
    - Fiber
    - A/VDSL ISDN
- A/VDSL POTS



From this version, the device no longer undergoes a reset after loading a CLI Script file through the Web interface (unless the script contains the `reload now` command).

### 2.8.1 New Features

This section describes the new features introduced in this version.

#### 2.8.1.1 Additional Flavor of External Cellular Module - Mediant 5G-EA-G

AudioCodes now offers an additional flavor of the external Mediant 5G-EA cellular module, called **Mediant 5G-EA-G**, which is based on a new generation chip. Unlike Mediant 5G-EA, this flavor also supports eSIM (SIM slot 2; regular SIM card in slot 1).

Access to Mediant 5G-EA-G configuration is through the new command option **m5g-ea-g**:

```
M500Li# configure data
M500Li(config-data)# interface cellular 0/0
M500Li(conf-cellular-0/0)# remote mode {m5g-ea-g|m5g-ea}
```

For enabling the eSIM:

```
M500Li# configure data
M500Li(config-data)# interface cellular 0/0
M500Li(conf-cellular-0/0)# sim slot 2
```

Except for the above, the Mediant 5G-EA-G shares the same command set as the Mediant 5G-EA.

**Note:** Only one SIM can be configured (either eSIM or physical SIM).

**Applicable Products:** Mediant 5G-EA-G

#### 2.8.1.2 Disabling Integrated LTE

The device's integrated (internal) LTE modem can now be disabled. This is required when using the Mediant 5G-EA cellular module.

Disabling the modem is done using the following new configuration parameter:

- INI File: DisableInternalLTEmodem
- CLI: `configure system > hw > disable-internal-lte-modem on`

**Applicable Products:** Mediant 500Li; Mediant 800Ci

### 2.8.1.3 Display of Mediant 5G-EA Cellular Firmware Version through CLI

The device now displays M5G-EA firmware version information in the output of the CLI command `show data cellular status`.

For example (shown in **bold**):

```
# show data cellular status
Cellular 0/0/1 interface status:
      Administrative:      UP
Remote M5G:
~~~~~
Status: Connected.
M5G firmware version: 7.26A.356.479
SIM card slot #1: Detected ICCID: 8997250400037912035F
SIM card slot #2: Absent.
SIM card active slot: 1 (SIM PIN code required)
```

**Note:** The *firmware version* is the software version of the device (MSBR) with which the Mediant 5G-EA is compatible (and later versions).

**Applicable Products:** All

### 2.8.1.4 Cellular Network Scanning

The device can now scan for 4G cellular networks in the surrounding area when the device operates with the Mediant 5G-EA module. Up until now, this functionality was supported only by the device's internal LTE modem.

The scan is done using the following existing CLI command:

```
show data cellular network-scan 4g
```

This feature is useful, for example, for searching the best provider (i.e., strongest signal) to connect the device's SIM.

**Applicable Products:** Mediant 5G-EA

### 2.8.1.5 RSA Signature Algorithm using SHA2

When using RSA keys, the device's embedded SSH server now supports signatures using the SHA2 hash function (`rsa-sha2-256` and `rsa-sha2-512`), per RFCs 8308 and 8332.

**Applicable Products:** All

### 2.8.1.6 WAN Backup Group in Web Interface

The Web interface now displays the WAN backup group on the new Backup Group Status page (**Monitor** menu > **Monitor** tab > **Network Status** folder > **Backup Group Status**). This page displays the WAN interfaces comprising the backup group, the priority of each interface, and the interface that is currently active.

**Applicable Products:** MP-532

### 2.8.1.7 FQDN for GRE Interface Tunnel Destination

The destination of the Generic Routing Encapsulation (GRE) interface tunnel can now be configured as an FQDN (instead of an IP address). This is useful when the tunnel peer IP address can dynamically change and therefore, by using DNS the device can be updated with the peer's current IP address.

In addition, a new DNS feature has been introduced that uses the DNS record's TTL to update the DNS client (GRE interface) with the new IP address resolution. Periodic DNS requests are sent to the DNS server per TTL time. If a new IP address is detected, the device reconnects to the peer using the new address through the GRE interface.

This feature is configured using the following CLI commands:

- Configuring the tunnel peer with an FQDN in the GRE interface:

```
interface gre 1
  tunnel destination <A.B.C.D | FQDN>
```

- Information of the GRE tunnel peer is displayed in the show data ip/interface commands:

```
Tunnel destination fqdn is <FQDN>
```

If FQDN is not resolved:

```
Tunnel destination IP address not resolved
```

If FQDN is resolved:

```
Tunnel destination resolved IP address is <IP address>
```

**Applicable Products:** All

### 2.8.1.8 IPv6 Neighbor Discovery (ND) Proxy

The IPv6 Neighbor Discovery (ND) Proxy feature enhances network communication efficiency by allowing a firewall to respond to Neighbor Solicit messages on behalf of devices within a local area network (LAN). When this feature is configured on a network interface and a prefix is delegated to one of the LAN interfaces, the firewall intercepts Neighbor Solicit messages and promptly replies with Neighbor Advertisement messages for any addresses within the received prefix from Router Advertisement (RA) messages. This capability optimizes network routing and ensures seamless connectivity for devices within the LAN.

To enable the IPv6 ND Proxy feature, the following CLI command is set on the WAN interface:

```
ipv6 nd proxy
```

**Note:** The firewall hook must be enabled on the respective network interface. This ensures that the firewall can intercept and respond to Neighbor Solicit messages effectively, facilitating smooth communication within the network.

**Applicable Products:** All

### 2.8.1.9 Prefix for External Line per FXS Port

Previously, a prefix for an external line (Tel-to-IP calls) could only be configured globally (i.e., for all FXS ports), using the existing Prefix2ExtLine parameter (`prefix-2-ext-line` CLI command).

Now, the external line can be applied to specific FXS ports using Tel Profiles. This is done by configuring the following new Tel Profile parameter 'Line Type' to one of the following values:

- **External** (default) – applies the setting of the Prefix2ExtLine parameter
- **Internal** – ignores the Prefix2ExtLine parameter (i.e., no external line prefix)

For FXS ports that use the external line, the assigned Tel Profile would have the 'Line Type' parameter set to **External**. For FXS ports not using the external line, the assigned Tel Profile would have the 'Line Type' parameter set to **Internal**.

**Applicable Products:** All

### 2.8.1.10 Configurable Hook-Flash with Digit Key Sequences for FXS Calls

Previously, hook-flash key sequences by pressing the flash button and a digit on the phone's keypad was hardcoded. The type of key sequence was specified by the 'Flash Keys Sequence Style' (FlashKeysSequenceStyle) parameter. Now, the key sequence can be user-defined.

A new value 3 has been added to the 'Flash Keys Sequence Style' parameter that enables configurable hook-flash key with digit combinations. The key combinations (0 to 9, \*, or #) with the hook-flash key are configured by the following new parameters:

- [FlashKeyToggleToSecondary] / gw-suppl-serv flash-key-toggle-to-secondary: Puts the primary call on hold, or toggles from primary to secondary call.
- [FlashKeyToggleToPrimary] / gw-suppl-serv flash-key-toggle-to-primary: Toggles from secondary to primary call.
- [FlashKeyCallTransfer] / gw-suppl-serv flash-key-call-transfer: Initiates call transfer.
- [FlashKeyConference] / gw-suppl-serv flash-key-toggle-to-primary: Initiates a three-way conference call.
- [FlashKeyByeAndToggle] / gw-suppl-serv flash-and-toggle: Ends the active call (sends a SIP BYE message) and the previously held call becomes active.
- [FlashKeyByeToSecondary] / gw-suppl-serv flash-key-bye-2-secondary: Ends the secondary call (sends a SIP BYE message) which was on hold.

**Applicable Products:** All

## 2.8.2 Resolved Constraints

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

**Table 13: Resolved Constraints for Version 7.26A.356.888**

Incident	Description
MSBR-18343	Device crashes because of low memory when PPPoE configured with BVI underlining interface. <b>Applicable Products:</b> Mediant 500Li
MSBR-18601	CLI command <code>public-key</code> when configuring a user returns an "invalid argument" error. <b>Applicable Products:</b> Mediant 500Li
MSBR-18616	Start Script file resets the remote underlying port of Mediant 5G-EA module. <b>Applicable Products:</b> Mediant 500Li
MSBR-18627	Startup Script file using Mediant 5G-EA module shuts down the GigabitEthernet 0/0 interface. <b>Applicable Products:</b> Mediant 500Li
MSBR-18628	Loading a Startup Script file causes script errors. <b>Applicable Products:</b> All
MSBR-18638	Device crashes with a reset. <b>Applicable Products:</b> Mediant 800Ci
MSBR-18712	SIP re-INVITE message for VBD coders doesn't increment SDP version. <b>Applicable Products:</b> Mediant 500
MSBR-18840	Device crashes with a restart. <b>Applicable Products:</b> Mediant 500Li
MSBR-18891	No protection of CWMP / TR-069 ACS connection against foreign access attempts. <b>Applicable Products:</b> Mediant 500; Mediant 800
MSBR-18985	No CLI command to stop BRI interface. <b>Applicable Products:</b> Mediant 500Li; Mediant 500L
MSBR-19118	Hotline feature not functioning completely. <b>Applicable Products:</b> Mediant 500Li

## 2.9 Version 7.26A.356.773

This version includes new features, known constraints and resolved constraints.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.9.1 New Features

This section describes the new features introduced in this version.

#### 2.9.1.1 CLAT for 464XLAT Enabled per LAN Interface

CLAT (customer-side translator) mechanism for 464XLAT must now be enabled per LAN interface. CLAT is enabled using the following new CLI command under the specific interface:

```
(config-data)# interface VLAN 1
(conf-if-VLAN 1)# clat-enable
```

Disabling CLAT is done using the no form (no clat-enable).

**Applicable Products:** Mediant 500Li; Mediant 800Ci

#### 2.9.1.2 DHCP Option 160 for Auto-Provisioning CLI Script and Configuration Package Files

The device now supports DHCP Option 160 for auto-provisioning the device with the CLI Startup Script file and Configuration Package file. Previously, this option supported only the software (.cmp) file and configuration (.ini) file.

A single URL in the DHCP Option 160 can specify either:

- Software file only
- Software file and ini file
- Software file and Configuration Package file
- Software file and CLI Startup Script file

DHCP 160 is enabled using the following existing command:

```
(config-data)# interface <Interface>
(conf-if-<Interface>)# ip dhcp-client request 160
```

**Applicable Products:** All

#### 2.9.1.3 LAN Source Address Sent in DHCP Relay Packets

The device (DHCP relay agent) can be configured to include the LAN interface's (DHCP client) address as the source address in DHCP relay unicast packets sent to the DHCP server from the WAN.

To configure this feature, the following new CLI command has been added for the LAN interface where the relay is configured:

```
ip dhcp-source-address interface
```

**Applicable Products:** MP-5xx; Mediant 500Li; Mediant 800Ci

### 2.9.1.4 Elliptic Curve Digital Signature Algorithm (ECDSA) Support for TLS

The device can now generate Elliptic Curve Digital Signature Algorithm (ECDSA) public-private keys. This means that the device can generate certificate signing requests (CSRs) and self-signed certificates that are digitally signed with ECDSA keys.

This feature also provides support for using ECDSA keys for accessing the device's CLI through an SSH connection. Instead of logging in with username and password, only username is required, and authentication is automatically done using the public key. (Up until now, only RSA was supported for SSH.)

To support this feature, a new parameter called 'Private Key Format' has been added to the Change Certificates page (TLS Context table > Change Certificates). The parameter defines the required key algorithm (ECDSA or RSA). When ECDSA is selected, the existing 'Private Key Size' parameter defines the required ECDSA key size (256-bit, 384-bit, or 521-bit).

**Applicable Products:** All

### 2.9.1.5 FXO Support for MP-508

The MP-508 device now also supports FXO interfaces. The hardware configuration of this model includes four FXO and four FXS interface ports.

**Applicable Products:** MP-508

### 2.9.1.6 USB Port Shut Down (Power Disconnect)

The device's USB port(s) can now be shut down, by disconnecting power to them. This may be useful for security purposes when the USB port(s) is not used.

Shutting down the USB port(s) is done using the following new CLI command:

```
(config-system)# hw
(hw)# usb-power {off|on}
```

On the Web interface's Monitor page, if a USB stick is connected to the USB port and it's shut down, the USB slot icon changes to gray.

**Applicable Products:** All

### 2.9.1.7 Improved Handling of Truncated DNS Responses

Previously, the device suffered limitations in handling DNS responses that exceeded a threshold of 30 A records (IP addresses) for a single hostname. These DNS responses, identified by the truncation flag (TC bit) -rest of IP addresses truncated to fit packet size - were discarded entirely.

Now, the device effectively handles truncated DNS responses. It uses the first 30 A records (and any in its cache) and ignores the rest of the truncated DNS-resolved IP addresses.

**Applicable Products:** All

### 2.9.1.8 Access Restricted to Device's TR-069 Server by ACS IP Addresses

The device can now be enabled to restrict access to its TR-069 server. When enabled, the device automatically configures the firewall with the ACS IP addresses (manually configured or DNS resolved if FQDN) to allow access to the TR-069 listening port (configured by [TR069HTTPPort]) and blocks all other traffic. The device can add up to six ACS IP addresses to the firewall.

This feature is enabled (disabled by default) using the new ini file parameter [TR069HTTPPortRestriction] or CLI command `configure system > cwmp > port-restriction`.

When enabled, the allowed IP addresses can be viewed using the new CLI command `configure system > cwmp > display-allowed-acs-ips`.

**Note:** This feature requires that the firewall be enabled on the TR-069 interface.

**Applicable Products:** Mediant 500Li; Mediant 800Ci; MP-5xx

### 2.9.1.9 WAN Link Redundancy

The device now supports WAN link redundancy, whereby the two WAN ports (GigabitEthernet 0/1 and GigabitEthernet 0/0) operate in active/standby mode. In case of a link failure, the device automatically switches to the second (redundant) WAN port interface.

This feature is supported by the new WAN Secondary Interface page (Setup menu > IP Network tab > Core Entities folder > WAN Secondary Interface).

**Applicable Products:** MP-532; MP-524

### 2.9.1.10 WAN MAC Placeholder for Auto Update, Zero Conf, and User-Agent Header

The device now supports a placeholder for its WAN MAC address (of gigabitethernet 0/0). The new placeholder string is "<WANMAC>" or "<wanmac>" (case sensitive) and can be used for the following features:

- Auto Update - URL path (including folders) and filename
- Zero Conf - URL path (including folders) and filename
- SIP User-Agent header –information in the outgoing message, configured by the existing parameter [AupdHttpUserAgent]

For the Auto Update and Zero Conf mechanisms, the placeholder can be used in any URL file parameter (e.g., IniFileUrl, CLISTartupScriptUrl, and AutoCmpFileUrl).

**Applicable Products:** All

### 2.9.1.11 Cellular Status Display of Mediant 5G-EA on Web Monitor Page

The device's Monitor page in the Web interface now displays the cellular status of Mediant 5G-EA. This includes whether its 4G or 5G, the cellular interface (e.g., 0/0), LAN port connectivity status, and existence of SIM cards (up to two).

**Applicable Products:** All

### 2.9.1.12 Web Display of IMEI Number of Internal LTE and External Mediant 5G-EA

The Web interface's Device Information page now differentiates between the International Mobile Equipment Identity (IMEI) number of the internal LTE cellular modem and the IMEI number of the external Mediant 5G-EA cellular module:

- 'IMEI' – displays the IMEI of the internal LTE.
- 'External IMEI' - displays the IMEI of the Mediant 5G-EA

**Applicable Products:** All

### 2.9.1.13 Web Access and Protection Updates

The following updates have been made to existing parameters related to web access and protection:

- The 'Web Hostname' parameter (WebHostname) has been renamed 'Web Server Name'. When configured, the device can be accessed using only the 'Web Server Name' value or the device's IP address.
- The following parameters are obsolete:
  - 'DNS Rebinding Protection' / [DNSrebindingProtectionEnabled]
  - [HostHeaderProtection]

**Applicable Products:** All

### 2.9.1.14 High Voltage and Loop Current Configuration for FXS

High voltage and loop current can now be configured per FXS port for IP-to-Tel calls, using the following parameters:

- EnhancedFXSLineCurrent - Defines the FXS off-hook current
- EnableTrapezoidRing - enables high voltage ringing of sinusoidal 75 Vrms per port (maximum ports listed below per product)

The high voltage capabilities are as follows:

- MP-504 can ring all four ports simultaneously.
- MP-508 can ring up to 4 ports simultaneously.
- MP-524 can ring all 24 ports simultaneously.
- MP-532 can ring all 32 ports simultaneously.

**Note:** "Trapezoid" remains in the parameter name EnableTrapezoidRing because of the previous model, where high voltage ringing could be obtained only by a trapezoid waveform. The current model generates a sinusoidal waveform high voltage ringing.

**Applicable Products:** MP-5xx

### 2.9.1.15 Network Configuration and Port Information Update in Web Interface

The following updates have been made in the Web interface regarding LAN and WAN port information and current network configuration:

- The Current Network Configuration page has been moved under the Advanced folder (Setup menu > IP Network tab > Advanced folder > Current Network Configuration).
- The Ethernet Port Information page (Monitor menu > Monitor tab > Network Status > Ethernet Port Information) has been removed.
- The Network View page (Setup menu > IP Network tab > Network View) now displays what the Ethernet Port Information page displayed (instead of current network configuration).
- When a LAN port icon is clicked on the Monitor page, it now opens the new Network View page instead of the removed Ethernet Port Information page.

**Applicable Products:** All

### 2.9.1.16 Configurable Hook-Flash with Digit Key Sequences for FXS Calls

Previously, hook-flash key sequences by pressing the flash button and a digit on the phone's keypad was hardcoded. The type of key sequence was specified by the 'Flash Keys Sequence Style' (FlashKeysSequenceStyle) parameter. Now, the key sequence can be user-defined.

A new value 3 has been added to the 'Flash Keys Sequence Style' parameter that enables configurable hook-flash key with digit combinations. The key combinations (0 to 9, \*, or #) with the hook-flash key are configured by the following new parameters:

- [FlashKeyToggleToSecondary] / gw-suppl-serv flash-key-toggle-to-secondary: Puts the primary call on hold, or toggles from primary to secondary call.
- [FlashKeyToggleToPrimary] / gw-suppl-serv flash-key-toggle-to-primary: Toggles from secondary to primary call.
- [FlashKeyCallTransfer] / gw-suppl-serv flash-key-call-transfer: Initiates call transfer.
- [FlashKeyConference] / gw-suppl-serv flash-key-conference: Initiates a three-way conference call.
- [FlashKeyByeAndToggle] / gw-suppl-serv flash-key-bye-and-toggle: Ends the active call (sends a SIP BYE message) and the previously held call becomes active.
- [FlashKeyByeToSecondary] / gw-suppl-serv flash-key-bye-2-secondary: Ends the secondary call (sends a SIP BYE message) which was on hold.

**Applicable Products:** All

### 2.9.1.17 Multiple Digit Map Sets for Tel-to-IP Calls

Up to two sets of digit maps (primary and secondary) can now be configured for Tel-to-IP calls. The digit map set to use is specified in the Tel Profile table.

This feature is supported by the following new parameters:

- 'Secondary Digit Mapping Rules' / [SecondaryDigitMapping] / gw-dtmf-and-dial secondary-digitmapping: A global parameter that defines the secondary digit map. The digit map patterns are separated by a vertical bar (|). The primary digit map is defined by the existing global parameter [DigitMapping] (Gateway > DTMF and Supplementary > DTMF and Dialing).
- 'Digit Mapping': A Tel Profile parameter that determines which digit map set to use (**Primary** or **Secondary**).

**Applicable Products:** All

### 2.9.1.18 Corresponding CLI Command for Fake Retry After

The SIP Retry-After header feature (configured by the ini file parameter [FakeRetryAfter]) is now also configurable through the device's CLI, using the new command `configure voip > sip-definition settings > fake-retry-after`.

**Applicable Products:** All

### 2.9.1.19 Additional Authentication Modes for Cellular Interface

Additional authentication modes are now available for the Mediant 5G-EA cellular modem (cellular 0/0/0 or 0/0/1). Previously, only CHAP and PAP (both) were enabled.

```
(config-data)# interface cellular 0/0/1
(conf-cellular-0/0/1)# profile
(profile-#default)# authentication {chap|mschapv2|none|pap|pap-chap}
```

**Applicable Products:** All

## 2.9.2 Known Constraints

This section lists known constraints.

**Table 14: Known Constraints in Version 7.26A.356.773**

Incident	Description
MSBR-18639	Configuring a customized name for a Dynamic DNS (DDNS) service provider isn't functioning. A workaround is to run the command without specifying a name ( <code>configure data &gt; dynamic-dns &gt; service custom</code> ). <b>Applicable Products:</b> All

## 2.9.3 Resolved Constraints

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

**Table 15: Resolved Constraints for Version 7.26A.356.773**

Incident	Description
MSBR-16768	M5G-EA loads changed configuration only after a reboot. <b>Applicable Products:</b> Mediant 500Li
MSBR-17435	High CPU load and low throughput observed on Layer 2 bridge. <b>Applicable Products:</b> Mediant 500Li
MSBR-17436	Layer 2 Bridge requires (shouldn't) an IP address on the WAN interface to forward traffic. <b>Applicable Products:</b> Mediant 500Li
MSBR-17518	Configuration of the remote port for the M5G-EA module doesn't delete existing routes of the remote port. <b>Applicable Products:</b> Mediant 500Li
MSBR-17795	IPv6 prefix delegation through DHCPv6 server isn't functioning with infinity lifetime. <b>Applicable Products:</b> Mediant 500Li
MSBR-17878	Incoming call failure when IP-to-Trunk Group calls attempted. <b>Applicable Products:</b> Mediant 500Li
MSBR-17906	The <code>ip dns server</code> command is missing from the CLI. <b>Applicable Products:</b> Mediant 500Li
MSBR-17997	REST CDR reporting fails, and connection isn't established with CDR REST server. <b>Applicable Products:</b> Mediant 500Li
MSBR-18175	Missing PAP-only option for authentication with M5G-EA. <b>Applicable Products:</b> Mediant 500Li
MSBR-18269	Device crashes (resets) upon DHCP and QoS configuration. <b>Applicable Products:</b> Mediant 500Li
MSBR-18323	Issues experienced with Proxy Hot Swap feature (CLI command <code>fake-retry-after</code> missing). <b>Applicable Products:</b> All
MSBR-18329	When a user is associated with two different FXS ports, the UUID is identical. <b>Applicable Products:</b> MP-50x

Incident	Description
MSBR-18343	The device crashes upon PPPoE with underline interface bvi. <b>Applicable Products:</b> Mediant 500Li
MSBR-18344	The device crashes upon the receipt of a response from AudioCodes Redirect Server. <b>Applicable Products:</b> Mediant 500Li
MSBR-18541	Echo heard on PSTN side of FXS-to-PSTN call (i.e., no echo cancellation). <b>Applicable Products:</b> Mediant 500Li
MSBR-18605	The device crashes when PPPoE dial-in or 5G WAN uplink is established. <b>Applicable Products:</b> Mediant 500Li
MSBR-18609	The device crashes if strict certificate validation is enabled for a TLS Context. <b>Applicable Products:</b> All

## 2.10 Version 7.26A.356.630

This version includes new features, known constraints and resolved constraints.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.10.1 New Features

This section describes the new features introduced in this version.

#### 2.10.1.1 Global IP Address Exposed to Public

The device can now discover and display its public-facing IP address as seen by external internet services. The device queries the ident.me web service via an HTTP request to determine its externally visible IP address.

The exposed IP address can be viewed using the following new CLI commands:

- **MSBR:**

```
debug get-global-ip source data [source-address] interface  
<Interface><Number>
```

- **Mediant 500Li / Mediant 800Ci / MP-5xx:**

```
debug get-global-ip network-source <Interface Name>
```

**Note:** When the device operates behind NAT, the displayed IP address is that of the upstream router or gateway providing internet access, not the device's local IP address.

**Applicable Products:** All

#### 2.10.1.2 Parameters for Provisioning URL to CMP File Now Online

The following parameters that configure the URL of the provisioning server where the device's software file (.cmp) is located no longer require a device reset for their settings to take effect:

- CmpFileURL
- AutoCmpFileUrl

**Applicable Products:** All

### 2.10.1.3 Direct Access to CLI Enabled Mode for Security Administrators

Users with Security Administrator privileges can now skip the `enable` command and start in Privileged User mode (`#` prompt) upon CLI login. This feature is enabled using the following new command:

```
system > cli-setting > direct-exec on|off
```

**Applicable Products:** All

### 2.10.1.4 Dual APNs for Cellular Interfaces

The device can be configured with up to two cellular Access Point Names (APN), which identify the packet data networks (PDN). This allows, for example, to have separate traffic on each APN.

This feature is supported by the following Web interface updates:

- The Monitor page now provides a SIM icon, which displays the physical status of the cellular modem.
- The WAN Interface page (Monitor > WAN > WAN Interface) provides a new read-only field called 'Mode' that displays the APN mode (**Single PDN** or **Multi PDN**).

**Applicable Products:** Mediant 500Li; Mediant 800Ci

### 2.10.1.5 Debug for Cellular Interfaces per APN

The device can debug the cellular interface per APN when dual APNs are configured. The debug is sent to syslog. This feature is supported using the following new CLI command:

```
# debug cellular [0/0|0/0/Sub Interface ID] syslog
```

**Applicable Products:** Mediant 500Li; Mediant 800Ci

### 2.10.1.6 Cellular Network Priority by RSRP

When the device is installed with a SIM card with multiple cellular carriers, the device can scan the different networks to identify the one with the strongest signal strength (highest RSRP level) and then automatically connect to it.

This feature is enabled by the new `mode scan-priority` command:

```
(conf-cellular-0/0)# pdn-policy  
(cell-pdn-policy)# mode scan-priority
```

**Note:**

- Once a cellular network is chosen, the device doesn't change the cellular network (even if another network later has a stronger signal strength).
- For this feature, the device only checks profiles that are configured with MCC and MNC values.
- If connectivity is lost with the chosen profile (or registration fails), the device falls back to the default profile.

**Applicable Products:** Mediant 500Li; Mediant 800Ci; Mediant 500L; Mediant 800C

### 2.10.1.7 Zero Configuration using Full INI File

The Zero Configuration feature now also supports the ini file for configuring the device. This is full configuration (not incremental). Previously, Zero Configuration could only process a CLI script file to configure the device.

For ini file download, the Redirect Service must be configured with a Location whose URL contains the ini configuration filename (.ini), for example, `http://172.17.125.19/myconfigfile.ini`.

**Applicable Products:** All

### 2.10.1.8 Advertising IPv6 WAN's MTU Size to LAN

The device can now be configured to inform the LAN interface which WAN interface's MTU size to use in the Router Advertisement Daemon (radvd) message. This feature is configured on the LAN interface, using the following new command:

```
ipv6 nd ra propagate-mtu <WAN Interface Name>
```

**Applicable Products:** All

### 2.10.1.9 Configurable Dynamic DNS Servers

Dynamic DNS (DDNS) service providers (IPv4 and IPv6) can now be configured. Previously, the device offered only three fixed domains for dynamic DNS (`dtc.com`, `dyndns.org`, and `no-ip.com`), which are still supported. When the interface changes its state to or from connected, the DDNS checks if the address was changed, and sends an update if so.

This feature is configured using the following new command:

```
(config-data)# dynamic-dns
(conf-dyndns)# service custom (DNS server provider name>
(conf-MyDDNS)#
  hostname          Name registered in DNS service
  interface         Set the interface to send the IP
  post-auth         DNS service credentials
  pwd              Display current configuration mode path
  success-response Server success response strings
  update-interval  Period to wait after each DNS update (in days)
  url              Change URL of message. After the https://
  use-ipvx         In URL use ipvx instead of myipvx
  use_ssl_mode
  username
```

The URL to update the DDNS server when an IP changes must be specified using the following format in the HTTP request: `[https/http://[username]:[password]@[provider_url]?[post-auth]&[hostname=]&[ip=]&[ipv6=]`

**Applicable Products:** All

### 2.10.1.10 CLI Display of Signal Strength per Cellular Antenna

The `show data cellular status` command now also displays LTE signal strength (RSRP) per antenna (in dBm). This can be used to detect, for example, bad antenna assembly and cable disconnections.

In normal conditions, each antenna should have similar RSRP values, as shown in the following command output example:

```
(conf-cellular-0/0)# do show data cellular status
```

```
Cellular 0/0 interface status:

Administrative:      UP
Modem status:       UP
Profile name:       default
Signal strength:    -102 dBm
  Antenna 0 (main): -103 dBm
  Antenna 1 (div):  -104 dBm>
...

```

**Applicable Products:** Mediant 500Li; Mediant 800Ci; Mediant 500L MSBR; Mediant 800C MSBR

### 2.10.1.11 SNMP for Getting Track Statistics

The device now supports getting track statistics through SNMP. This is done using the new SNMP table `acSysDataStatusTrackStatsTable`. Previously, track statistics could only be done through CLI (`show data track`).

**Applicable Products:** All

### 2.10.1.12 DSL Debug Level

The debug level for DSL interfaces can now be configured using the following new CLI command:

```
debug dsl [1-8]
```

**Applicable Products:** Mediant 500Li; Mediant 800Ci

### 2.10.1.13 MP-504/MP-508 Product Name Reflected in Management Interfaces

The License Key for MP-504/508 now correctly reflects the product names and user-agent names of these devices in the Web interface, CLI, and SNMP.

**Applicable Products:** MP-504; MP-508i

### 2.10.1.14 Updated CLI Command Names

The following CLI commands were renamed to align with AudioCodes CLI syntax conventions:

Old Name	New Name
<code>audc_sw_ver</code>	<code>audc-sw-ver</code>
<code>firmware_rev_id</code>	<code>firmware-rev-id</code>
<code>firmware_version</code>	<code>firmware-version</code>
<code>sim_iccid</code>	<code>sim-iccid</code>
<code>sim_lock_status</code>	<code>sim-lock-status</code>
<code>sim_pin_code_change</code>	<code>sim-pin-code-change</code>
<code>sim_pin_code_unlock</code>	<code>sim-pin-code-unlock</code>
<code>sim_puk_code_unlock</code>	<code>sim-puk-code-unlock</code>

**Applicable Products:** All

## 2.10.2 Known Constraints

This section lists known constraints.

**Table 16: Known Constraints in Version 7.26A.356.630**

Incident	Description
MSBR-14614	<p>If the command <code>ipv nd ra propagate-mtu &lt;WAN interface name&gt;</code> or <code>ipv nd pd &lt;WAN interface name&gt; &lt;prefix suffix&gt;</code> is configured on any LAN interface, if the user deletes the WAN interface after upgrading from M10 to this version, the <code>show run</code> output is incorrect. The <code>show run</code> output of the LAN interface doesn't display the <code>propagate-mtu</code> and <code>nd pd</code> command settings. A workaround is to remove (<code>no</code> command) and reconfigure the CLI command(s) on the LAN interface.</p> <p><b>Applicable Products:</b> Mediant 500Li; Mediant 800Ci</p>

## 2.10.3 Resolved Constraints

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

**Table 17: Resolved Constraints for Version 7.26A.356.630**

Incident	Description
MSBR-16642	<p>The CLI command output of <code>show data ip dhcp binding vlan [id]</code> doesn't display the binding of the specific VLAN.</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-16756	<p>Stopping the rpcap server causes the device to reset.</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-16760	<p>Remark can't be added to the Access List (<code>access-list &lt;name&gt; remark</code>).</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-16800	<p>No corresponding CLI command for the ini file parameter <code>EnableAutoSaveConfiguration</code>.</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-16837	<p>The device doesn't send the NTP option 42 in the DHCP offer if configured for "auto" (<code>ip dhcp-server ntp-server auto</code>).</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-17070	<p>When configured as an L2TP server, unnecessary routes are shown in the output of <code>sh d ip route</code>.</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-17199	<p>ATM interfaces can't be configured ("doesn't exist") after upgrade to 7.26A.356.174.</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-17225	<p>Cancel call waiting issue after software upgrade.</p> <p><b>Applicable Products:</b> Mediant 500L</p>
MSBR-17229	<p>Hook flash feature for toggling between call parties doesn't function.</p> <p><b>Applicable Products:</b> Mediant 500Li</p>
MSBR-17247	<p>The device resets during Auto-Update even though a reset is not needed for the parameters (<code>reload if-needed</code> in CLI Script file).</p> <p><b>Applicable Products:</b> Mediant 500Li</p>

Incident	Description
MSBR-17315	Emergency call routing failure for FXS endpoints that aren't registered (even though enabled with FXSEmergencyCallForUnregisteredPort parameter). <b>Applicable Products:</b> Mediant 500Li
MSBR-17342	The Web interface's Save and Reset buttons are always red after configuring device as an ATA for Teams SIP Gateway. <b>Applicable Products:</b> Mediant 500Li
MSBR-17356	Selection of cellular carrier network not according to best signal strength. <b>Applicable Products:</b> Mediant 500Li
MSBR-17358	Call conferencing failure between BRI ISDN phones. <b>Applicable Products:</b> Mediant 500Li
MSBR-17441	The "<MAC>" placeholder in URL for HTTPS-based provisioning isn't functioning. <b>Applicable Products:</b> Mediant 500Li
MSBR-17449	The Web interface's Reset button highlights following auto provisioning because CmpFileURL and AutoCMPFileURL parameters are erroneously defined as offline. <b>Applicable Products:</b> Mediant 500Li
MSBR-17466	CPU overload due to TR-069 traffic, freezing Web interface. <b>Applicable Products:</b> Mediant 500Li
MSBR-17512	Error when running the CLI command <code>sh data cellular network-scan 4g</code> . <b>Applicable Products:</b> Mediant 500Li
MSBR-17657	Fake alarm after software upgrade ("SW Upgrade error. Request failed:Registered Users"). <b>Applicable Products:</b> Mediant 500Li
MSBR-17667	The phone displays voicemail status notification even though the voicemail was deleted on the server. <b>Applicable Products:</b> Mediant 500Li
MSBR-17695	T.38 Version 3 isn't supported. <b>Applicable Products:</b> Mediant 500Li
MSBR-17722	The device doesn't resolve TR-069 ACS DNS when reconnecting after a connection loss. <b>Applicable Products:</b> Mediant 500Li
MSBR-17727	The device crashes (resets) due to a kernel panic. <b>Applicable Products:</b> Mediant 500Li
MSBR-17731	The device sometimes crashes (resets). <b>Applicable Products:</b> Mediant 800
MSBR-17781	User with Administrator role can change (elevate) to Security Administrator role. <b>Applicable Products:</b> Mediant 500Li
MSBR-17799	NAT translation doesn't function correctly. <b>Applicable Products:</b> Mediant 500L
MSBR-17803	ICE candidates are missing from the SDP of the outgoing SIP reINVITE message. <b>Applicable Products:</b> Mediant 800
MSBR-17897	No OVOC access when using Trap Manager Host Name. <b>Applicable Products:</b> Mediant 500Li

## 2.11 Version 7.26A.356.459

This version includes new features, known constraints and resolved constraints.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.11.1 New Features

This section describes the new features introduced in this version.

#### 2.11.1.1 Allow Emergency or Hotline Calling for Unregistered FXS Endpoints

The device can now be enabled to allow FXS endpoints (ports) to make emergency calls (Tel-to-IP), even if registration of a specific port to the SIP proxy server has failed for whatever reason, for example, payment required. This feature applies to all FXS endpoints, including ports configured for automatic dialing (Automatic Dialing table).

When an analog phone connected to a port that fails to register, goes off-hook, the device plays a reorder tone to the port, indicating to the end user that the service is unavailable. However, this end user can still place an emergency call (or call to any of the user-defined emergency numbers). These calls go through the same IP destination (i.e., proxy server).

This feature is enabled (by default, disabled) by the following new global parameter:

- **ini File:** [FXSEmergencyCallForUnregisteredPort]
- **CLI:** `configure voip > gateway analog fxs-setting > fxs-emg-call-for-unreg-port`

**Note:** This feature also requires configuring the 'Set Out-Of-Service On Registration Failure' [OOSOnRegistrationFail] to **Enable**.

**Applicable Products:** FXS Gateways

#### 2.11.1.2 DHCPv6 Support for VRRP IPv6

The device now supports Virtual Router Redundancy Protocol (VRRP) over IPv6.

This feature is configured using the following new CLI command, which associates the DHCPv6 server with the VRRP logical interface:

```
(config-data)# interface <Interface>
(conf-if-<Interface>)# ipv6 dhcp-server vrrp_id <VRRP ID>
```

**Applicable Products:** All

#### 2.11.1.3 Support for CLAT in 464XLAT Architecture

The device now supports the CLAT (customer-side translator) mechanism for 464XLAT. 464XLAT provides a simple technique for an IPv4 client with a private address to connect to an IPv4 host over an IPv6 network. 464XLAT only supports IPv4 in the client-server model, where the server has a global IPv4 address. This means, it's not suited for IPv4 peer-to-peer communication or inbound IPv4 connections.

The architecture includes the following components:

- PLAT (provider-side translator): Translates N:1 global IPv6 addresses to global IPv4 addresses, and vice versa.
- CLAT: Translates private IPv4 addresses to global IPv6 addresses, and vice versa. **Only this component is supported by the device.**

This feature (CLAT) is configured using the following new CLI commands:

```
(config-data)# router clat
(conf-router-clat)#
ipv4-dst-network          IPv4 destination network to reach via
translation (using CLAT)
ipv6-dst-prefix          IPv6 destination prefix (PLAT prefix)
ipv6-src-prefix          IPv6 source prefix (CLAT prefix)
```

**Note:**

- The IPv6 route must be entered in the destination prefix.
- Up to 5 destination networks can be added.
- The IPv6 source prefix can be added statically, or by using prefix delegation interface.

**Applicable Products:** Mediant 500Li; Mediant 800Ci

#### 2.11.1.4 Controlling 5G Modes NSA and SA for M5G-EA Module

The M5G-EA cellular module can now be configured to operate in either 5G Non-Standalone (NSA) or 5G Standalone (SA) mode. By default, both modes are enabled, and the module automatically chooses a mode according to the cellular network.

The mode that is not required is disabled using the following new CLI command:

```
(conf-cellular-0/0)# sim disable-nr5g-mode {nsa|sa}
```

**Applicable Products:** All

#### 2.11.1.5 Cellular PPP Mode Now Obsolete

The device no longer supports PPP mode for cellular interfaces. Consequently, the following CLI command has been removed:

```
(config-data)# interface cellular 0/0
(conf-cellular)# mode ppp
```

**Applicable Products:** All

#### 2.11.1.6 Dual APN for M5G-EA Module

The M5G-EA cellular module now supports dual APN, whereby the installed SIM card can have two APNs.

This feature is configured by the following new CLI command?

```
(config-data)# interface cellular 0/0/1
(conf-cellular-0/0/1)# profile
(cell-profile-config)# apn
```

**Applicable Products:** All

### 2.11.1.7 DHCP Option 160 for Auto-Provisioning

The device now supports DHCP Option 160 for auto-provisioning (Auto-Update). DHCP Option 160 provides the device with the URL address of the provisioning server from where it can download the software (.cmp) and configuration (.ini) files.

This feature is configured by the existing command:

```
M500Li(config-data)# interface <Interface>
M500Li(conf-if-< Interface>)# ip dhcp-client request 160
```

**Applicable Products:** All

### 2.11.1.8 Digest Authentication for Zero Configuration

The device now supports digest authentication for the Zero Configuration feature. If the Redirect server provides the device with a provisioning server URL that contains a username and password, the device can now use these credentials during the authentication process between it and the provisioning server.

**Applicable Products:** All

### 2.11.1.9 Responder Support for Cisco's IP SLA UDP Jitter Operation

The device can now be configured as a responder to Cisco's IP Service Level Agreements (SLAs) UDP jitter test monitor protocol (MOS and QoS), by replying with control packets and UDP echo measurement packets. Up to one instance of the service (in one VRF) is supported and up to 5 UDP measurement streams are supported.

This feature is supported by the following new CLI commands:

- Start service in main-vrf:  

```
(config-data)# ip sla responder udp-echo
```
- Start service in specific VRF:  

```
(config-data)# ip sla responder udp-echo vrf <Name>
```
- Stop service (no command):  

```
(config-data)# no ip sla responder udp-echo
```
- View service status:  

```
show data ip sla responder
```

**Applicable Products:** All

### 2.11.1.10 Configuration Package File Enhancements

The following enhancements to the Configuration Package file have been introduced:

- The 7-Zip file format (.7z) is now used (instead of .tar.gz) for the Configuration Package file. 7-Zip allows the file to be compressed (LZMA2) and optionally, encrypted with a password and the AES-256 algorithm.

The Configuration File also supports the inclusion of TLS private keys, trusted root certificates, and TLS certificates (when file encryption is used).

- The CLI command for copying the Configuration Package file supports a new option for encrypting the file and optionally, for including certificates (only to):

```
copy configuration-pkg to|from <URL> encrypted <password>
certificates
```

- The Auto-Update mechanism can now provision the device with the Configuration Package file, using the following new CLI command:

```
(config-system) # automatic-update
(auto-update) # configuration-pkg <URL>
```

If the file is password-protected, the password can be specified in the CLI, using the following new command:

```
(config-system) # automatic-update
(auto-update) # default-configuration-package-password
<password>
```

This feature is also applicable when downloading the Configuration Package file through SFTP.

**Note:** For backward compatibility, the device supports the upload of the Configuration Package file in TAR (.tar.gz) format.

**Applicable Products:** All

### 2.11.1.11 Display of Static Routes and Tracks Configuration

The device can now display the static routes and tracks (data) configuration, using the following new CLI show commands:

```
show running-config data static-routes
show running-config data tracks
```

**Applicable Products:** All

### 2.11.1.12 Hiding Passwords in Activity Log

The device now automatically hides all passwords in the Activity Log. Passwords are hidden by asterisks (\*). Up until now, some passwords were visible in the Activity Log (depending on configuration parameter or command).

**Applicable Products:** All

### 2.11.1.13 Hiding Passwords in CLI Command History Buffer

The device can now be configured to show or hide (default) passwords in the CLI command history buffer. The device hides the passwords by replacing them with asterisks (\*).

Therefore, when using the up and down arrow keys on the CLI prompt to recall previously typed commands from the history buffer, or using the existing `history` command to view the history buffer, passwords are hidden.

This feature is configured using the following new CLI command:

```
conf system > cli-settings > password-history-visible {off|on}
```

**Applicable Products:** All

### 2.11.1.14 Clearing CLI Command History

The device's CLI command history buffer, which stores previously typed commands during the current CLI session, can now be cleared using the following new commands:

- To clear all history records:

```
clear history
```
- To clear a specific history record (by index):

```
clear history <index>
```

The CLI history of commands (and their indices) is displayed using the existing `history` command. Recalling previously typed commands from the history buffer is done using the up and down arrow keys, as previously supported.

**Applicable Products:** All

### 2.11.1.15 Web Interface Support for IPv6 Configuration

The device's Web interface now supports configuration for IPv6:

- MONITOR -> NETWORK STATUS -> Routing table
- SETUP -> IP NETWORK -> NETWORK VIEW
- SETUP -> IP NETWORK -> CORE ENTITIES -> WAN Interface
- SETUP -> IP NETWORK -> CORE ENTITIES -> Static Routes

**Applicable Products:** MP-5xx

### 2.11.1.16 CLI Command `classification_fail_response_type` Renamed

The CLI command `classification_fail_response_type` (in SIP Interfaces table) has been renamed `classification-fail-response-type`. This change aligns with the device's CLI naming conventions.

**Applicable Products:** All

## 2.11.2 Known Constraints

This section lists known constraints.

**Table 18: Known Constraints in Version 7.26A.356.459**

Incident	Description
MSBR-14614	The Web Interfaces table ( <code>web-if</code> ) configuration doesn't appear in the <code>show run</code> output after invoking the CLI command <code>write factory</code> . <b>Applicable Products:</b> Mediant 500Li; Mediant 800Ci

## 2.11.3 Resolved Constraints

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

**Table 19: Resolved Constraints for Version 7.26A.356.459**

Incident	Description
MSBR-15652	The GE 1/1 LED remains lit when the port is shutdown. <b>Applicable Products:</b> Mediant 500Li
MSBR-15685	File transfer over the device's IP public address instead of private IP address. <b>Applicable Products:</b> All
MSBR-15755	The global [ <code>SIPGatewayName</code> ] parameter overrides the 'Gateway Name' parameter in the Trunk Group Settings table. <b>Applicable Products:</b> All
MSBR-15806	High CPU utilization when processing UDP traffic. <b>Applicable Products:</b> Mediant 500Li
MSBR-16041	Pickup feature issue.

Incident	Description
	<b>Applicable Products:</b> Mediant 500Li
MSBR-16081	The device keeps sending the error message "SWWD : Run Task SPLB" on SSL handshake. <b>Applicable Products:</b> Mediant 500Li
MSBR-16219	FXS on-hook puts the call on hold instead of disconnecting it. <b>Applicable Products:</b> All
MSBR-16322	Device crashes when remote SSH session is terminated suddenly (e.g., due to a reset). <b>Applicable Products:</b> Mediant 500Li
MSBR-16358	Devices doesn't try a reregister after a SIP 480 response. <b>Applicable Products:</b> All
MSBR-16484	GRE tunnel requires slight improvement. <b>Applicable Products:</b> Mediant 500Li
MSBR-16512	GRE tunnel configuration fails. <b>Applicable Products:</b> All
MSBR-16567	The syslog includes unnecessary DSP messages. <b>Applicable Products:</b> All
MSBR-16574	Untagged EFM interface overrides tagged interface in bridge mode. <b>Applicable Products:</b> All
MSBR-16613	The [RetryAfterMode] parameter isn't functioning correctly. <b>Applicable Products:</b> All
MSBR-16624	File can't be downloaded (copied) through SFTP. <b>Applicable Products:</b> All
MSBR-16643	The End-User Web interface doesn't display the PPPoE WAN interface when the underlying interface is BVI. <b>Applicable Products:</b> All
MSBR-16736	Music On Hold (MoH) isn't played to FXS endpoint. <b>Applicable Products:</b> All
MSBR-16758	One-way or no audio from and to PSTN/SIP. <b>Applicable Products:</b> All
MSBR-16763	CLI command <code>classification_fail_response_type</code> in the SIP Interfaces table uses underscores instead of hyphens. <b>Applicable Products:</b> All
MSBR-16874	Hook flash doesn't function for call waiting and three-way conferencing calls. <b>Applicable Products:</b> All
MSBR-16960	The PPP interface obtains the local prefix from <code>ipv6cp.interface_identifier</code> . <b>Applicable Products:</b> All
MSBR-16962	BGP network import check doesn't function with IPv6. <b>Applicable Products:</b> All
MSBR-16963	The L2TP server <code>tunnel auth-key</code> isn't added to configuration. <b>Applicable Products:</b> All

Incident	Description
MSBR-17030	Users defined in the Local Users table can connect to the device even when TACACS authentication is enabled. <b>Applicable Products:</b> All
MSBR-17069	The L2TP server ignores the username and password for authentication and allows connection regardless. <b>Applicable Products:</b> All

## 2.12 Version 7.26A.356.180

This version includes known constraints only.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.12.1 Known Constraints

This section lists known constraints.

**Table 20: Known Constraints in Version 7.26A.356.180**

Incident	Description
MSBR-16758	For devices with BRI interfaces and running Version 7.26A.356.174, a bug exists in memory allocation process during device initialization, causing one-way voice. Customers are advised not to use Version 7.26A.356.174, but to upgrade to this version (7.26A.356.180) or later. <b>Applicable Products:</b> Mediant 500; Mediant 500L; Mediant 800B; Mediant 800C

## 2.13 Version 7.26A.356.174

This version includes new features, known constraints and resolved constraints.



- This version is recommended **only** for Mediant 500Li, Mediant 800Ci, and MP-5xx.
- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.13.1 New Features

This section describes the new features introduced in this version.

#### 2.13.1.1 New Product Launch - M5G-EA 5G Cellular Modem

AudioCodes has launched a new product called M5G Extended Access (M5G-EA) 5G cellular modem. This modem can be connected to Mediant 500Li or to any other MSBR device. This version provides preliminary beta release support for M5G-EA.

- Brings 5G connectivity.
- Suitable for indoor and outdoor (IP65 compliant) installations.
- Supports SA and NSA modes.
- Supports dual SIM.

**Applicable Products:** All.

#### 2.13.1.2 Track Destination Obtained Automatically from DNS

The device can now be configured to automatically obtain the tracking destination for a specific source interface, instead of manually configuring a static IP address. The destination is obtained from the DNS server of the associated interface when it uses DHCP or PPP.

The feature is supported by the new optional command `dyn-dns-server`:

```
(config-data)# track 1 icmp echo | icmpv6 echo dyn-dns-server
<interface>
```

**Applicable Products:** All.

#### 2.13.1.3 IPv6 Support for Cellular LTE Interface

The device now supports IPv6 addressing scheme for its cellular LTE interface.

IPv6 is configured using the following new commands under the cellular interface:

```
(config-data)# interface cellular 0/0
(conf-cellular-0/0)# ipv6 enable
(conf-cellular-0/0)# ipv6 address autoconfig
```

**Applicable Products:** Mediant 500Li; Mediant 800Ci; Mediant 500L; Mediant 800C

### 2.13.1.4 Distributing IPv6 Addresses when DHCPv6 Server Unavailable

DHCPv6 facilitates Prefix Delegation (PD), in which the device, as a DHCPv6 client, receives a prefix (on its WAN interface) for delegation and uses it to perform SLAAC connectivity on its LAN side (sending prefix in ICMPv6 Router Advertisement message).

However, if the DHCPv6 server is unavailable, the device (per RFC 7278) can now take a prefix received in an ICMPv6 Router Advertisement message received on the WAN side and use it for SLAAC on the LAN side (as if it were a prefix for PD).

This feature is typically intended (but not limited to) cellular.

This feature is configured as follows:

- WAN interface is configured with the following new CLI command:  

```
(conf-if-<interface>)# ipv6 address autoconfig extnd-prfx-lan
```
- LAN interface is configured with the existing CLI command `ipv6 nd pd` and appropriate SLAAC commands.

**Applicable Products:** All.

### 2.13.1.5 VRRP over IPv6

The device now supports VRRP over IPv6 (in addition to the already supported VRRP over IPv4).

VRRP over IPv6 is configured using the same CLI commands as used for IPv4, but with the new command option `ipv6`:

```
(config-data)# interface vlan <VLAN ID>
(conf-if-vlan <VLAN ID>)# vrrp 1 ipv6
{ip|preempt|priority|timers|track}
```

**Note:** The device uses VRRPv2 for IPv4, and VRRPv3 for IPv6.

**Applicable Products:** All.

### 2.13.1.6 QinQ Support

The devices listed below (Applicable Products) also now support 802.1Q-in-802.1Q (QinQ), as defined by IEEE 802.1ad. QinQ expands VLAN space, by adding an additional 802.1Q tag to 802.1Q-tagged packets.

This feature is enabled using the new CLI command `configure network -> network-setting > wan-copper-fiber-mode` (ini file [WanCopperFiberMode] parameter). It must be configured to `single-copper` or `single-fiber`, depending on the used WAN interface. When not implementing QinQ, the parameter is left at default (`use-all`).

**Note:**

- This feature is supported only on the WAN (not LAN).
- The device must be in single WAN mode (i.e., copper or fiber).

**Applicable Products:** Mediant 500Li; Mediant 800Ci.

### 2.13.1.7 Connection to TR-069 ACS Only when Synchronized with NTP

When the device is configured to connect securely to the TR-069 Auto Configuration Server (ACS) over TLS and to verify the certificate, it can also be configured to connect only when the device is synchronized with the NTP server. This is supported by the new CLI command `configure system > cwmp > ntp-dependency` (ini file [TR069NTPDependency]). The feature is disabled by default.

**Applicable Products:** All.

### 2.13.1.8 Handling Multiple SDP Answers

The device can now be configured to process only the first SDP answer and ignore the others in scenarios where it receives multiple SDP answers (e.g., SIP 183 with SDP and then a 200 OK with SDP, or two 183's with SDP). Therefore, even if a different SDP answer is received, the voice channel doesn't change.

This feature is configured by the new CLI command `configure voip > sip-definition settings > gw-ignore-multiple-answers (ini file parameter [GwIgnoreMultipleAnswers])`.

**Applicable Products:** All.

### 2.13.1.9 New Performance Monitoring for Maximum Active IP-to-Tel and Tel-to-IP Calls

The device now provides the following new SNMP Performance Monitoring MIBs (gauges) that indicate the maximum number of currently active IP-to-Tel and Tel-to-IP calls, globally and per IP Group:

- Per IP Group:
  - acPMSipIPGroupIP2TelActiveCallsTable
  - acPMSipIPGroupTel2IPActiveCallsTable
- Global:
  - acPMSipIP2TelActiveCallsTable
  - acPMSipTel2IPActiveCallsTable

**Applicable Products:** All.

## 2.13.2 Known Constraints

This section lists known constraints.

**Table 21: Known Constraints in Version 7.26A.356.174**

Incident	Description
MSBR-16663	<p>Port forwarding doesn't function when VRRP is enabled.</p> <p><b>Note:</b> Therefore, if you need to use VRRP (IPv4) with port forwarding, it's recommended not to upgrade to this new version, but to remain with version M8, M8.1, or M8.2.</p> <p><b>Applicable Products:</b> All</p>

### 2.13.3 Resolved Constraints

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

**Table 22: Resolved Constraints for Version 7.26A.356.174**

Incident	Description
MSBR-15653	No DSL synchronization occurs on VDSL2 (no vectoring) with keymile DSLAM. <b>Applicable Products:</b> Mediant 500Li
MSBR-15702	The SNMP alarm acAnalogPortSPIOutOfService is raised (analog port SPI out of service), and calls disconnect. <b>Applicable Products:</b> Mediant 500Li
MSBR-15850	If PPPoE has a bridge virtual interface underlying and device connects to BRAS (TR-069), the device resets. <b>Applicable Products:</b> Mediant 500L; Mediant 500Li
MSBR-15871	IPv6 VoIP functionality fails intermittently. <b>Applicable Products:</b> Mediant 500Li
MSBR-15981	The device takes a long time to run CLI commands. <b>Applicable Products:</b> Mediant 500L
MSBR-15982	When the device operates with ARM, it sends the incorrect SIP error code. <b>Applicable Products:</b> Mediant 800
MSBR-16006	The Device resets after running certain CLI commands. <b>Applicable Products:</b> Mediant 500Li
MSBR-16113	After upgrading the device, the cellular interface doesn't go back up again. <b>Applicable Products:</b> Mediant 500Li
MSBR-16151	The <code>authentication</code> command for the cellular profile doesn't accept the value correctly. <b>Applicable Products:</b> Mediant 500Li
MSBR-16218	The device fails to send a response from the Redirect server to the provisioning server when using the URL of the Redirect server in the voice configuration. <b>Applicable Products:</b> Mediant 500Li
MSBR-16220	PPPoE WAN interface is not displayed in the End-User Web interface. <b>Applicable Products:</b> Mediant 500Li
MSBR-16241	OVOC-managed licensing (floating license) has an issue. <b>Applicable Products:</b> Mediant 500L
MSBR-16250	The Web interface's Topology View displays the incorrect assignment of FXS ports to Trunk Groups. <b>Applicable Products:</b> Mediant 500Li
MSBR-16254	In the Web interface's Coders Groups table, when selecting G.722, the 'Payload Type' field becomes empty after clicking <b>Apply</b> . <b>Applicable Products:</b> Mediant 500Li
MSBR-16268	Modifying the default queue in a service map ( <code>qos service-map</code> ) causes loss of connectivity. <b>Applicable Products:</b> Mediant 500Li

Incident	Description
MSBR-16278	Hook flash isn't functioning for call waiting and three-way conference calls. <b>Applicable Products:</b> Mediant 500Li
MSBR-16309	Fallback to the Local Users table for logging into the device when there is no connectivity with the RADIUS server fails. <b>Applicable Products:</b> Mediant 500Li
MSBR-16314	The device's Auto-Update mechanism doesn't redirect when receiving an HTTP 302 Found response. <b>Applicable Products:</b> Mediant 500Li
MSBR-16317	If NTP is disabled, the date and time can't be configured through the Web interface. <b>Applicable Products:</b> Mediant 500Li
MSBR-16319	MAC address of devices whose leases have expired on the LAN are still visible in the output of the command <code>show data ip dhcp binding</code> . <b>Applicable Products:</b> Mediant 500Li
MSBR-16321	The CWMP service doesn't start (no connection with ACS) after a device reset. <b>Applicable Products:</b> Mediant 500Li
MSBR-16370	When the device's HTTPS port for the management interface is changed, there is no longer access to the Web interface. <b>Applicable Products:</b> Mediant 500Li
MSBR-16480	Assigning active WAN interface in VRF causes a device reset. <b>Applicable Products:</b> Mediant 500Li
MSBR-16566	GRE interface line can't be configured. <b>Applicable Products:</b> Mediant 500Li
MSBR-16574	Untagged EFM interface overrides tagged interface in bridge mode. <b>Applicable Products:</b> Mediant 500Li

## 2.14 Versions 7.26A.356.070 / 7.26A.356.074 / 7.26A.356.075

This version includes new features and resolved constraints only.



- **Version 7.26A.356.070** is applicable only to Mediant 500, Mediant 500C, Mediant 500L, and Mediant 800C MSBRs.
- **Version 7.26A.356.074** is applicable only to Mediant 800B MSBRs (see the [Product Notice](#)).
- **Version 7.26A.356.075** is applicable only to Mediant 500Li and Mediant 800Ci.
- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.14.1 New Features

This section describes the new features introduced in this version.

#### 2.14.1.1 Display of IMEI Number for Cellular Interfaces

The International Mobile Equipment Identity (IMEI) number, which is a unique identification or serial number of smartphones is now displayed in the CLI (`show data cellular status`) and Web interface (Device Information page). This feature applies to devices providing the internal cellular modem.

**Applicable Products:** Mediant 500L; Mediant 500Li; Mediant 800C.

#### 2.14.1.2 Multiple LTE Cellular Carriers Support

The device can now be configured with multiple LTE carriers.

In addition, the device can be configured to always connect to a specific carrier, or automatically select a carrier based on signal strength and carrier priority.

Below are the new commands for configuring this feature:

- Multiple carriers are configured using the new `profile` command:

```
(conf-cellular-0/0)# profile MyCarrier
(profile-#MyCarrier)#
```

If a profile is created without a name, "default" is assigned the name. Below shows a configuration example:

```
(conf-cellular-0/0)# do show running-config data interface
cellular 0/0
interface Cellular 0/0
desc "QMI Cellular connection"
mode dhcp
profile default
apn net.hotm
authentication pap
exit
profile peplephone
apn jjjyyyy
```

```

authentication pap
exit
profile verizon
apn vzw
authentication pap
exit

```

- The carrier's MCC/MNC (mobile country code, mobile network code) can be configured, using the new `mcc` and `mnc` commands, for example:

```
(profile-#MyCarrier) # mcc 425 mnc 07
```

- For manually selecting a carrier, the new `profile-selection fixed` command is used, for example:

```
(conf-cellular-0/0) # profile-selection fixed MyCarrier
```

- For automatic selection of carrier, the following new command enables this feature:

```
(conf-cellular-0/0) # profile-selection policy priority
```

- For automatic selection of carrier, the following new commands are used to configure the signal strength threshold for switching carriers if below threshold for a specific duration, and for assigning priority to the carriers (where 1 is highest):

```

(config-data) # interface cellular 0/0
(conf-cellular-0/0) # pdn-policy
(cell-pdn-policy) # rule reception lte rsrp -100
(cell-pdn-policy) # evaluation-time 120
(cell-pdn-policy) # priority 1 Carrier1
(cell-pdn-policy) # priority 2 Carrier2

```

**Applicable Products:** Mediant 500Li.

### 2.14.1.3 Enabling and Disabling Cellular Data Roaming

The device can now be configured to enable or disable cellular data roaming for a specific cellular interface (SIM), using the following new CLI command:

```
(conf-cellular-0/0) # sim roaming
```

**Applicable Products:** Mediant 500L; Mediant 500Li; Mediant 800C.

### 2.14.1.4 Cellular Network Scanning

The device can now scan for cellular networks (3G and 4G, or only 4G) in the surrounding area, using the following new CLI command:

```
show data cellular network-scan {3g-4g|4g}
```

The command's output displays available cellular providers with various cellular information, as shown in the following example:

```

Technology: 3G
Operator: Partner IL
Operator numeric format: 42501
Band: WCDMA 2100
Channel: 10687
Location area code: 27B1
Cell ID: 10CA1E
Primary scrambling code: 499
RSCP: -77
ECIO: -2

```

This feature is useful, for example, for searching the best provider (i.e., strongest signal) to connect the device's SIM.

**Applicable Products:** Mediant 500L; Mediant 500Li; Mediant 800C; Mediant 800Ci.

### 2.14.1.5 Display of Currently Connected Cellular Network

The device can now display information of the cellular network provider to which it's currently connected, using the following new CLI command:

```
show data cellular status servingcell
```

The command's output displays various cellular information such as registration status and signal strength, as shown in the following example:

```
Registration status code: Data mode connected
Registration description: UE is camping on a cell and has
registered to the network in data mode.
Technology: LTE
TDD/FDD: FDD
MCC: 425
MNC: 01
Cell ID: 0xCA1C02
Physical cell ID: 157
E-UTRA-ARFCN: 1600
E-UTRA frequency band: 3
UL bandwidth: 20 MHz
DL bandwidth: 20 MHz
Tracking area code: 3EEF
RSRP: -82
RSRQ: -5
RSSI: -57
SINR: 23
srlevel: 39
```

**Applicable Products:** Mediant 500L; Mediant 500Li; Mediant 800C; Mediant 800Ci.

### 2.14.1.6 Flow Control Status in Show Run

The flow control status for physical interfaces is now displayed in the `show run` command:

```
"Flow Control: RXTX (Remote: RX) "
```

Where:

- *Flow Control* indicates the ability to send (Tx) or receive (Rx) PAUSE frames from a local (device) perspective.
- *Remote* indicates the partner port's ability to send or receive PAUSE frame.

This feature is supported only by the following interfaces: Gigabitethernet (0/0, 1/1, 1/2, 1/3, 1/4) and fiber 0/0.

**Applicable Products:** All.

### 2.14.1.7 Display of Track Destination Failures

Information on track failures (i.e., "up" to "down" state) can now be displayed in the CLI, using the new CLI command option `failure`:

- To display when the last failures occurred for each track:

```
show data track brief failures
```

Example:

```
# show data track brief failures
track 1 has no failures (target 8.8.8.8, Description
"ping_google")
track 2 failed in the last 24 hours (target 8.8.4.4,
Description)
track 10 never been UP (target 1.11.2.22, Description)
track 3 failed in the last hour (target 8.8.8.8, Description)
```

- To display when the last failure occurred for each track for a specified IP address or interface:

```
show data track brief failures <IP address|interface>
```

- To display how many times a track failed and for how long (total), in the last x hours (1-720):

```
show data track brief failures <last x hours>
```

Example:

```
# show data track brief failures 24
track 1 failed 2 times for a total of 40 seconds (target
8.8.8.8, Description "ping google")
track 2 had no failures (target 10.1.1.1, Description)
track 3 Never been UP (target 10.2.1.1, Description)
track 4 failed 5 times for a total of 70 seconds (target
8.8.4.4, Description "google 2")
```

- To display failures (when and duration) for a specified track and optionally, in last x hours (1-72):

```
show data track <track ID> history failures [<last x hours>]
```

Example:

```
# show data track 2 history failures 72
Failed at 01-01-2003@05:16:23 for 1 second
Failed at 01-01-2003@15:29:59 for 1 second
Failed at 01-01-2003@22:58:39 for 1 second
Failed at 01-02-2003@00:09:20 for 1 second
```

**Applicable Products:** All.

### 2.14.1.8 Cryptographic Algorithms for AH with the SHA-256

The device now supports Authentication Header (AH) with SHA-256 algorithm:

```
(config-data)# crypto ipsec transform-set <name> ah-sha256-hmac
```

**Applicable Products:** All.

### 2.14.1.9 MAC and Serial Number Placeholders for Device's Hostname

When configuring the device with a hostname, the hostname value can include placeholders for the device's MAC address and serial number. These placeholders are replaced by the actual MAC address and serial number of the device, respectively.

This feature is configured using the following existing CLI command:

```
(config-data)# ip domain localhost <hostname>
```

Where the *hostname* can also include the following placeholders (case-insensitive):

- For MAC address: {mac}
- For serial number: {sn} or {serial number}

For example:

```
(config-data)# ip domain localhost msbr-{mac}
```

will be replaced by "msbr-11:11:11:11:11:11" (if 11:11:11:11:11:11 is the device's MAC)

```
(config-data)# ip domain localhost msbr-{sn}
```

will be replaced by "msbr-1343452" (if 134452 is the device's serial number).

**Applicable Products:** All.

#### 2.14.1.10 Dedicated TCP for SIP Traffic per FXS in Trunk Group

Dedicated TCP for SIP traffic per FXS in a Trunk Group (TrunkGroupSettings\_DedicatedConnectionMode) can now be configured in the Web interface. This is supported by the new Web parameter field 'Dedicated Connection Mode' in the Trunk Group Settings table.

**Applicable Products:** MP-5xx; Mediant 500Li.

#### 2.14.1.11 Overriding Location in ISDN Progress Indicator

The device can now be configured to override the Location value of the ISDN PRI (per trunk or all trunks) in Q.931 messages sent to the Tel side. This is configured by a new parameter called [ProgressIndicatorLocation2ISDN] (configure voip > interface e1-t1|bri > pi-location-to-isdn).

**Applicable Products:** MP-5xx; Mediant 500Li.

#### 2.14.1.12 FXS Polarity Reversal per NTT Japan

The device can now be configured to comply with the NTT Japan standard for line polarity reversal for IP-to-Tel calls (FXS).

This is enabled by the new parameter [FXSNTTPolarityReversal].

**Note:** When this feature is enabled, the existing [EnableReversePolarity] and [TimeBeforeReorderTone] parameters are ignored for IP-to-Tel calls.

**Applicable Products:** All.

#### 2.14.1.13 FQDN for Primary CDR Syslog Server

The primary syslog server to where CDRs are sent can now be configured with an FQDN address.

The feature affects the [CDRSyslogServerIP] parameter.

**Applicable Products:** All.

#### 2.14.1.14 Interworking No-ID Cause for IP-to-Tel (FXS) Calls

The device can now be enabled to map a no-id cause value from IP (SIP From header) to FXS for IP-to-Tel calls. For anonymous calls, the device maps the following no-id causes (instead of caller ID) from SIP to the Tel side:

SIP Display Name (Anonymous) in From Header	FXS No-ID Value
"Unavailable"	"O"
"Anonymous"	"P"
"Interaction with other service"	"S"

SIP Display Name (Anonymous) in From Header	FXS No-ID Value
"Coin line/payphone"	"C"

The device sends "O", "P", "S", or "C" to the FXS side according to the cause from the SIP side. This allows the phones to know the reason of the no-id and display the reason on the phone's LCD.

Below shows an example of a From header with a cause (mapped to the Tel side as "C"):

```
From: "Coin line/payphone" <sip:anonymous@anonymous.invalid;pstn-params=9082828088>;tag=gK09696b03
```

This feature is configured using a new parameter called [FxsNttNoldInterworkingMode].

**Note:** For this feature to be functional, the [EnableCallerID] parameter must be enabled (1).

**Applicable Products:** All.

### 2.14.1.15 Device Resets via CLI Blocked for Emergency Calls

The device can now be configured to block device resets triggered through CLI (`reload` command) during emergency calls (IP-to-Tel or Tel-to-IP) and for a user-defined period after the call ends (after successfully being established) or after it failed (e.g., SIP 403). The timeout is configured by a new parameter called [ReloadTimeoutForEmergencyCall] (`configure voip > sip-definition settings > reload-timeout-for-emergency-call`).

This feature also introduces a new way in which the device identifies IP-to-Tel calls as emergency calls. If the device receives a SIP message containing an Alert-Info header whose value is the same as that configured by the new parameter [EmergencyCallAlertInfoUri], then the call is considered an emergency call. If not configured, then the call is not considered an emergency call (even if the header is present).

(For Tel-to-IP calls, calls are considered emergency calls if their dialed numbers are the same as that configured by the existing [EmergencyNumbers] parameter.)

**Applicable Products:** All.

### 2.14.1.16 Attempted Calls Performance Monitoring

For the attempted calls (IP-to-Tel and Tel-to-IP) performance monitoring, the part of the call (start or terminated) that must be included in the count can now be configured. This is done using the new AttemptedCallCountOnStart parameter.

**Applicable Products:** All.

### 2.14.1.17 OVOC-based Management when behind NAT through WebSocket Tunnel



To check on which cloud platforms WebSocket is supported, refer to the [OVOC documentation](#).

When the device is located behind NAT, it can now be managed by OVOC when deployed in a public cloud, by implementing WebSocket tunneling (over HTTP/S). In this tunneling application, the device is a WebSocket client and OVOC is the WebSocket server.

WebSocket tunneling has many advantages over the alternative method used up until now for connecting OVOC to the device when located behind NAT. The main advantage is that it easily resolves NAT traversal problems and requires less configuration (no need for port forwarding and no need for firewall settings to allow certain traffic).

The WebSocket tunnel connection is secure (HTTPS). When the device initiates a WebSocket tunnel connection, it verifies that the TLS certificate presented by OVOC is signed by one of the CAs in the trusted root store of its default TLS Context (ID #0). The device authenticates itself with OVOC using username-password credentials, which must be the same as configured on OVOC.

This feature is configured on the device in the existing Web Service Settings page, using the following new parameters:

- 'OVOC WebSocket Tunnel Server Address' / WSTunServer / configure network > ovoc-tunnel-settings > address: Defines the OVOC WebSocket tunnel server's IP address or hostname.
- 'Path' / WSTunServerPath / configure network > ovoc-tunnel-settings > path: Defines the OVOC WebSocket tunnel server's path.
- 'Username' / WSTunUsername / configure network > ovoc-tunnel-settings > username: Defines the username for connecting to the OVOC WebSocket tunnel server.
- 'Password' / WSTunPassword / configure network > ovoc-tunnel-settings > password: Defines the password for connecting to the OVOC WebSocket tunnel server.
- 'Secured (HTTPS)' / WSTunSecured / configure network > ovoc-tunnel-settings > secured: Enables (default) secure (HTTPS) WebSocket connection.
- 'Verify Certificate' / WSTunVerifyPeer / configure network > ovoc-tunnel-settings > verify-server: Enables (default) certificate verification from WebSocket tunnel server.
- 'Interface': Defines the local network interface for WebSocket communication.

**Applicable Application:** All.

**Applicable Products:** All.

## 2.14.2 Resolved Constraints

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

**Table 23: Resolved Constraints for Version 7.26A.356.074 / 7.26A.356.075**

Incident	Description
MSBR-15884	A/VDSL interface 0/1 is missing after upgrading to 7.26A.356.070. <b>Applicable Products:</b> Mediant 800B
MSBR-15702	Analog devices audit task. <b>Applicable Products:</b> Mediant 500Li
MSBR-13137	Device software upgrade via OVOC fails due to incorrect SNMP EngineID. <b>Applicable Products:</b> All
MSBR-13566	When configured as a VDSL modem, DHCP reply isn't displayed. <b>Applicable Products:</b> Mediant 500Li
MSBR-13957	When connected with a DSL bridge, the IP address is not received from the DHCP server. <b>Applicable Products:</b> Mediant 500Li
MSBR-14079	The device crashes with VRRP activated on the WAN sub-interface. <b>Applicable Products:</b> All
MSBR-14256	CPU utilization reaches 100% even though low traffic and VRRP enabled. <b>Applicable Products:</b> All
MSBR-14801	Fiber interface goes down after software upgrade. <b>Applicable Products:</b> All

Incident	Description
MSBR-14879	Low bandwidth performance in VRRP setups. <b>Applicable Products:</b> Mediant 500C
MSBR-14912	SIP register accounts need to be done manually after a device reset. <b>Applicable Products:</b> Mediant 500Li
MSBR-14955	In some cases, SIP responses received from the WAN aren't routed toward the LAN. <b>Applicable Products:</b> Mediant 500Li
MSBR-14969	CRP configuration is not reflected in Web interface, and IP Groups and IP-to-IP Routing rules can't be configured. <b>Applicable Products:</b> All
MSBR-14988	Trunk Group table display "Your access level does not allow you to view this page" even though current access level (Admin) allows read-write. <b>Applicable Products:</b> Mediant 500Li
MSBR-15060	The device doesn't support fixed full-duplex interface when the Link Partner is also configured with 100 full duplex (interface behave as if down). <b>Applicable Products:</b> Mediant 500Li
MSBR-15106	When adding G.722 codec in the CLI, the Web interface's Coder Groups table doesn't display the 'Rate' field value. <b>Applicable Products:</b> Mediant 500Li 8 FXS
MSBR-15108	When adding G.722 codec in the Web or CLI, the Web interface's Coder Groups table doesn't display the 'Rate' and 'Payload' field values. <b>Applicable Products:</b> Mediant 500Li 8 FXS
MSBR-15113	Sometimes syslog with IPv6 doesn't function properly. <b>Applicable Products:</b> All
MSBR-15115	Incorrect BRI status is displayed on the Web interface's Monitor View page. <b>Applicable Products:</b> All
MSBR-15125	SSH disconnects when uploading a CLI file. <b>Applicable Products:</b> All
MSBR-15135	On the Web interface's Monitor View page, the wrong SFP port icon is displayed green when DSL is connected. <b>Applicable Products:</b> All
MSBR-15139	Handling vulnerability CVE-2011-3188. <b>Applicable Products:</b> All
MSBR-15140	The Web interface doesn't display the D-channel as active. <b>Applicable Products:</b> Mediant 500
MSBR-15141	The device rejects WebRTC calls. <b>Applicable Products:</b> Mediant 500Li
MSBR-15166	The device's hostname (even if configured) doesn't appear in DHCP requests. <b>Applicable Products:</b> All
MSBR-15168	In some cases, the cellular interface doesn't go down when the IP address is released by the service provider. <b>Applicable Products:</b> Mediant 500Li

Incident	Description
MSBR-15173	Issue experienced with NAT. <b>Applicable Products:</b> Mediant 500Li
MSBR-15188	When configured as a bridge, DHCP reply isn't displayed. <b>Applicable Products:</b> All
MSBR-15257	SNMP discrepancies in counters for calls from Gateway application to SBC application. <b>Applicable Products:</b> All
MSBR-15399	The 'User Security Mode' parameter also (erroneously) applies to IP Groups of type Gateway. <b>Applicable Products:</b> All
MSBR-15400	Sometimes no DHCP communication to client and no traffic over transparent bridge. <b>Applicable Products:</b> All
MSBR-15404	SFP-GE-T doesn't function when set as duplex/speed auto mode. <b>Applicable Products:</b> All
MSBR-15407	Wi-Fi security mac mode command fails. <b>Applicable Products:</b> Mediant 500Li
MSBR-15409	Identical crypto map exists on different PPPoE isn't functioning (show sys tec causing reboot). <b>Applicable Products:</b> All
MSBR-15419	The device fails upon disabling call forwarding. <b>Applicable Products:</b> Mediant 500Li
MSBR-15423	In specific cases, the device fails frequently. <b>Applicable Products:</b> Mediant 500Li
MSBR-15424	The show data qos queue command has a display problem. <b>Applicable Products:</b> All
MSBR-15431	The device can't allocate media channels for SBC calls. <b>Applicable Products:</b> Mediant 500Li
MSBR-15447	High CPU utilization is observed. <b>Applicable Products:</b> Mediant 500Li
MSBR-15456	Wi-Fi goes down and up after Wi-Fi password configured. <b>Applicable Products:</b> Mediant 500Li
MSBR-15505	403 Forbidden Page is displayed when access to the device from an IP address not in Management Access List. <b>Applicable Products:</b> All
MSBR-15510	After a session timeout, the cellular interface sometimes doesn't go back up. <b>Applicable Products:</b> Mediant 500Li
MSBR-15518	Sudden loss of connection with the device occurs. <b>Applicable Products:</b> Mediant 800
MSBR-15575	The device fails to comply with some IPv tests (VerifyReceivedRequestUri). <b>Applicable Products:</b> All

Incident	Description
MSBR-15577	The device sometimes fails. <b>Applicable Products:</b> Mediant 500Li
MSBR-15600	Timeouts experienced for Web interface session when accessed from WAN. <b>Applicable Products:</b> All
MSBR-15622	When a Proxy Set is configured with multiple A-records and a SIP 408 response is received for the sent REGISTER, alternative routing to the next IP address in the SRV (as configured by <code>alternative-routing-reason tel2ip</code> ) doesn't work. <b>Applicable Products:</b> All
MSBR-15634	SNMP problem with counters experienced with ADSL/VDSL interface. <b>Applicable Products:</b> All
MSBR-15639	After configuring a TLS Context, the Web interface disconnects when the <b>Save</b> button is clicked. <b>Applicable Products:</b> All
MSBR-15643	nslookup for SRV/NAPTR doesn't function when using VRFs. <b>Applicable Products:</b> All
MSBR-15659	Autorun causes error messages (related to command <code>mac auto</code> ). <b>Applicable Products:</b> Mediant 500Li
MSBR-15664	The device is no longer manageable over HTTPS. <b>Applicable Products:</b> All
MSBR-15679	RTCP isn't forwarded after a change in the SSRC, causing calls to be dropped from Microsoft Teams. <b>Applicable Products:</b> All

## 2.15 Version 7.24A.356.914

This version includes new features and resolved constraints only.



- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.15.1 New Features

This section describes the new features introduced in this version.

#### 2.15.1.1 Description for Cellular Interface

A description can now be configured for a cellular interface. This is supported by the new CLI command `desc`, which is entered under the cellular interface mode, as shown in the following example:

```
(config-data)# interface cellular 0/0
(conf-cellular-0/0)# desc MyExample
```

**Applicable Products:** Mediant 500Li; Mediant 800Ci.

#### 2.15.1.2 SIM Card Unlocking and PIN Code Enhancements

The following procedures can now be performed on SIM cards:

- Changing PIN code of an already locked SIM card.
- Defining new PIN code for a SIM card locked by the Personal Unlocking Key (PUK) code (due to three wrong PIN code attempts). The PIN code is reset (unlocked) with the PUK code (located on the printed label) and the new PIN code can then be defined.

This feature introduces the following new CLI commands under the new advanced mode:

```
(config-data) # interface cellular 0/0
(conf-cellular-0/0)# adv
(adv-cell-config)#
sim_lock_status      / Displays SIM lock status
sim_pin_code_change  / Changes SIM PIN code
sim_pin_code_unlock  / Unlocks locked SIM using PIN code
sim_puk_code_unlock  / Unlocks locked SIM by PUK code and defines
new PIN code
```

**Applicable Products:** Mediant 500Li; Mediant 800Ci.

#### 2.15.1.3 Weighted Fair Queuing in Bytes or Percentage

Weighted Fair Queuing (WFQ) can now be displayed in bytes or percentage (in addition to weight, which was already supported).

This feature is supported by the new `wfq_mode` CLI command:

```
(config-data)# qos service-map GigabitEthernet 0/0 output
```

```
(conf-s-map) # wfq_mode
bytes           Set to bytes mode
percent        Set to percent mode
weight         Set to weight mode
```

**Applicable Products:** Mediant 500Li; Mediant 800Ci.

#### 2.15.1.4 Disable Authentication Failure SNMP Trap Now Configurable

The device can now be configured to disable the Authentication Failure SNMP trap (authenticationFailure, OID 1.3.6.1.6.3.1.1.5.5) so that it's never sent. This is done using the new parameter EnableSnmpAuthenticationTrap (configure system > snmp settings > enable-authentication-trap). By default, the trap is enabled.

**Applicable Products:** Mediant 500Li; Mediant 800Ci.

#### 2.15.1.5 Flow Control of Physical Ports

The device now supports a flow control mechanism to prevent buffer congestion and packet drop switch.

In full duplex operation, the sender is notified to start or stop the transmission via a PAUSE frame, based on IEEE 802.3x standard. The Gigabit Ethernet switch can transmit/receive and react accordingly to 802.3x flow control frames. Flow control can be enabled or disabled per port.

New commands:

- `flowcontrol auto`: Flow control auto mode.
- `flowcontrol off`: Disables the interface to receive and send pause frames.
- `flowcontrol rx`: Enables the interface to receive and process pause frames.
- `flowcontrol rxtx`: Enables the interface to send and receive pause frames.
- `flowcontrol tx`: Enables the interface to send pause frames to remote devices.

Supported interfaces: Gigabitethernet (0/0, 1/1, 1/2, 1/3, 1/4) and fiber 0/0.

Default values: All interfaces, except Fiber 0/1 by default are configured with `flowcontrol auto` mode. Fiber 0/1 is configured with `flowcontrol rxtx`.

**Applicable Products:** Mediant 500Li; Mediant 800Ci.

### 2.15.2 Resolved Constraints

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

**Table 24: Resolved Constraints for Version 7.24A.356.914**

Incident	Description
MSBR-14818	Tab key for CLI command auto-completion functionality for BGP configuration doesn't function as expected. <b>Applicable Products:</b> Mediant 500Li
MSBR-15063	Unlocking SIM PIN code is available only after a device reset. <b>Applicable Products:</b> Mediant 500Li
MSBR-15337	Sometimes cellular SIM card reporting that it's missing ("ABSENT") after reconfiguration. <b>Applicable Products:</b> Mediant 500Li

## 2.16 Versions 7.24A.356.854 / 7.24A.356.867

This version includes new features and resolved constraints only.



- **Version 7.24A.356.867** is applicable only to Mediant 500Li and Mediant 800Ci.
- **Version 7.24A.356.854** is applicable only to Mediant 500, Mediant 500C, Mediant 500L, and Mediant 800B/C MSBRs.
- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.16.1 New Features

This section describes the new features introduced in this version.

#### 2.16.1.1 Serial Darkening for Mediant 500Li

The device now supports serial darkening, which is enabled by default. Serial darkening hides the log messages (bootup processes) from being displayed in the CLI console during a device reset (boot up). However, if the device fails to load, serial darkening is disabled in the next bootup attempt.

This feature is configured by the CLI command `configure troubleshoot > startup-n-recovery > startup-dark-mode` (EnableDarkenMode ini file parameter).

(This feature is already supported in the other MSBR products not mentioned below.)

**Applicable Products:** Mediant 500Li.

#### 2.16.1.2 MAC Address Prefix Configuration

The device provides a pool of eight MAC addresses whose prefix can be automatically generated (02:90:8f:XX:XX:XX to 02:97:8f:XX:XX:XX) or manually configured. The suffix (XX:XX:XX) of the MAC addresses is obtained from the underlying interface. These MAC addresses can be assigned to the device's interfaces (e.g., giga 0/0), which can then be used as underlying interfaces for PPP interfaces (e.g., ppp0). In other words, a specific MAC address can be used for a specific PPP interface.

This feature is configured by the following new CLI commands:

- To configure if prefix of the MAC addresses in the pool are automatically or manually set:
 

```
(config-data)# admin-global-mac
```
- To associate a MAC address from the pool with an underlying interface:
 

```
(conf-if-<interface>)# mac auto
```
- To view the pool of MAC addresses (free and used):
 

```
show global-mac-table
```

**Applicable Products:** Mediant 500Li.

#### 2.16.1.3 IEEE 802.1x as Client (Supplicant)

The Mediant 500Li now supports 802.1x as a client (supplicant) - the authenticated device. Up until now, it supported 802.1x only as an authenticator. (This feature is already supported by Mediant 500; Mediant 500L; Mediant 800 MSBRs.)

To configure this new feature, the following new CLI commands were added under `configure data > dot1x supplicant`:

- `identity` – Supplicant's identity string
- `mode (disable/md5/peap/tls)`
- `password / obscured-password` – Supplicant's password string
- `port-type` – Supplicant's port type to run on
- `tls-ctx` – Supplicant's TLS Context index

Once you configure above (and `exit`), configuration is loaded and negotiation with the authenticator (e.g., secure LAN switch) using Extensible Authentication Protocol (EAP) begins. If the supplicant's credentials are valid, the Authenticator authorizes traffic on the secure port connected with the device.

You can view the configuration under `show running-config data` and also the status of the negotiation using `show data dot1x-supplicant-status`.

**Applicable Products:** Mediant 500Li.

#### 2.16.1.4 Default Gateway via DHCP as Default Route for VRF

The device can now be configured to use the Default Gateway received through DHCP as the default route for a specific VRF.

```
ip dhcp-client default-route vrf <VRF name or "main-vrf">
```

This CLI command is used when the interface is configured to obtain an IP address through DHCP.

**Applicable Products:** Mediant 500; Mediant 800.

#### 2.16.1.5 AES-GCM Cryptographic Algorithms for ESP Transform Sets

The device now supports the following algorithms for ESP transform using Galois Counter Mode (GCM) cipher:

- `esp-gcm 128`: 128-bit key AES-GCM with 128-bit ICV
- `esp-gcm 192`: 192-bit key AES-GCM with 128-bit ICV
- `esp-gcm 256`: 256-bit key AES-GCM with 128-bit ICV

```
(config-data)# crypto ipsec transform-set <name> esp-gcm  
[128|192|256]
```

**Applicable Products:** All.

#### 2.16.1.6 Configuration Backup by OVOC when Using Hostname

The device now supports configuration backup by OVOC when OVOC defines itself as an FQDN (hostname). In this scenario, the device uses a DNS server to resolve OVOC's hostname into an IP address and then sends the configuration backup file to this IP address (IPv4 or IPv6).

**Applicable Products:** All.

#### 2.16.1.7 New SNMP Alarm for No DNS Reply

The new SNMP alarm `acNoReplyFromDNSServerAlarm` has been added, which is raised when the device sends a DNS query, and the DNS server doesn't reply. DNS queries are sent for Proxy Sets configured with FQDNs.

**Applicable Products:** All.

### 2.16.1.8 SNMP MIBs for Call Attempts per Second Monitoring

The device now provides performance monitoring for call attempts per second. This is provided in the new performance monitoring MIBs, acSBCCallAttemptsPerSecTable and acPMCPCallAttemptsPerSecTable for SBC and Gateway calls, respectively.

Low and high thresholds can be configured, using the following MIBs:

- SBC:
  - acPMSbcCallAttemptsPerSecHighThreshold
  - acPMSbcCallAttemptsPerSecLowThreshold
- Gateway:
  - acPMCPConnectionAttributesCallAttemptsPerSecHighThreshold
  - acPMCPConnectionAttributesCallAttemptsPerSecLowThreshold

If the high threshold is reached or exceeded, the device sends the existing alarm acPerformanceMonitoringThresholdCrossing (if enabled by the existing parameter PM\_EnableThresholdAlarms). The alarm is cleared if the value goes below the low threshold.

**Applicable Products:** All.

### 2.16.1.9 Increased Characters Support for 'tag' in SIP To/From Headers

The maximum number of supported characters of the 'tag' parameter in the SIP To and From headers has been increased from 99 to 150.

**Applicable Products:** All.

### 2.16.1.10 FQDN for CDR Syslog Server

The address of the Syslog server for CDRs can now be configured as an FQDN.

**Applicable Products:** All.

### 2.16.1.11 CLI Error Messages Displays Valid Range

For CLI commands whose value can be any integer within a specific range of numbers, if the user inputs a number that is outside of the range, the CLI's error message now shows the valid range, as shown in the following example.:

```
(cli-settings)# window-height 70000
Invalid argument "70000". Value must be in range [0-65535]
```

**Applicable Products:** All.

### 2.16.1.12 Device UP Time Added to Debug File

The duration (in seconds) that the device was operational (up time) before it underwent a reset is now shown in the downloaded debug file (reset-table-of-content.txt) as well as in the output of the CLI command show debug-file reset-info, for example:

```
# show debug-file reset-info list
** Current Reset Counter [155] **

***** Reset *****
Reset Counter:154
Up Time (seconds): 3844
Reset Reason: CLI Reset
```

```

Reset Time: 8.1.2021 18.1.21
SwVersion: 724A-356-833
*****

```

**Applicable Products:** All.

## 2.16.2 Resolved Constraints

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

**Table 25: Resolved Constraints for Version 7.24A.356.854 & 7.24A.356.867**

Incident	Description
MSBR-12760	IPV6CP Identifier (RFC 5072) isn't modified with EUI-64 and is changed after each PPP reconnect. <b>Applicable Products:</b> Mediant 500L MSBR
MSBR-12761	The device erroneously sends an NS message for duplicate address detection (DAD) to the WAN. <b>Applicable Products:</b> Mediant 500L MSBR
MSBR-12762	The device takes too long in sending IPV6 router solicitation messages after an IPV6CP session starts successfully. <b>Applicable Products:</b> Mediant 800 MSBR
MSBR-13361	The device doesn't set the IP fragment flag correctly. <b>Applicable Products:</b> All
MSBR-13623	The device sends unsolicited RA messages to LAN too often. <b>Applicable Products:</b> Mediant 500L MSBR
MSBR-14017	The device sends a SIP REGISTER from its internal IP address (instead of WAN address). <b>Applicable Products:</b> All
MSBR-14101 MSBR-14198	No HTTPS access to the device after updating to Ver. 7.24A.356.508. <b>Applicable Products:</b> All
MSBR-14178	The device sends its hostname instead of the SNMP Version type (SNMPv3) to OVOC. As a result, OVOC continues communicating with the device using SNMPv2. <b>Applicable Products:</b> All
MSBR-14198	No HTTPS access to the device after updating to 7.24A.356.508 with customer ini. <b>Applicable Products:</b> All
MSBR-14276	The device sometimes resets when in VRRP configuration (VRRP backup Router). <b>Applicable Products:</b> Mediant 500 MSBR
MSBR-14307	SIP Session Timer behavior when both IP Profiles are configured to transparent doesn't function as expected. <b>Applicable Products:</b> All
MSBR-14312	The device doesn't forward media for Tel-to-IP, causing one-way voice. <b>Applicable Products:</b> Mediant 800 MSBR
MSBR-14329	Call forward no answer deactivation (CFNA) feature doesn't function. <b>Applicable Products:</b> Mediant 500L MSBR

Incident	Description
MSBR-14381	Configuration of the NQM feature fails. <b>Applicable Products:</b> Mediant 500 MSBR
MSBR-14487	IPv6 Prefix delegation no longer functions. <b>Applicable Products:</b> Mediant 500 MSBR
MSBR-14542	PI=8 (Progress Indicator) isn't sent in the ISDN DISCONNECT message. <b>Applicable Products:</b> All
MSBR-14581	VRRP setup doesn't function after upgrading to Ver. 7.24A.356.248. <b>Applicable Products:</b> Mediant 800 MSBR
MSBR-14861	The CLI command echo-canceller-nlp-mode doesn't appear in the CLI ((config-voip)# media voice-processing). <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-13633	Even though DSCP and ToS is configured (QoS mapping), no ToS bits are set on the VLAN in outbound packets. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14795	When configuring the gig 0/0 interface to speed 1000 and full-duplex mode, the interface goes down. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14758	The CLI and Web interface freeze after a while. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14544	NAT settings on SIP Interfaces doesn't function. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14533	A SIP REGISTER message from the Account table is not sent after a device reset. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14404	Autorun of the CLI command copy cli-script aborts. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14577	BFD configuration settings are not displayed in the CLI. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14575	The link-state monitor status is not displayed in CLI. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14572	Device fails to load an incremental INI file when the IniFileURL parameter is configured with an FQDN. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14494	The device resets due to the External Application Exception "Force system crash due to HW Watchdog" because watchdog process is stuck. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-13567	Noise heard during a gateway consultation call. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14351	The device resets when user attempts to add a new TLS Context. <b>Applicable Products:</b> Mediant 500Li MSBR

Incident	Description
MSBR-13917	No ADSL/VDSL connection with a BRAS after upgrading from Ver. 7.20AN.456.678 to 7.24A.356.481 / 7.24A.356.508. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14693	The fiber port interface is not displayed on the Web interface's Monitor page. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14816	When using DHCP, the track interface bounces on NTP update with a time change. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14740	The device crashes (resets) with a "sw hardware watchdog reset" reason. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14808	Versatel SIM card is not registering. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14862	Row index #1 of SIP Interface and Media Realm are not configured correctly when loading a CLI file. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14863	When executing the "Show QoS queue" command, sometimes too many sent bytes are displayed. <b>Applicable Products:</b> Mediant 500Li MSBR
MSBR-14878	LTE reception shows RSSI values instead of RSRP. <b>Applicable Products:</b> Mediant 500Li MSBR

## 2.17 Versions 7.24A.356.706 / 7.24A.356.747

This version includes new features and resolved constraints only.



- **Version 7.24A.356.747** is applicable only to Mediant 500Li MSBR;
- **Version 7.24A.356.706** is applicable to Mediant 500 MSBR, Mediant 500C MSBR, Mediant 500L MSBR, and Mediant 800B/C MSBR.
- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.17.1 New Features

This section describes the new features introduced in this version.

#### 2.17.1.1 Increase in Multiple Traffic Selectors per IPSec Tunnel

The maximum number of traffic selectors per IPSec tunnel has been increased from 10 to 16.

**Applicable Products:** All.

#### 2.17.1.2 Configuration Tables for Binding SSH and Telnet Applications

Binding network interfaces (e.g., VRFs) to SSH and Telnet applications are now configured using tables:

- Telnet Interfaces table - configure system > cli-settings > telnet-if [TelnetInterfaces]
- SSH Interfaces table - configure system > cli-settings > ssh-if [SshInterfaces]

These tables can be bind using IPv4 and IPv6 networks. Each table can be configured with up to 16 entries (rows).

These tables replace the following (now obsolete) parameters: TelnetIPv4Interface, TelnetIPv6Interface, TelnetServerPort, SSHIPv4Interface, SSHIPv6Interface, SSHServerPort.

**Applicable Products:** Mediant 500Li.

#### 2.17.1.3 Binding SNMP Application to IPv6 Interface

The SNMP application can now be binded to an IPv6 interface. This feature is supported by the following new parameters in the SNMP Community Strings page:

- 'IPv4 Interface Name' - configure system > snmp settings > snmp-server-interface > ipv4-snmpp-network-source [SNMPInterface\_InterfaceName]
- 'IPv6 Interface Name' - configure system > snmp settings > snmp-server-interface-ipv6 > ipv6-snmpp-network-source [SNMPIPv6Interface\_InterfaceName]

**Applicable Products:** Mediant 500Li.

### 2.17.1.4 AES-GCM Cryptographic Algorithm Support for IKEv2

The device now supports Advanced Encryption Standard with Galois Counter Mode (AES-GCM) for authenticated encryption (128- and 256-bit secret keys with 16-byte ICV) for IKEv2 only.

```
(config-data)# crypto isakmp policy x
(config-isakmp)# encryption aes-gcm {128|256}
```

**Applicable Products:** All.

### 2.17.1.5 PRF Cryptographic Algorithm Support for IKEv2

The device now supports pseudo-random function (PRF) as the algorithm to derive keying material and hashing operations for the IKEv2 tunnel encryption. The hash algorithms for PRF can be configured to 256-bit SHA, 384-bit SHA or 512-bit SHA (HMAC variant).

```
(config-data)# crypto isakmp policy x
(config-isakmp)# prf {sha256|sha384|sha512}
```

**Applicable Products:** All.

### 2.17.1.6 Diffie-Hellman Groups 19, 20 and 21 Support

The device now also supports Diffie-Hellman (DH) group identifiers 19, 20 and 21 for IKE.

```
(config-data)# crypto isakmp policy x
(config-isakmp)# group {1|14|15|16|19|2|20|21|5}
```

**Applicable Products:** All.

### 2.17.1.7 FQDN for TACAS Server Address

The TACACS+ server can now be configured as an FQDN (in addition to the already supported IP address). Configuration is done by the existing CLI command:

```
tacacs-server host <IP address or FQDN>
```

**Applicable Products:** All.

### 2.17.1.8 Acceptance of Any Remote ID from IPSec Peer

During IPSec tunnel negotiation, the device can accept any remote-id presented by the peer to connect. This is configured by the following new option `use-remote-id-any`:

```
(config-data)# crypto isakmp policy x
(config-isakmp) use-remote-id-any
```

**Applicable Products:** All.

### 2.17.1.9 Global Configuration of Syslog Severity Level

The syslog severity level can now be configured globally, using the `[SyslogLogLevel]` ini file parameter. In addition, for this parameter and for the existing 'Severity Level' parameter in the Syslog Servers table, the optional values **Debug** and **Info** have been renamed **Debug [not recommended]** and **Info [not recommended]** to indicate that setting the severity level to any of these values may cause excessive use of device resources.

**Applicable Products:** All.

### 2.17.1.10 FQDN for Syslog Server Address

The Syslog server's address can now be configured as an FQDN, allowing the device to do DNS resolution with a DNS server to obtain the IP address (IPv4 or IPv6).

The feature affects the following parameters: [SyslogServerIP] (global) and [SyslogServers\_Address] (Syslog Servers table).

To enable DNS-resolution for IPv6, a new parameter was introduced called [SyslogIPv6Enable] (configure troubleshoot > syslog > ipv6-enable).

**Applicable Products:** All.

### 2.17.1.11 Stop Proxy Server Retry upon ICMP Error

When using UDP as the transport protocol, the device retries the proxy server upon failed transmissions, according to the [ProxySet\_FailureDetectionRetransmissions] parameter. However, when the failed attempt receives an ICMP error (which indicates Host Unreachable or Network Unreachable) as opposed to a timeout, it may be desirable to abandon additional retries in favor of trying the next IP address (proxy server) in the Proxy Set. This is often desirable when Proxy Hot Swap is enabled.

**Applicable Products:** All.

### 2.17.1.12 Transcoding between G.711 and G.722 Voice Coders

The device now supports transcoding of voice streams between SIP user agents using G.711 and G.722 coders (64 kbit/s rate only).

**Applicable Products:** Mediant 500Li.

### 2.17.1.13 Enforcement of DNS Information over DHCPv6

The device can now be configured to enforce the receipt of DNS information over DHCPv6. As the DHCPv6 Solicit/Request includes Option 23 (DNS), the device retries the Solicit if the DHCPv6 Advertise/Reply does not include a response for Option 23. This is enabled by the new CLI command `option force-dns`:

```
ipv6 dhcp-client force-dns
```

**Applicable Products:** All.

## 2.17.2 Resolved Constraints

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

**Table 26: Resolved Constraints for Version 7.24A.356.706 & 7.24A.356.747**

Incident	Description
MSBR-12444	The device crashes with the error message "External Application Exception". <b>Applicable Products:</b> Mediant 500Li
MSBR-12838	The Web interface doesn't show the 'Log Severity Level' (SyslogLogLevel) parameter. <b>Applicable Products:</b> Mediant 500
MSBR-12939	DHCPv6 request retries are incomplete. <b>Applicable Products:</b> All
MSBR-13195	Error messages for the new software version is generated after the device is upgraded. <b>Applicable Products:</b> Mediant 500Li

Incident	Description
MSBR-13202	The device has an IPv6 renewal issue. <b>Applicable Products:</b> Mediant 500Li
MSBR-13293	Insufficient memory to save configuration due to file system full. <b>Applicable Products:</b> Mediant 500L
MSBR-13312	Configuring PPPoE to an IPv6 address autoconfig causes a device reboot. <b>Applicable Products:</b> All
MSBR-13315	Password is missing in run config. <b>Applicable Products:</b> All
MSBR-13330	The RFC2833RxPayloadType and RFC2833TxPayloadType parameters are hidden in CLI. <b>Applicable Products:</b> All
MSBR-13343	Configuring PPPoE to IPv6 address autoconfig reports the incorrect interface (internal address) if no IP address is received. <b>Applicable Products:</b> All
MSBR-13361	The device doesn't set the IP fragment flag correctly. <b>Applicable Products:</b> Mediant 800C
MSBR-13468	NTP host name resolution sends A-type query in DNS instead of AAAA-type. <b>Applicable Products:</b> All
MSBR-13475	The Web server is not accessible when assigning multiple interfaces (VRFs). <b>Applicable Products:</b> Mediant 800C
MSBR-13503	The device is unstable and often reboots. <b>Applicable Products:</b> Mediant 500Li
MSBR-13504	The device reboots when the video stream starts. <b>Applicable Products:</b> Mediant 500Li
MSBR-13505	Low cellular signal strength. <b>Applicable Products:</b> Mediant 800C
MSBR-13506	Software downloads through TR-069 is not functioning (modifying URL). <b>Applicable Products:</b> All
MSBR-13521	The device drops NOTIFY messages containing XML with a big MTU size. <b>Applicable Products:</b> Mediant 500L
MSBR-13593	DNS resolution for the NTP server's FQDN doesn't function. <b>Applicable Products:</b> All
MSBR-13726	The Web interface doesn't display the status of the GE port LED on the Monitor page, even though the link is up. <b>Applicable Products:</b> All
MSBR-13733	The device rejects certain incoming calls, <b>Applicable Products:</b> All
MSBR-13742	The device increments the Session Version in SDP 'o' line upon a session refresh (re-INVITE). <b>Applicable Products:</b> All

Incident	Description
MSBR-13821	Device randomly resets due to a Linux Signal. <b>Applicable Products:</b> Mediant 500L
MSBR-13897	The command <code>ip tcp adjust-mss</code> is missing under interface PPPoE. <b>Applicable Products:</b> All
MSBR-13911	Even though the cellular interface (LTE) functions ok, L2TP doesn't function sometimes. <b>Applicable Products:</b> All
MSBR-13966	The DataInterfaceStatus alarm is generated upon a DHCP lease renewal when using Track, <b>Applicable Products:</b> Mediant 500Li
MSBR-14277	FTTH bandwidth is below 1 GB. <b>Applicable Products:</b> Mediant 500Li
MSBR-14441	Multiple phone registration failure when operating in L2TP mode. <b>Applicable Products:</b> Mediant 500Li
MSBR-14635	Upload bandwidth is limited due to dot1p tag issue. <b>Applicable Products:</b> Mediant 500Li

## 2.18 Version 7.24A.356.508

This version includes resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.18.1 Resolved Constraints

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

**Table 27: Resolved Constraints for Version 7.24A.356.508**

Incident	Description
MSBR-10768	The output of the CLI command <code>debug capture data physical</code> shows the incorrect time. <b>Applicable Products:</b> All
MSBR-12303	Sometimes with specific vendors, the IPsec tunnel can't be re-established after being disconnected. <b>Applicable Products:</b> All
MSBR-13437	Upgrade from 7.24A.356.468 to 7.24A.356.481 generates the error message "Process Failed. Failed running execv". <b>Applicable Products:</b> All
MSBR-13566	When the device functions as a VDSL modem, DHCP replies don't pass from LAN to WAN through the bridge group. <b>Applicable Products:</b> Mediant 500Li
MSBR-13574	The cellular interface is removed from configuration after upgrading to Ver. 7.24A.356.481. <b>Applicable Products:</b> All
MSBR-13587	The predefined timer for the Auto-Update mechanism doesn't function when configured through CLI. <b>Applicable Products:</b> All

## 2.19 Version 7.24A.356.481

This version complies with Product Notice #0451, which can be downloaded from AudioCodes website by clicking [here](#).



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.19.1 New Features

This section describes the new features introduced in this version.

#### 2.19.1.1 Proxy Keep-Alive using Fake Register Requests

Proxy keep-alive can now be done by sending fake REGISTER request messages (Contact header contains a fake name). The mode of operation is identical to the method using OPTIONS messages, but with REGISTER messages. This feature is supported by the new optional value **Using Fake REGISTER** for the 'Proxy Keep-Alive' parameter in the Proxy Sets table.

**Applicable Products:** All.

## 2.20 Version 7.24A.356.468

This version includes new features, known constraints and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.20.1 New Features

This section describes the new features introduced in this version.

#### 2.20.1.1 LAN Port Redundancy Groups

The LAN port redundancy feature has been enhanced and can now be configured with more than one group of active-standby LAN ports.

For example:

```
# conf d
(config-data)# interface fastethernet 1/1
(conf-if-FE 1/1)# port-redundancy fastethernet 1/2
```

```
(config-data)# interface fastethernet 1/3
(conf-if-FE 1/3)# port-redundancy fastethernet 1/4

(conf-if-FE 1/4)# do show data port-redundancy
Port Redundancy Status
-----
First Port    FastEthernet 1/1
Second Port   FastEthernet 1/2
Active Port   FastEthernet 1/1

Port Redundancy Status
-----
First Port    FastEthernet 1/3
Second Port   FastEthernet 1/4
Active Port   FastEthernet 1/4
```

**Applicable Products:** All.

### 2.20.1.2 CLI Command Aliases

The device now allows the user to create aliases which are shortcuts in the CLI to shorten commands, Aliases are useful for commands that are frequently used. Aliases are configured in the new configuration table, CLI Aliases (Setup > Administration > Web & CLI > CLI Aliases) - `configure system > cli-settings > cli-alias`.

The alias can be configured for a specific command (`copy`) or for a command sequence (`copy cli-script`). For example, if the alias for the `copy cli-script` command is "copyC", then instead of entering the following in the CLI:

```
# copy cli-script from ...
```

The following can be entered:

```
# copyC from
```

A list of all the configured aliases can be viewed in the CLI, using the new command `show aliases`.

**Applicable Products:** All.

### 2.20.1.3 DNS Address by DHCPv6 Server

When the device is configured as a DHCPv6 server, it can now propagate the DNS server IPv6 address that is learned by the DHCPv6 client running on the WAN. This is configured by the new optional value "auto" for the command `ipv6 dhcp-server dns-server auto`.

In addition, the behavior of the existing `ipv6 dhcp-server dns-server ::` command has been modified –device publishes its own link-local ipv6 address as the DNS server address.

**Applicable Products:** All.

### 2.20.1.4 CLI Display of Bridging Information

The device now displays Ethernet bridging information, using the new CLI command `show data bridge info`. The existing command `show data bridge configuration` displays Ethernet bridging configuration.

**Applicable Products:** All.

### 2.20.1.5 Cached DNS Resolution

For Proxy Sets configured with FQDNs, the device queries the DNS server to resolve FQDNs every user-defined interval (ProxyIPListRefreshTime), which refreshes the Proxy Set's list of DNS-resolved IP addresses. However, up until now, if the DNS server went offline, the device placed the entire Proxy Set offline as well.

This feature now allows the device to cache (store) the last successful DNS resolution and if the DNS server subsequently goes offline when the device needs to do a refresh DNS query, instead of taking the Proxy Set offline, the device reuses the cached DNS-resolved addresses. In this scenario, the device continues attempting to query the DNS server every 10 seconds. Thus, service is not impacted. The device deletes the cached DNS-resolved addresses 30 minutes after the time to live (TTL) value expires (received in the DNS response).

**Applicable Products:** All.

### 2.20.1.6 Display of DNS-Resolved IP Addresses from ACL

A new CLI command, `show data access-lists resolved` displays the DNS-resolved IP addresses of hostnames configured in the Access List (ACL).

For example, for the ACL rule

```
access-list www permit ip host walla.co.il host google.com
```

this command outputs the following:

```
access-list www permit ip host walla.co.il [13.226.6.71  
13.226.6.16 13.226.6.124 13.226.6.20] host google.com  
[172.217.16.142]
```

**Applicable Products:** All.

### 2.20.1.7 Vendor-Specific Sub-options 4-10 (Option 17) for DHCPv6

The device as a DHCP client now supports the Vendor-specific sub-options 4-10 for DHCPv6 requests (Option 17), which provide device identification properties to the DHCP server. (Up until now, the device supported this for DHCPv4 only.)

The sub-options provided the following information:

- Sub-option code 4: Device serial number
- Sub-option code 5: Hardware version
- Sub-option code 6: Software version
- Sub-option code 7: Boot ROM version
- Sub-option code 8: Vendor OUI
- Sub-option code 9: Device model number
- Sub-option code 10: Vendor identifier

The sub-options are configured under the `ipv6 dhcp-client` command:

```
(conf-if-GE 0/0)# ipv6 dhcp-client  
  
opt-17-sub-1 enterprise <number> // Enterprise number for sub-  
option 1 and 4-10; If not set, they are not sent; If set, they are  
sent under the enterprise set.  
  
cable-labs-opt-17 // default on (sub-options 4-10 sent); If set to  
no, sub-options not sent even if above command set.
```

**Applicable Products:** All.

### 2.20.1.8 Increase in Maximum ACL Rules

The number of ACL rules (`configure data > access-list`) that can be assigned to a single ACL has been increased from 50 to 200.

**Applicable Products:** Mediant 500Li.

### 2.20.1.9 Logged Status of TR-069 Scheduled File Download

The device now reports the status of the TR-069 ScheduleDownload to Syslog:

- Received request - "Received ScheduleDownload request. time mode"
- Start download process - "Transfer Scheduler Download started"
- Complete download process (after reset and events sending) - "Transfer Scheduler Download completed"

**Applicable Products:** All.

### 2.20.1.10 Interworking SIP 183 without SDP and ISDN Progress

The device can now be configured to interwork incoming SIP 183 without SDP responses to outgoing Q.931 Progress/Alerting messages for Tel-to-IP calls. This is configured using the new parameter [ISDNSendProgressOn183WithoutSDP].

**Applicable Products:** All.

### 2.20.1.11 IEEE 802.1x as Client (Supplicant)

The device now supports 802.1x as a client (supplicant) - the authenticated device. Up until now, it supported 802.1x only as an authenticator.

To configure this new feature, the following new CLI commands were added under `configure data > dot1x supplicant`:

- `identity` – Supplicant's identity string
- `mode (disable/md5/peap/tls)`
- `password / obscured-password` – Supplicant's password string
- `port-type` – Supplicant's port type to run on
- `tls-ctx` – Supplicant's TLS Context index

Once you configure above (and `exit`), configuration is loaded and negotiation with the authenticator (e.g., secure LAN switch) using Extensible Authentication Protocol (EAP) begins. If the supplicant's credentials are valid, the Authenticator authorizes traffic on the secure port connected with the device.

You can view the configuration under `show running-config data` and also the status of the negotiation using `show data dot1x-supplicant-status`.

**Applicable Products:** Mediant 500; Mediant 500L; Mediant 800.

### 2.20.1.12 Improved Design of Monitor Page

The Monitor page, which displays a graphical design of the device and indicates various statuses using LED icons, has been redesigned. (The re-design was already implemented in Mediant 500Li MSBR).

**Applicable Products:** Mediant 500L; Mediant 800.

### 2.20.1.13 Port Mirroring Configuration through Web

Port Mirroring can now be configured through the Web interface. Up until now, it was only configurable through the CLI. This is supported by the new Port Mirroring page (Troubleshoot menu > Troubleshoot tab > Debug folder > Port Mirroring).

**Applicable Products:** All.

### 2.20.1.14 TR-069 Session Retry Policy Support

The device now fully supports the TR-069 Session Retry Policy. If the TR-069 session between the device (CPE) and ACS fails because of a new event (for example, power outage or routing failure), the device now waits a randomly selected time interval (from a range) before attempting to re-establish the session with the ACS. This time is random to prevent large numbers of CPEs from trying to reconnect to the ACS at the same time.

**Applicable Products:** All.

### 2.20.1.15 LLDP-MED Support

The device now supports LLDP Media Endpoint Discovery (LLDP-MED), which is an extension to LLDP. This protocol is specifically used to support VoIP applications and enables network discovery between network connectivity devices and media endpoints such as, softphones, IP telephones, VoIP gateways and conference bridges.

**Applicable Products:** All.

### 2.20.1.16 FQDN for IPSec Tunnel Peer

The address of the IPSec tunnel peer can now also be configured as an FQDN:

```
(config-crypto-map)# set peer <IP Address or FQDN>
```

Up until now, it could only be configured as an IP address.

**Applicable Products:** All.

### 2.20.1.17 Enhanced Utilization of QoS Resources

The device's QoS functionality has been enhanced to improve utilization of resources for QoS.

In addition, the following new command displays current traffic classification ID (tc assignment):

```
show data qos tc
```

Up until now, it could only be configured as an IP address.

**Applicable Products:** Mediant 500Li.

## 2.20.2 Known Constraints

This section lists known constraints.

**Table 28: Known Constraints in Version 7.24A.356.468**

Incident	Description
MSBR-11086	RADIUS servers can't be configured with IPv6 addresses. <b>Applicable Products:</b> Mediant 500Li
MSBR-12250	QoE is not supported through VLAN interfaces or VRFs. <b>Applicable Products:</b> All

Incident	Description
MSBR-12629	The <code>automatic-update</code> and <code>copy</code> commands via SCP and bonded to source VRF, fails. <b>Applicable Products:</b> Mediant 500Li

### 2.20.3 Resolved Constraints

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

**Table 29: Resolved Constraints for Version 7.24A.356.468**

Incident	Description
MSBR-10622	For Predictive Dialing, nothing is sent to ISDN when receiving a SIP 183 Without SDP. (Resolved by new parameter <code>ISDNSendProgressOn183WithoutSdp</code> ). <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-10905	The <code>cwmp service</code> command is not in CLI. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-11007	IPSec VPN statistics doesn't function. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-11013	LAN port status is not correctly displayed in the Web interface (CLI is correct). <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-11028	The L2TP server connection doesn't timeout and can't connect again. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-11040	When the device is configured as an L2TP server, connecting to the VPN from an Android phone causes problems. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-11706	An unexpected cyclic message is sent to the device's console. <b>Applicable Products:</b> Mediant 500Li
MSBR-11710	Problem with 'upping' the BRI interface. <b>Applicable Products:</b> Mediant 500Li
MSBR-12025	SNMP port 1161 should always be the initiator only, but it accepts traffic. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12031	The DHCP service sends the wrong DNS IPv4 (translated IPv6 address). <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12037	Syslog shows error messages for DR session buffer size limit. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12234	DHCP FORCERENEW with Secret ID is 1 does not function. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12241	The End User Web interface doesn't function as expected. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12251	The interval of DPD packets for IPSec is sometimes unstable. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800

Incident	Description
MSBR-12260	The device experiences a boot loop after a factory reset. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12392	The device shows an inactive configured route ( <code>ip route</code> ) and it can't be deleted. <b>Applicable Products:</b> Mediant 500Li
MSBR-12398	The DHCP REQUEST for RENEW sent by the device does not have the correct hash value. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12478	The device freezes when an attempt is made to download the CLI script using the Web interface or when running the CLI <code>show run</code> command. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12484	The device is generating warning messages - "mu_lock while in AcLockStart" and "Un nested AcLockEnd". <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12488	When a switchover occurs between interfaces, the Call-ID SIP header shows "0.0.0.0" for the hostname even after local address is assigned. <b>Applicable Products:</b> Mediant 500Li
MSBR-12514	Configuration of debug recording (Logging Settings) is not possible (Web interface and CLI). <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12566	The device crashes when generating a TLS Context private key. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-12707	Memory leak causes the device to crash. <b>Applicable Products:</b> All
MSBR-12716	Web interface allows the configuration of a too small Idle period for TR-069. <b>Applicable Products:</b> Mediant 500Li
MSBR-12858	Warning messages are displayed. <b>Applicable Products:</b> Mediant 500, Mediant 500L, Mediant 800
MSBR-13001	The [AllowWanHTTP] and [AllowWanHTTPS] parameters are missing from the Web interface. <b>Applicable Products:</b> Mediant 500Li

## 2.21 Version 7.24A.356.263

This version includes new features, known constraints and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.21.1 New Features

This section describes the new features introduced in this version.

#### 2.21.1.1 LAN Port Redundancy

The device can now be configured for LAN port redundancy, where one of the ports is active while the other is the backup port (only one of them forwards packets).

Port backup operates in non-retrieve mode. The active port remains active until its link fails at which stage a switch-over to the backup port is done. When the first port link comes up again, no switch over (back) is made to this port, and it remains as the backup port.

After a device reset, if both ports have a link, the first port that was configured becomes the active port.

Port redundancy is configured as follows:

```
conf d
interface <first LAN port>
port-redundancy <second LAN port>
```

Example:

```
# conf d
(config-data)# interface fastethernet 1/4
(config-if-FE 1/4)# port-redundancy fastethernet 1/2
(config-if-FE 1/4)# do show data port-redundancy
Port Redundancy Status
-----
First Port    FastEthernet 1/4
Second Port   FastEthernet 1/2
Active Port   FastEthernet 1/4
```

**Applicable Products:** All.

#### 2.21.1.2 LLDP Client on LAN Ports

The device now supports enabling Link Layer Discovery Protocol (LLDP) client on its LAN ports. This is supported by the new CLI command:

```
conf d
lldp set-lan-as-client
```

**Applicable Products:** All.

## 2.21.2 Known Constraints

This section lists known constraints.

**Table 30: Known Constraints in Version 7.24A.356.263**

Incident	Description
MSBR-12250	QoS is not supported through data-router VLAN interfaces or VRFs. (Currently, supported only for WAN interfaces or directly through CMX OAMP interface in dual mode network.)

## 2.21.3 Resolved Constraints

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

**Table 31: Resolved Constraints for Version 7.24A.356.263**

Incident	Description
MSBR-12223	Optimize FQDN handling upon firewall reconfiguration.
MSBR-12034	A boot loop occurs after the device is upgrade from Version 7.20A.202.307 to 7.24A.356.248.
MSBR-12099	The device crashes (resets) when setting an illegal IPv6 address.
MSBR-12222	Remarks in the <code>access-list</code> command rules are sent for DNS resolution (should be disabled).
MSBR-12216	The device crashes (RMX Kernel Panic) upon the <code>show run</code> command.
MSBR-12213	RSyslog stops sending logs in case of a network/server problem.

## 2.22 Version 7.24A.356.248

This version includes new features, known constraints and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.22.1 New Features

This section describes the new features introduced in this version.

#### 2.22.1.1 OpenSSL Updated to Version 1.1.1k

OpenSSL, which is implemented in AudioCodes devices for secure communication using TLS, has been updated to OpenSSL Version 1.1.1k.

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.22.1.2 Multiple Access Lists per IPSec Tunnel

Multiple access lists (up to 10) can now be configured per IPSec tunnel, enabling multiple subnets to "reside" behind an IPSec tunnel.

**Applicable Products:** All.

#### 2.22.1.3 PADT Packet for Unknown PPPoE Sessions

The device now responds with a PPPoE Active Discovery Termination (PADT) message for unknown PPPoE sessions, which terminates the session.

**Applicable Products:** All.

#### 2.22.1.4 Registration Stickiness and Change in Proxy Set's IP Addresses

If an Account is registered with a registrar server which the device no longer "knows" (e.g., it was removed from the IP address results of the DNS resolution for the related Proxy Set), and the Registrar Stickiness feature is enabled, the device immediately initiates a new registration process for the Account (towards a different server that belongs to the destination Proxy Set).

**Applicable Application:** All.

**Applicable Products:** All.

#### 2.22.1.5 RADIUS over IPv6

RADIUS servers can now be configured with IPv6 addresses (per RFC 3162). In addition, the device now supports the RADIUS attribute *NAS-IPv6-Address* for IPv6 server; *NAS-IP-Address* for IPv4 server.

**Applicable Products:** All.

### 2.22.1.6 Mediant 800C MSBR Support for LTE WWAN

The device now supports Long-Term Evolution (LTE) wireless WAN (WWAN). This is supported by an integrated 4G LTE cellular modem, two cellular antennas, and a slot for inserting a Subscriber Identity Module (SIM) card to connect with the 4G cellular network.

**Applicable Products:** All.

### 2.22.1.7 SBC Registered Users Page for End-User Web Interface

The SBC Registered Users page has been added to the End-User Web interface (**Monitor > Voice** folder).

**Applicable Products:** All.

### 2.22.1.8 Random String in Contact User Part for Re-Registrations

A new value (2) has been added to the existing [UseRandomUser] parameter, which enables the device to generate a randomized string for the user part of the Contact header for every sent SIP REGISTER message, including initial registrations as well as registration refreshes.

**Applicable Products:** All.

### 2.22.1.9 Registration Refresh upon Receipt of DHCP FORCERENEW Message

The device can now be configured to send a new SIP REGISTER request (refresh) upon the receipt of a FORCERENEW message, under certain conditions. This applies to Accounts whose serving IP Group is associated with a Proxy Set that is configured to obtain the SIP server addresses through DHCP.

**Applicable Products:** All.

### 2.22.1.10 Transport Layer for Syslog

The transport layer protocol (UDP, TCP or TLS) for communicating with the Rsyslog server can now be configured. Up until now, the device used UDP only.

This feature is supported by the following new configuration:

- A new field in the Syslog Servers table called 'Protocol' configures the transport protocol of the secondary syslog servers. (The Syslog Servers table is now also configurable through the Web interface.)
- The new 'Syslog Protocol' parameter (SyslogProtocol) configures the transport protocol of the primary syslog server (applies also to CDR and SDR servers).
- The new 'Syslog TLS Context' parameter assigns a TLS Context when TLS transport is used (applies also to CDR and SDR servers).

**Applicable Products:** All.

### 2.22.1.11 TR-069 Scheduled File Download Update

Instead of downloading files at the beginning of the configured "idle" period, the device now randomly chooses a time within the "idle" period to download the files. (This occurs when the TR-069 ACS sends a request to the device, using the ScheduleDownload method, to download and apply files.)

**Applicable Products:** All.

### 2.22.1.12 Locking and Unlocking Device through TR-069

The TR-069 ACS can now lock and unlock the device. This is supported by the proprietary TR-069 object, `InternetGatewayDevice.X_00908F_Admin.{i}`.

**Applicable Products:** All.

### 2.22.1.13 Handling Device Root Certificates through TR-069 (TR-098)

The TR-069 ACS can now manage the device's root certificates through the TR-098 data model (`InternetGatewayDevice.ManagementServer.X_00908F_RootCertificate.{i}`). Up until now, it was supported only by the TR-181 data model.

**Applicable Products:** All.

## 2.22.2 Known Constraints

This section lists known constraints.

**Table 32: Known Constraints in Version 7.24A.356.248**

Incident	Description
-	The TLS Context selected for the syslog servers, using the 'Syslog TLS Context' parameter only uses the root certificate of the TLS Context and not the parameters (e.g., 'TLS Version') of the TLS Context. In addition, the maximum length of the certificate chain is 2. <b>Applicable Products:</b> MSBR.

## 2.22.3 Resolved Constraints

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

**Table 33: Resolved Constraints for Version 7.24A.356.248**

Incident	Description
MSBR-10215	A user cannot be removed from TACACS.
MSBR-10292	After an upgrade, a TLS Context issue occurs.
MSBR-10631	The device sends a syslog message in SIP headers.
MSBR-10745	NQM MOS-CQ and MOS-LQ threshold alarms are incorrectly triggered.
MSBR-10754	IPSec VPN connection repeats down/up.
MSBR-10778	No media occurs when forwarding a call in a vendor PBX.
MSBR-10787	The device does not send a DPD packet for IPSec with the expected interval.
MSBR-10839	The device does not resend an ARP.
MSBR-10869	GenerateRTP is not functioning for SBC functionality.
MSBR-10870	SSH from Ubuntu to the device does not function.
MSBR-10875	The device does not send a DHCP DISCOVER message when receiving a DHCP FORCERENEW.
MSBR-10889	Regression SNMP error since 7.24A.356.069.
MSBR-10897	Periodic device crash due to a Linux signal.

Incident	Description
MSBR-10903	The device crashes after running the <code>mac auto</code> command.
MSBR-10912	The configured <code>vlan-mac-prefix</code> for the ATM interface does not appear in the CLI script.
MSBR-10921	Cellular backup does not connect after a random time.
MSBR-10934	Even though the SDP offer changed, the 'o' attribute was not increased.
MSBR-10935	SNMP InterfaceIndex included in Link Up/Down traps needs to be excluded.
MSBR-10941	Allowed audio coders (AllowedAudioCodersGroup) in IP Profile are not recovered.
MSBR-10943	The device does not receive a SIP INVITE when using IPv6 with ICMPv6.
MSBR-10945	The device restarts due to a Kernel Panic.
MSBR-10946	IP Profiles table and Tel Profiles table in the Web interface start from index #1 (instead of 0).
MSBR-10967	The SIP REGISTER message must be sent when receiving a DHCP ACK triggered by DHCP FORCERENEW.
MSBR-10975	Problem connecting to the device's L2TP server or a third-party L2TP server.
MSBR-10979	A new user cannot be configured through CLI.
MSBR-11011	The device sends a SIP BYE message without a user part in the From header.
MSBR-11015	The PSTNAlertTimeout parameter does not function for Network Side.
MSBR-11051	The PRI interface goes down after a software update to 7.24A.356.069.
MSBR-11345	After upgrading to 7.24A.356.069, the L2TP tunnel no longer comes up.
MSBR-11426	The device crashes (restarts) almost every day due to a "SW Watchdog" reason.
MSBR-11490	When trunk comes up and all channels are busy, the device replies to SIP OPTIONS messages with a SIP 404 response (instead of 200 OK).
MSBR-8617	A PPP reset through TR-069 should wait until the ACS TCP session closes.

## 2.23 Version 7.24A.356.069

This version includes new features and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.23.1 New Features

This section describes the new features introduced in this version.

#### 2.23.1.1 RADIUS over IPv6

RADIUS servers can now be configured with IPv6 addresses. In addition, the device now supports the RADIUS attribute *NAS-IPv6-Address*.

**Applicable Products:** All.

#### 2.23.1.2 SNMP over IPv6

The device can now receive SNMP packets over IPv6. Trap Destinations can now be IPv4 and IPv6 (mix).

Note:

- The 'SNMP Transport Type' parameter (SnmpTransportType / snmp-transport-type) is now obsolete.
- SNMP Trusted Managers still only IPv4

**Applicable Products:** All.

#### 2.23.1.3 Web over IPv6

The device can now be configured with an IPv6 address (previously, only IPv4 was supported). In addition, the Access List table (Setup menu > Administration tab > Web & CLI folder > Access List), which limits access by clients to the web interface, can also be configured with IPv6 addresses.

**Applicable Products:** All.

#### 2.23.1.4 IPv6 DNS Resolution for Remote Web Server

When an FQDN is configured for a Remote Web Service (Setup menu > IP Network tab > Web Services > Remote Web Services), the device now supports DNS resolution for an IPv6 address. Up until now, only IPv4 DNS resolution was supported. If the DNS lookup results in an IPv4 and an IPv6 address, the IPv6 address is used (prioritized).

**Applicable Products:** All.

### 2.23.1.5 OVOC IPv6 Address for QoE

The OVOC server can now be configured on the device with an IPv6 address for Quality of Experience reporting (QOESettings\_SecondaryServerName).

**Applicable Products:** All.

### 2.23.1.6 Enhanced Authentication Protocol Support for SNMPv3 Users

The authentication protocol (SNMPUsers\_AuthProtocol) for SNMPv3 users can now be configured with any of the following secure hashing algorithms: SHA-2 224-bit, SHA-2 256-bit, SHA-2 384-bit, and SHA-2 512-bit. Up until now, only MD5 and SHA-1 were supported.

**Applicable Products:** All.

### 2.23.1.7 File Transfer using SCP

The device can now transfer files using Secure Copy Protocol (SCP). This is used with the `copy <File Type> to|from` command. The authentication username and password is included in the URL using the following syntax:

```
copy <File Type> from|to scp://<Username>:<Password>@<IP>/<Path>
```

For example:

```
copy firmware from scp://sue:1234@10.4.10.0/firmware.cmp
```

**Applicable Products:** All.

### 2.23.1.8 Syslog Enhancements

The following enhancements were introduced for Syslog:

- The device can be configured to send Syslog messages to up to four remote Syslog servers. This is configured in a new table `configure troubleshoot > syslog > syslog-servers` (SyslogServers).

**Applicable Products:** All.

### 2.23.1.9 New Performance Monitoring Display on Monitor Page (Dashboard)

The Monitor home page now also displays Gateway-related performance monitoring statistics. Up until now, only SBC statistics were displayed. The Monitor page displays the SBC and Gateway statistics under separate tabs ("SBC" and "GW", respectively). If there is no Gateway configuration, only the SBC tab is displayed.

**Applicable Products:** All.

### 2.23.1.10 Multicast Voice Traffic over T1/E1

The device can now route multicast voice traffic over T1/E1. The source and destination of the traffic are multicast groups.

**Applicable Products:** All.

### 2.23.1.11 Tracking Destinations Enhancements

The following enhancements have been done for tracking destinations:

- A description can be added when configuring tracking destinations, using the new subcommand `description`, for example:

```
track 1 icmp echo 8.8.8.8 GigabitEthernet 0/0 description
track_google_from_ge
```

- Output of the `show data track brief` command:
  - Output interface and description (if configured) are included
  - Filtering tracks by interface or destination

**Applicable Products:** All.

### 2.23.1.12 TR-069 Scheduled File Download

The device can now be configured with an "idle" period during which the TR-069 ACS can request (using the `ScheduleDownload` method) to download and apply a file to the CPE (device). This is useful in that it allows file download to be done during periods of relatively low traffic, avoiding disruption to calls. The device rejects the `ScheduleDownload` request if it is received out of the idle period.

This feature is configured under the new group, "Idle Period", which contains the following new parameters (SETUP -> ADMINISTRATION -> CWMP -> TR069 / conf sys > cwmp):

- 'Day of week' (TR069IdleTimeDayWeek)
- 'Start Time' (TR069IdleTimeStart)
- 'End Time' (TR069IdleTimeEnd)

**Applicable Products:** All.

### 2.23.1.13 IPsec Tunnel Establishment Modes

The device supports the following IPsec tunnel establishment modes:

- Active – (default) once configured, the device immediately initiates establishment of an IPsec tunnel with the remote peer
- Trigger – the device initiates establishment of an IPsec tunnel with the remote peer only if the device needs to send traffic through the tunnel (or the remote peer initiates it)
- Passive – the device establishes an IPsec tunnel only if the remote peer initiates it

The mode is configured using the new CLI command `set tunnel start-action-mode`.

Using the Trigger or Passive mode prevents both peers from initiating the tunnel simultaneously.

(Up until now, the device supported the Active mode only.)

**Applicable Products:** All.

### 2.23.1.14 Debug Recording over IPv6

The device now supports sending debug recording packets to a remote server with an IPv6 address. The address is configured using the existing parameter, `DebugRecordingDestIP`.

**Applicable Products:** All.

### 2.23.1.15 Trace Route Enhancements

The following trace route enhancements have been introduced:

- `traceroute <Destination> max-ttl <1-30>`  
Maximum number of hops to the destination (default 30).
- `traceroute <Destination> proto icmp|udp`  
Defines the protocol for the outgoing probes.
- `traceroute <Destination> resolve-to-name`

If a DNS server has been configured, this option displays the FQDN of each node on the path to the destination (where possible).

**Applicable Products:** All.

### 2.23.1.16 SIP Session Refreshes Based on Allow Header

For refreshing the timer of active SIP sessions, the device can be configured to send session refreshes using SIP UPDATE messages only if the SIP Allow header in the last received SIP message from the user contains the value "UPDATE". If the Allow header does not contain the "UPDATE" value, the device uses re-INVITE messages for session refreshes.

This feature is supported by the new optional value **According Remote Allow** (3) for the existing 'Session Expires Method' (SessionExpiresMethod) Gateway parameter.

**Applicable Products:** All.

### 2.23.1.17 Avoiding Previous Registrar Request

This feature is designed to prevent the device from sending register requests to a registrar server where the device previously registered, if the device also registered successfully to another server since the last successful registration to the registrar server. This can occur if the registrar server has been offline for a brief time. The device avoids attempting to register to this server for a duration that is calculated according to the cumulative value of the Proxy Server last "Expires" time and a new configurable grace time value.

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

- A new value for the existing Account\_RegistrarSearchMode parameter - Avoid Previous Registrar Until Expiry (2)
- A new global parameter - AccountRegistrarAvoidanceTime (configure voip/sip-definition proxy-and-registration/account-registrar-avoidance-time)

**Applicable Products:** All.

### 2.23.1.18 SIP Interworking of ISDN Disconnect with Facility IE

The device can be enabled to handle "known" Facility information elements (IE) that are included in incoming ISDN Disconnect messages.

For example, during the establishment (ISDN Setup) of an IP-to-Tel call, if the device receives an ISDN Disconnect message that includes a Facility Rerouting IE, it sends a SIP 302 to the IP side. If this feature were disabled, the device would ignore the Facility IE (except for Advice of Charge / AOC).

This feature is enabled (disabled by default) by the new parameter HandleISDNFacilityOnDisconnect.

**Applicable Products:** All.

## 2.23.2 Resolved Constraints

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

**Table 34: Resolved Constraints for Version 7.24A.356.069**

Incident	Description
MSBR-10209	TR-069 HTTP GET request for downloading firmware should not include port 80.
MSBR-10215	User cannot be removed through TACACS.
MSBR-10237	Configuration with five WAN interfaces no longer works.

Incident	Description
MSBR-10241	TR-069 violation of SetParameterValues - duplicated parameters.
MSBR-10288	TR-069 violation of SetParameterValues - wrong parameter type.
MSBR-10318	The TLS cipher suite is obsolete.
MSBR-10467	SNMP InterfaceIndex needs to be changes
MSBR-10516	SW Watchdog - Reset Reason
MSBR-10538	The device doesn't send SIP REGISTER message upon the receipt of a SIP 401 with 'Stale=FALSE'.
MSBR-10568	Some monitor bugs in device's End-User Web GUI.
MSBR-10570	The device lock feature (admin state lock) doesn't work as expected.
MSBR-10605	Cause of No ID translation between SIP and ISDN works only if CallingName is present in ISDN.
MSBR-10618	The ISDN RELEASE message doesn't have a Cause in case of a Timeout.
MSBR-10733	The device crashes (resets) when the CLI command <code>show activity log</code> is run.
MSBR-10769	CLI command <code>coders-and-profiles ip-profile new</code> doesn't function correctly.
MSBR-10770	The URL for CLI file upload exceeds the maximum number of characters (100) and therefore, upload files.
MSBR-8610	Cellular settings are not blocked for the End-User Web GUI when the <code>allow-wan-settings disable</code> is set.
MSBR-8680	Modification to an interface's IPv6 address fails.
MSBR-9505	VRRP master device reboots after it becomes master again.

## 2.24 Version 7.24A.256.329

This version includes new features and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.24.1 New Features

This section describes the new features introduced in this version.

#### 2.24.1.1 Universal CPE Solution

The AudioCodes Mediant 800 Universal Customer Premises Equipment (uCPE) is an ideal platform for UCaaS providers looking to reap the benefits of Network Function Virtualization. The platform integrates an Intel server module that can host SD-WAN or other third-party applications. These devices include branch routers, VoIP SBC and media gateways for SIP interoperability, connectivity, security and resiliency, allowing the customer to have real all-in-one device for SD-WAN or other NFV application.

**Applicable Products:** Mediant 800 MSBR.

#### 2.24.1.2 Automatic Provisioning via Remote Web (HTTP) Service

The device now supports automatic provisioning (configuration) from a remote HTTP server, using its Remote Web Service feature. Whenever the device boots up and this feature is enabled, it uses REST API to send an HTTP/S POST request with JSON content to the server with identification information (WAN MAC, WAN IPv6 address, serial number, and a hard-coded string value). If the server identifies the device and has an updated configuration file, it transfers the file to the device using Secure Copy Protocol (SCP), which uses SSH.

If the request fails (any HTTP response other than 200 OK), the device sends another request after 30 seconds. The maximum number of retries is three, after which the device's LED blinks green and the Web interface displays the provisioning status.

The feature is enabled and configured by a new group of parameters on the Web Service Settings page (Setup > IP Network > Web Service > Web Service Settings):

- Enabled: Enables the feature.
- Retry Interval: Defines the time in seconds between requests.
- Max Retries: Defines the maximum number of attempts to send the request, before considered a failure.
- Server URL: Defines the relative path of the provisioning server to send the request to.
- Server Username / Server Password: Defines the username and password for authentication with the server.
- Status: Displays provisioning status.

**Applicable Products:** MSBR.

### 2.24.1.3 Enhanced Device Restart Option

The existing `reload now` CLI command provides an additional optional value, `graceful if-no-calls`, which provides the following functionality when run:

- If calls exist, the device doesn't restart and displays "Not Good (In Call)".
- If no calls exist, the device restarts immediately and displays "OK".
- If the device is unable to restart (for whatever reason), it displays "Not Good".

(Configuration burning is done before reset.)

**Applicable Products:** MSBR.

### 2.24.1.4 Track Retries Enhancements

The following `track` command options have been added:

- `retries-up`: If the tracking destination status is "down" and the device probes it successfully for this user-defined number of consecutive attempts, the track status changes to "up" (i.e., reachable).
- `max-rtt`: Defines the maximum round-trip time (RTT) in milliseconds for each probe of the `retries` command, and if unsuccessful, the track status changes to "down".

**Applicable Products:** MSBR.

### 2.24.1.5 Up to Two Tracking Objects for Static Routes

A static route can now be configured to depend on two tracking objects. In this case, the route will only be active if both tracking objects are in "up" state. The feature is configured using the following commands:

```
(config-data)# ipv6 route [vrf vrf] destIP destMask next-hop  
interface [A-distance] [track 1 number] [track 2 number]
```

**Applicable Products:** MSBR.

### 2.24.1.6 On-the-Go Re-latching of Gratuitous ARP

The device supports on-the-go re-latching of gratuitous ARP to update its ARP cache on live traversing connections. Upon GARP issued by a LAN station, the MSBR changes the MAC address of the relevant connection, if required.

**Applicable Products:** MSBR.

### 2.24.1.7 End-User Web Interface Enhancements

The following has been added to the End-User Web interface's **Monitor > Voice** folder:

- Calls Count page, displaying statistics for IP-to-Tel and Tel-to-IP calls
- Registration Status page, displaying user registration on the device
- Gateway CDR History page, displaying gateway-related CDRs

**Applicable Products:** MSBR.

### 2.24.1.8 ISDN Behavior Enhancements

The following enhancements have been done for ISDN behavior configuration (on the Trunk Settings page):

- The existing 'ISDN NS Behaviour 2' parameter, which defines (by bit-field) several options that influence the behavior of the Q.931 protocol, now has an additional option, [256] **RESTART CLASS 7 IN FORCE RESTART** (0x0100). When this bit is set, the device sends RESTART (Class 7) if there is no call, on data link (re)initialization.
- The existing 'General Call Control Behavior' parameter, which defines (by bit-field) several general call control behavior options, now has an additional option, [4096] **NO B CHANNEL CONTROL** (0x1000). When this bit is set, B-channels allocation and control is left according to the application level. Call control doesn't control/allocate B-channels. The application provides the B-channel information within the appropriate ACU primitives. Call Control simply provides the received Channel-ID IE contents to the user, without checking its availability, validity or consistency with other calls in progress. This bit should be set when the B-channel can be changed in Q.931 Proceeding, Alerting, or Connect.

**Applicable Products:** MSBR.

### 2.24.1.9 Channel Identification IE Format (Number or Slotmap) in ISDN Messages

Up until now, the device supported only the channel number format in the Channel Identification IE when sending Q.931 ISDN messages. Now, for NTT protocol, it also supports the slotmap format.

The following new parameters have been added to specify the format:

- (Global) ISDNChannelIDFormat (gw-digital-settings isdn-channel-id-format): 0 for Channel Number (default) and 1 for Slotmap.
- (Per trunk) ISDNChannelIDFormatForTrunk (e1-t1 isdn-channel-id-format-for-trunk): 0 for Channel Number and 1 for Slotmap. Default is according to the global parameter (above).

The device's handling of the Channel Identification format is as follows:

- Device as Network Termination (NT):
  - Device-to-PBX: The device includes the configured Channel Identification format (Slotmap or Channel Number) in the outgoing ISDN SETUP. The PBX can respond (CPROC, ALERT or CONNECT) with its own Channel Identification, which the device adopts. However, if the PBX doesn't include information for the Channel Identification, the device adopts the one that it offered in the SETUP.
  - PBX-to-Device: The device adopts the same Channel Identification received in the SETUP from the PBX (and notifies this to the PBX in the CPROC). However, if the PBX didn't include information for the Channel Identification, the device adopts the configured format (and notifies this to the PBX in CPROC).
- Device as Terminal Equipment (TE):
  - Device-to-PBX: The device includes the configured Channel Identification format (Slotmap or Channel Number), and notifies this to the PBX in the SETUP.
  - PBX-to-Device: The device includes the configured Channel Identification format (Slotmap or Channel Number), and notifies this to the PBX in the CPROC.

**Applicable Products:** MSBR.

### 2.24.1.10 Improved Prefix Delegation (PD) with Router Advertisement (RA) and DHCP Server Operation

It is now possible to select where to apply the prefix from the PD to the RA, DHCP server, or both. This is supported by the following new CLI commands:

- Prefix added only to RA:
 

```
ipv6 nd prefix 2001:2001:: default no-import-to-dhcps
```
- Prefix added to RA and DHCP server:

```
ipv6 nd prefix 2001:2001:: default
```

- Prefix from PD added to DHCP server only:

```
ipv6 nd pd GigabitEthernet 0/0 ::2:0:0:0:0:0/64 no-import-to-ra
```

- Prefix from PD added to RA and DHCP server:

```
ipv6 nd pd GigabitEthernet 0/0 ::2:0:0:0:0:0/64
```

**Applicable Products:** MSBR.

## 2.24.2 Resolved Constraints

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

**Table 35: Resolved Constraints for Version 7.24A.256.329**

Incident	Description
MSBR-10216	SIM pin code changes when upgrading software version.
MSBR-10232	Inconsistent naming of ISDN interfaces between the output of <code>sh voip calls act</code> and <code>sh voip calls his gw</code> .
MSBR-10233	Tel-to-IP Routing table's 'Connectivity Status' field doesn't reflect correct connectivity status (causing backup route issues).
MSBR-10289	TR-069 - lack of type specification in SOAP elements
MSBR-10324	TTL value for outbound SIP/RTP traffic.
MSBR-10334	No corresponding CLI command for the UseRandomUser ini file parameter. Now added <code>-- configure voip &gt; sip-definition proxy-and-registration use-rand-user</code> .
MSBR-8621	TR-069 configuration restoration via Device.DeviceInfo.X_T-ONLINE-DE_ConfigFile does not function.
MSBR-9640	Prefix delegation forwarding interoperability with Router Advertisement is not correct.
MSBR-9684	SNMP traps for MIB-2 or IF-MIB are missing.
MSBR-9685	L2TP network can't go up after the cellular APN is changed.
MSBR-9846	Default payload type for data call is set to 56. (Constraint resolved by new parameter TransparentPayloadType.)
MSBR-9943	When the CWMP interface is bound to the loopback interface, DNS requests are not sent from the loopback address (i.e., sent with wrong source).
MSBR-9978	Some websites cannot be accessed by LAN computers connected to the MSBR.
MSBR-9986	Configuring ISDN Gateway in Single Network mode for ISDN backup route is not functioning.

## 2.25 Version 7.24A.256.219

This version includes new features and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.25.1 New Features

This section describes the new features introduced in this version.

#### 2.25.1.1 Waiting for Calls to End before Graceful Lock

An additional option has been added to the device's graceful lock feature that allows the device to wait without a timeout, until all active calls end before going into lock state. No new calls are accepted during this period.

This feature is activated using the new CLI command option, `forever`:

```
# admin state lock graceful forever
```

**Applicable Products:** MSBR.

#### 2.25.1.2 REST-Based API for Performance Monitoring

The device now supports REST-based management (IPv4 only) for viewing performance monitoring. The REST APIs are accessed using the following REST URL path: `api/v1/performanceMonitoring/<Performance Monitoring Parameter>`

Where *Performance Monitoring Parameter* is:

- `gwAttemptedCalls (acPMSIPAttemptedCallsValIP2Tel)`
- `gwIP2TelTrunkEstablishedCalls (acPMSIPEstablishedCallsValIP2Tel)`
- `gwAttemptedCalls (acPMSIPAttemptedCallsValTel2IP)`
- `gwTel2IPTrunkEstablishedCalls (acPMSIPEstablishedCallsValTel2IP)`
- `TrunkUtilization (acPMTrunkUtilizationMax)`
- `TrunkUtilization (acPMTrunkUtilizationMin)`

**Applicable Products:** MSBR.

#### 2.25.1.3 Using Interface Descriptive Name for Associations

For all CLI commands, there is an option to configure a descriptive name for the interface and then use this name in other CLI commands to refer to the interface. This makes it more user-friendly for users, enabling them to easily identify the interface. The command that configures the description name is `desc`.

For example, the below configures the descriptive name of the Gigabit Ethernet interface to "MyGbE":

```
#configure data
```

```
(config-data)# interface gigabitethernet 0/0
(conf-if-GE 0/0)# desc MyGbE
```

Once, configured, the descriptive name can be used in other CLI commands, for example:

- Example:

```
# show data interfaces desc MyGbE
```

- Example:

```
(config-data)# interface desc MyGbE
(conf-if-GE 0/0)#
```

**Applicable Products:** MSBR. I

### 2.25.1.4 IPSec Hash Algorithms SHA-384 and HAS-512

The device now supports enhanced IPSec / IKE security protocol:

- ESP Authentication Transform: ESP with the SHA-256 bit key combined with HMAC variant as the authentication algorithm:

```
(config data)# crypto ipsec transform-set <Name> esp-
<Encryption> esp-sha256-hmac
```

- Hash Algorithm within IKE Policy: SHA-384 and SHA-512:

```
(config-isakmp)# hash {md5|sha|sha256|sha384|sha512}
```

**Applicable Products:** MSBR.

### 2.25.1.5 TR-069 File Download Enhancements

The device now supports loading a TLS certificate file \*.pem (without a private key) through TR-069, using the DownloadFile method with File Type = 1 (Firmware Upgrade Image).

After loading the file, the device resets.

**Applicable Products:** MSBR.

### 2.25.1.6 New Filtering Switch for show voip calls Command

The CLI command for filtering the output of the `show voip calls` command has been updated. Instead of the `| grep` switch for filtering, the new `match` switch is used, which provides a simple string match of the call detail record text. For example:

```
show voip calls active sbc match abc
```

**Applicable Products:** MSBR.

### 2.25.1.7 Track Command Enhancements

The track feature has been enhanced:

- Clear track minimum RTT values:

```
# clear counters track [<track id>
```

- Minimum / 60sec, average and target has been added to the output of the following command:

```
show data track brief
```

- Displays two graphs of the average RTT (round trip time) of probes sent by a specific track in the last 60 minutes and 72 hours:

```
show data track <ID> rtt-history
```

**Applicable Products:** MSBR.

### 2.25.1.8 Denying Access to Failed Login Attempts

The following two new parameters have been added to the denying access after failed login attempts:

- **BlockDurationFactor:** Defines the number to multiple the previous blocking time for blocking the user upon the next failed login scenario. For example, assume the following configuration:
  - The 'Deny Access On Fail Count' parameter is configured to 3 (failed login attempts).
  - The 'Block Duration' parameter is configured to 10 (seconds).
  - The BlockDurationFactor parameter is configured to 2.

After three failed login attempts, the device blocks the user for 10 seconds. If the user tries again to login but fails after three attempts, the device blocks the user for 20 seconds (i.e., 10 x 2). If the user tries again to login but fails after three attempts, the device blocks the user for 40 seconds (i.e., 20 x 2), and so on.

- **DenyAccessCountingValidTime:** Defines the maximum time interval (in seconds) between failed login attempts to be included in the count of failed login attempts for denying access to the user. For example, assume the following:
  - The 'Deny Access On Fail Count' parameter is configured to 3 (failed login attempts).
  - The DenyAccessCountingValidTime parameter is configured to 30 (seconds).

If the user makes a failed login attempt, and then makes another failed login attempt 32 seconds later, and another failed login attempt 10 seconds later, the user is not blocked by the device. This is because the interval between the first and second attempt was greater than the 30 seconds configured for the DenyAccessCountingValidTime' parameter. However, if the interval between all three failed login attempts is less than 30 seconds, the device blocks the user.

**Applicable Products:** MSBR.

### 2.25.1.9 DHCP Enhancements

The device now provides the following DHCP enhancements:

- DHCP Option 125 to configure the SIP account.
- To make the MSBR not request the previous address obtained through DHCP, a new command has been added:

```
ip dhcp-client retain-address
```

- To request SIP server's IP address (and other information) the device can now send a DHCP Option 120 request as Request List Items in Option 55, using a new command:

```
ip dhcp-client sip-server-address
```

- Second authentication key is now supported. The CLI command is the same as for the first key (configure another key with a different, usually unique key ID):

```
ip dhcp-client authentication key-id ...
```

**Applicable Products:** MSBR.

### 2.25.1.10 Fax Transmission

For Tel-to-IP fax transmission, the IsFaxUsed parameter now has a new optional value, G.711 reject T.38 (4). It is like the value G.711 Transport (2), but if the incoming media is of type IMAGE, the device rejects it.

**Applicable Products:** MSBR.

## 2.25.2 Resolved Constraints

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

**Table 36: Resolved Constraints for Version 7.24A.256.219**

Incident	Description
MSBR-8343	Security vulnerability – the device responds with CGI script on TCP port 4.
MSBR-8583	IPv6 DNS relay does not function.
MSBR-8611	The device doesn't support a TR-069 redirect link that is long (now it supports up to 256 characters).
MSBR-8612	The device sends the wrong User-Agent value for TR-069.
MSBR-8617	After performing a PPP reset via the TR-069 ACS by the data parameter Reset (Device.>>PPP.>>Interface.>>1.>>Reset), instead of waiting for the current TCP session with ACS to end, the device performs an immediate termination of the PPP session by sending "PADT".
MSBR-8618	The Event Code 4 is missing in the Inform message sent to the TR-069 ACS after the device resets.
MSBR-8706	DNS TTL of 5 seconds is not supported.
MSBR-8707	After performing a diagnostics test Download/Upload from the ACS, the URL changes back to default before device performs a restart.
MSBR-8708	When the device communicates with the TR-069 ACS, for example, after a restart, in CWMP-XML communication, the time offset is incorrect.
MSBR-8718	When ACS performs an IP Download Diagnostics after completion, the device does not send an INFORM message to ACS to change the status of Device.IP.Diagnostics.DownloadDiagnostics.DiagnosticsState.
MSBR-8770	The device becomes unresponsive if TCP/TLS options keep-alive are configured but unreachable.
MSBR-9011	The TR-069 data model of the MSBR 800C device under the Device.>DeviceInfo.>ModelName parameter value is showing "M800B" instead of "M800C".
MSBR-9421	IPSec in Single Networking Mode routes SIP REGISTERS outside the tunnel.
MSBR-9507	Busy-out event doesn't trigger the LED on the device's chassis to turn red.
MSBR-9555	IPv6 packets sent from the PPPoE interface have incorrect payload in the PPP header.
MSBR-9583	Dynamic DNS service doesn't function correctly.
MSBR-9611	SIP Account (Accounts table) attempts to register before the ISDN port interface is cabled (trunk is down).

Incident	Description
MSBR-9618	Corresponding CLI commands of SBCMINSE (for SBC) and MINSE (FOR Gateway), which configure the session expiry time, have the same names. Now, Gateway parameter has been relocated in CLI.
MSBR-9619	Filtering the <code>show voip calls</code> command output using the <code>grep</code> filter ( <code>  grep</code> ) doesn't function. This was resolved by removing the <code>grep</code> switch and replacing it with the new <code>match</code> switch, which provides a simple string match of the call detail record text. For example, to search the string "abc": <pre>show voip calls active sbc match abc</pre>
MSBR-9641	When sending an INVITE, the host part in the From header should be that configured by the SIP Group Name parameter of the IP Group. But sometimes, it sends the IP address of the destination.
MSBR-9644	PPP session via LTE cannot be established. (Now, the <code>show data cellular status</code> command displays reception signal for LTE based on RSRP (instead of RSSI).
MSBR-9648	DHCPv4 authentication second key is not supported, DHCP client option 120 and 150 CLI support.
MSBR-9653	Device crashes (resets) when long condition is configured in the Message Manipulations table.
MSBR-9659	After software upgrade, TR-069 ProvisioningCode is incorrect.
MSBR-9677	If there is only a single Security Administrator uses, the user can configure its status to <b>Inactivity</b> , meaning that the user will never be allowed to log in to the device.
MSBR-9684	Trap alarms sent only from the AC MIBS but not from MIB-2 or IF-MIB.
MSBR-9704	The following parameters don't have corresponding CLI commands: Maxsdpsessionversionid, Unregisteronstartup, and Sipdigestauthorizationurimode. CLI commands now added (max-sdp-sess-ver-id, unreg-on-startup, digest-auth-uri-mode).
MSBR-9705	No CWMP output for the commands <code>show voip calls active</code> and <code>show voip calls history gw last 5</code> .
MSBR-9730	The device crashes (WEB Tasks) when using Google Chrome (long cookie field).
MSBR-9733	The device changes the SDP body in the outgoing SIP 200 OK even though the version in the 'o=' line does not increase.
MSBR-9739	Tel-to-IP fax transmission fails. To resolve the issue, the IsFaxUsed parameter now has a new optional value, G.711 reject T.38 (4). It is like the value G.711 Transport (2), but if the incoming media is of type IMAGE it is rejected.
MSBR-9765	Root certificate file upload through TR-069 is not preserved after power off.
MSBR-9812	After upgrading the device, it crashes (resets) after being up for about a day.
MSBR-9816	Device doesn't connect to the TR-069 ACS after a reset to factory defaults.
MSBR-9820	When loading a CLI script file, some configuration lines are missing.
MSBR-9826	DHCP Option 125 for obtaining (device acting as DHCP client) SIP user information such as phone number and SIP domain does not function.
MSBR-9827	Internal clock (date and time) synchronization with remote server (SIP Date header) using SIP (according to RFC 3261) is not functioning.

Incident	Description
MSBR-9859	The MSBR crashes (resets) when Trunk Group settings are configured, using the command <code>gateway trunk-group-setting</code> .
MSBR-9860	Different syntax (for endpoint name) in command output between <code>show voip calls active gw</code> and <code>show voip calls history gw</code> .
MSBR-9865	TACACS configuration is not fully saved.
MSBR-9883	An issue with transcoding due to lack of DSP resources.
MSBR-9894	When the License Key file is loaded to the device using the Auto-Update mechanism (IniFileUrl parameter), some configured parameters return to their default settings (instead of remaining at their current values).

## 2.26 Version 7.24A.256.105

This version includes new features and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.26.1 New Features

This section describes the new features introduced in this version.

#### 2.26.1.1 New Licensing Method - Floating License

The device now supports a new licensing method called *Floating License*. The Floating License is a network-wide SBC capacity-related license pool, which is managed by AudioCodes OVOC and the cloud-based License Manager. The license pool is shared dynamically among multiple devices. The Floating License is a 'pay as you grow' service, eliminating the need to manually purchase additional SBC licenses each time capacity requirements increase. A Floating License is initially purchased based on estimated SBC capacity requirements. If capacity later increases and exceeds the initially purchased licenses, the License Manager allows this excess and the Customer is billed at the end of the month for the additional licenses.

**Applicable Products:** MSBR.

#### 2.26.1.2 Cellular Status Display Enhancements

The existing command `show data cellular status` has been enhanced:

- Displays signal strength (in dBm) for LTE (already supported for PPP mode)
- Displays history status of signal strength using the new subcommand, `show data cellular status history [1-60]`

**Applicable Products:** MSBR.

### 2.26.1.3 Registration Based on Trunk Group Status

The device can now send a registration request (SIP REGISTER) to a serving IP Group (SIP registrar) even when the Trunk Group is out-of-service. Up until now, registration requests were sent only if it was in-service.

For example, this feature may be useful for deployments that require the device to register a configured Trunk Group, before its PSTN cable has been connected to the device (i.e., out-of-service).

The feature is configured by the new parameter 'Register By Served Trunk Group Status' (RegisterByTrunkGroupStatus / configure voip / gateway advanced / register-by-served-tg-status), with the following optional values:

- Register Only if In-Service (0): (Default) Registration request is sent only if the Trunk Group's status is in-service (supported until now).
- Register Always (1): Registration request is always sent, regardless of the Trunk Group's status (in-service or out-of-service).

**Note:**

- The feature is applicable only to E1/T1 ISDN/CAS.
- The feature is applicable only to Trunk Group's whose 'Registration Mode' is configured to Per Account (in the Trunk Group Settings table).

**Applicable Products:** MSBR.

### 2.26.1.4 Clock Synchronization through SIP

The device's internal clock can synchronize its date and time settings with a remote server using SIP (according to RFC 3261). The device obtains the date and time from the Date header in the incoming 200 OK in response to the REGISTER request sent by the device, as shown in the example below:

```
Date: Sat, 12 Mar 2020 23:29:00 GMT
```

The feature is enabled by the following new parameters:

- 'Synchronize Time from SIP Date Header' (DateHeaderTimeSync): Enables the feature (by default, it's disabled).
- 'Time Synchronization Interval' (DateHeaderTimeSyncInterval): Defines the minimum time (in seconds) between synchronization updates (60 to 86400; default 900).

**Note:**

- The device only uses the date in the Date header if its value is year 2016 or later.
- If both this feature and NTP are enabled, synchronization by the NTP server takes precedence (device ignores received Date headers). When both are enabled, the device sends an SNMP alarm acClockConfigurationAlarm (1.3.6.1.4.1.5003.9.10.1.21.2.0.149).
- Once a week, the device stores the clock's date and time in its flash memory. If the device is restarted, its clock is set to the stored date and time.

**Applicable Products:** MSBR.

### 2.26.1.5 SIP-ISDN Interworking of NTT Japan No-ID Cause

The device now supports SIP-ISDN interworking between NTT Japan's No-ID cause in the Facility information element (IE) of the ISDN Setup message, and the calling party number (display name) in the From header of the SIP INVITE message. The No ID cause in the Facility IE indicates one of four reasons (see table below), for example, why the call was blocked.

The feature is configured by the new parameter IsdnNttNoidInterworkingMode (gw-digital-settings isdn-ntt-noid-interworking-mode), with the following values:

- 0 – (default) No interworking of No-ID cause.
- 1 – Interwork No-ID cause from IP to Tel.
- 2 – Interwork No-ID cause from Tel to IP.
- 3 - Interwork No-ID cause from IP-to-Tel and Tel-to-IP sides.

The table below shows the mapping between the SIP display name in the From header and the cause of the Facility IE in the ISDN Setup message:

SIP Display Name in From Header	Cause in ISDN Setup Facility IE
Unavailable	IE[03]=1c 11 91 a1 0e 02 01 00 06 06 02 83 38 66 01 01 0a 01 00
Anonymous	IE[03]=1c 11 91 a1 0e 02 01 00 06 06 02 83 38 66 01 01 0a 01 01
Interaction with other service	IE[03]=1c 11 91 a1 0e 02 01 00 06 06 02 83 38 66 01 01 0a 01 02
Coin line/payphone	IE[03]=1c 11 91 a1 0e 02 01 00 06 06 02 83 38 66 01 01 0a 01 03

Below shows an example of an ISDN No-ID cause mapped to SIP for "Interaction with other service":

```
From: "Interaction with other service"
<sip:anonymous@anonymous.invalid;pstn-
params=9082828088>;tag=gK09696ce6
```

Note: The feature is applicable only to Trunks configured with the JAPAN NTT ISDN PRI (T1) protocol variant (ProtocolType = 16).

**Applicable Products:** MSBR.

### 2.26.1.6 ISDN Restart Class 7 and Q.931 Layer Response Behavior

The device now sends a Restart Class 7 when forcing a restart - sends an ISDN Restart message if there is no call, on a data link (re)initialization. Up until now, Restart Class 6 was sent for forced restart. This feature affects the existing ISDNBehavior parameter when configured to 4194304 (FORCED RESTART). Note that Restart Class 7 is also sent for all the other optional values.

**Applicable Products:** MSBR.

### 2.26.1.7 Multiple Access Lists per Rule

Multiple access lists (up to 10) can now be configured per access list rule, for example:

```
access-list 101 permit ip 150.150.150.0 0.0.0.255 200.200.200.0
0.0.0.255
access-list 101 permit ip 101.101.101.0 0.0.0.255 201.201.201.0
0.0.0.255
access-list 101 permit ip 150.150.150.0 0.0.0.255 201.201.201.0
0.0.0.255
```

**Applicable Products:** MSBR.

### 2.26.1.8 TR-069 over IPv6 Enabling

TR-069 over IPv6 must be enabled (disabled, by default). If not enabled, the device uses only IPv4. Configuration is done by the new parameter 'IPv6' (configure system > cwmp > ipv6 enable)

**Applicable Products:** MSBR.

### 2.26.1.9 TR-069 Connection to ACS via VRF or Loopback Interface

The device's TR-069 service can now connect to the ACS also through a loopback interface in the main VRF. The source interface is configured as follows:

```
configure system > cwmp > source data source-address interface  
loopback <ID>
```

**Note:**

- Device reset is no longer required for configuration to take effect.
- Above replaces `configure system > cwmp > vrf-name`.

Loopback interface has been added to the TR-069 tree (TR-098 and TR-181).

**Applicable Products:** MSBR.

### 2.26.1.10 Incremental CLI Script Download via TR-069

Incremental CLI script download via TR069 is now supported using the TR-069 DownloadFile method.

**Applicable Products:** MSBR.

### 2.26.1.11 SNMP Alarm for Status Change of LTE Cellular

The device now sends the SNMP alarm `acWirelessCellularModemStatusChanged` (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.104) when a status change (signal strength or cellular technology used) occurs in the integrated LTE (4G) cellular WAN modem.

**Applicable Products:** Mediant 500L MSBR.

### 2.26.1.12 Increased Security using IPSec Transform Set ESP SHA-256-HMAC

The device now supports IPSec security protocol ESP with the SHA-256 bit key combined with HMAC variant as the authentication algorithm. This is configured by the new optional value `esp-sha256-hmac` in the following CLI command:

```
config-data)# crypto ipsec transform-set <name> esp-sha256-hmac
```

**Applicable Products:** MSBR.

### 2.26.1.13 Configurable Default TR-069 Product Class

The default TR-069 Product Class ("MSBR") can now be changed (configurable), by the new ini file parameter `TR069CustomerProductClass`.

**Applicable Products:** MSBR.

### 2.26.1.14 SIP Server (Proxy Set) Addresses from DHCPv4 Server

The device can now obtain a Proxy Set's address(es) from a DHCP server. When this feature is enabled, the device sends a DHCP request with Option 120 to a DHCP server. This occurs upon a DHCP refresh (lease renewal). When the device receives the list of IP addresses (or FQDN) from the server, it adds them to the Proxy Set (replaces any existing IP addresses or FQDNs). This occurs for the Proxy Set that is associated with the SIP Interface that is associated with the WAN interface.

The feature is enabled by the new Proxy Sets table parameter 'Accept DHCP Proxy List'.

**Applicable Products:** All.

### 2.26.1.15 DHCPv4/v6 Authentication and Options

The device now supports the following DHCP client features:

- Authentication of DHCPv4 messages, configured by the new CLI command:

```
(config-data) # interface <Interface>
(conf-if-<Interface>) # ip dhcp-client authentication key-id
<ID> key-string|obscured-key-string <Key/Obscured Key>
```

- Authentication of DHCPv6 messages, configured by the new CLI command:

```
(config-data) # interface <Interface>
(conf-if-<Interface>) # ipv6 dhcp-client authentication realm
<Realm Name> key-id <ID> key-string|obscured-key-string
<Key/Obscured Key>
```

- Receipt of DHCPv6 Reconfigure messages from DHCP servers (RFC 3315), which indicate if the MSBR client must respond with a Renew or an Information-request message.
- Receipt of DHCP Options for list of SIP server IP addresses:
  - DHCPv6 - Option 22 (RFC 3319)
  - DHCPv4 - Option 120

**Applicable Products:** All.

### 2.26.2 Resolved Constraints

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

**Table 37: Resolved Constraints for Version 7.24A.256.105**

Incident	Description
MSBR-8983	The IPSec connection (IKEv2) takes a long time to establish.
MSBR-9056	There is no corresponding CLI command for the 'Forking Handling Mode' Web parameter.
MSBR-9062	The device can't load a Dial Plan file (.csv) through CLI from a remote IPv6-based server.
MSBR-9076	IPSec connection cannot use source based ACLs (only works when ACL is destination based).
MSBR-9077	BFD is not correctly shutting down the interface (IPv6).
MSBR-9210	The BFD timer not negotiated correctly (IPv6).
MSBR-9249	The device opens a second TCP session even though the initial one still exists.
MSBR-9290	Fax transcoding fails when all coders are unsupported.
MSBR-9372	IPv6 - no ping from LAN to WAN when WAN is a PPPoE interface.
MSBR-9383	The Auto-Update mechanism is not functioning.
MSBR-9419	Sometimes the VPN setup process takes a long time.
MSBR-9431	The device doesn't support the receipt of Prefix Delegation (PD) greater than 64 bits, and therefore, doesn't forward it.
MSBR-9473	The parameter CEDTRANSFERMODE is missing from the device's management interface.
MSBR-9503	VPN client doesn't connect to the device's L2TP server.

Incident	Description
MSBR-9541	Device failure due to TR-069 database corruption.
MSBR-9668	After loading trusted root certificate ("*.cert") using the TR-069 DownloadFile method, the certificate is not saved to flash.

## 2.27 Version 7.20A.256.125

This version includes new features and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.27.1 Resolved Constraints

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

**Table 38: Resolved Constraints for Version 7.20A.256.125**

Incident	Description
MSBR-8915	The device's IPSec feature doesn't function with a certain vendor's firewall. (This was resolved by a new command, <code>crypto isakmp identity address &lt;public IP address&gt;</code> , which allows peers to identify themselves by IP address.)
MSBR-9258	For TR-069, after a factory reset or reboot, after resolving the ACS URL the device loses connectivity with the ACS.
MSBR-9271	The display format of the CLI command <code>show data interfaces switchport</code> needs improvement. (Now, it's in table format.)
MSBR-9310	Device crashes (resets) due to RMX module issue.

## 2.28 Version 7.20A.256.107

This version includes new features and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.256.024.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

## 2.28.1 New Features

This section describes the new features introduced in this version.

### 2.28.1.1 Bandwidth Usage History per Interface

The device now provides bandwidth usage history per interface. This is supported by the following new command:

```
show data interfaces <Interface> history bandwidth [hours|minutes]
```

where:

- *hours* displays the mean bandwidth usage every 10 minutes for the past 72 hours
- *minutes* displays bandwidth usage every 15 seconds for the past 120 minutes

The CLI output is displayed in descending order (i.e., most recent measurement displayed on top of the list).

For example, the below lists bandwidth usage every 15 minutes of the PPPoE interface:

```
show data interfaces pppoe 0 history bandwidth minutes
Jan 19 20 07:24:35 - Tx:2533 [bps], Rx:25933 [bps]
Jan 19 20 07:24:20 - Tx:2666 [bps], Rx:2666 [bps]
Jan 19 20 07:24:05 - Tx:0 [bps], Rx:29333 [bps]
Jan 19 20 07:23:50 - Tx:0 [bps], Rx:0 [bps]
```

**Applicable Products:** All.

### 2.28.1.2 DNS Rebinding Protection

The device now provides protection against DNS rebinding attacks. This may occur when management users access the device using its hostname (configured by the existing parameter HostName) instead of the IP address. The feature is enabled by the new parameter 'DNS Rebinding Protection Enabled'.

**Applicable Products:** All.

### 2.28.1.3 TLS Version 1.3 Support

The device now supports TLS version 1.3. As a result, the following changes have been made to the existing TLS Contexts table:

- Following new values have been added to the 'TLS Version' parameter:
  - [8] TLSv1.3
  - [12] TLSv1.2 and TLSv1.3
  - [14] TLSv1.1 TLSv1.2 and TLSv1.3
  - [15] TLSv1.0 TLSv1.1 TLSv1.2 and TLSv1.3

The value [0] Any - Including SSLv3 has been renamed [0] Any TLS 1.x, which now supports only TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3. SSL is no longer supported.

- For TLS 1.3, a dedicated cipher list needs to be configured, using the following new parameters:
  - Cipher Server TLS1.3
  - Cipher Client TLS1.3
- To configure groups that are supported for key exchange, the new parameter 'Key Exchange Groups' has been added. This is applicable to all TLS versions. Values include X25519, P-256, P-384, and X448.

- For TLS 1.3, it can be configured to enable TLS clients to send dummy handshake packets to imitate the handshakes of TLS 1.2 and lower TLS versions to prevent blockage by intermediate network nodes. This is enabled using the new parameter 'Middlebox Compatibility Mode'.
- The default of the 'DH Key Size' parameter has been changed to 2048.

**Applicable Products:** All.

#### 2.28.1.4 TR-069 over IPv6

The device now also supports IPv6 for TR-069 communication with the TR-069 Auto-Configuration Server (ACS). The device determines whether to use an IPv4 or IPv6 interface for communication according to the URL of the ACS, which is configured on the device. If the URL contains a domain name (FQDN), the device determines the IPv4/IPv6 interface according to the IP address version from the DNS resolution.

The following parameter object has been added for this feature:

- Device.IP.Interface.{i}.IPv6Address.{i}.

**Applicable Products:** All.

#### 2.28.1.5 Delay Time for Resending Failed SIP OPTIONS Keep-Alive Messages

The device can now be configured to wait a user-defined duration (in seconds) before re-sending a SIP OPTIONS keep-alive message to the SIP proxy server after receiving a failed SIP response from the previously sent keep-alive message. The feature is configured by the new ini file parameter, FailedOptionsRetryTime.

**Applicable Products:** All.

#### 2.28.1.6 Proxy Keep-Alive for Active Proxy Server Only

Up until now, when the device was enabled to send keep-alive SIP OPTIONS messages to proxy servers belonging to a Proxy Set, it sent them to all the proxies regardless of the configured redundancy mode (parking or homing), configured by the 'Redundancy Mode' parameter. Now, the device can be configured to regard the redundancy mode, using the new optional value **Using OPTIONS on Active Server** for the existing 'Proxy Keep-Alive' parameter in the Proxy Sets table:

- Parking mode: The device sends keep-alive OPTIONS messages only to the currently active proxy server.
- Homing mode: The device sends keep-alive OPTIONS messages to the currently active proxy server as well as to all servers (offline) with higher priority than the active server. Once a higher priority server comes online, the device stops sending OPTIONS to the previously active server and connects to this higher priority server. The device now sends keep-alive messages to it and all servers (offline) with higher priority.
- If the 'Redundancy Mode' parameter is not specified and the 'Proxy Load Balancing Method' parameter is configured to any value other than **Disable**, the device sends keep-alive OPTIONS messages to all active proxy servers (same behavior as if the Proxy Keep-Alive parameter was configured to **Using OPTIONS**).

**Applicable Products:** All.

## 2.28.2 Resolved Constraints

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

**Table 39: Resolved Constraints for Version 7.20A.256.107**

Incident	Description
MSBR-8760	When SIP Message Manipulation is configured to add a P-Early-Media header with value 'supported' and alternative routing is used, the call fails.
MSBR-8891	After the device is upgraded from Ver. 6.8 to Ver. 7.2, configuration of the Access List for IPv6 addresses ( <code>ipv6 access-list</code> ) is modified (address is removed).
MSBR-8971	In L2TP tunneling, LCP negotiation with a limited MRU size doesn't function.
MSBR-9037	Classification by Proxy Set fails ('Classify By Proxy Set' parameter configured to Enabled) in certain scenarios when the Proxy Set address is an FQDN (DNS resolution).
MSBR-9051	A prefix cannot be configured for the IPv6 DHCP server.
MSBR-9056	No corresponding CLI command exists for the Web parameter 'Forking Handling Mode'. (Now, the corresponding command has been added: <code>configure voip &gt; gateway advanced &gt; forking-handling</code> ).

## 2.29 Version 7.20A.254.733

This version includes new features only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.254.006.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.29.1 New Features

This section describes the new features introduced in this version.

#### 2.29.1.1 Cellular PIN Code Hidden from CLI Output

The cellular pin code is now displayed obscured in the output of CLI commands (e.g., `debug usb-3g cellular` and `show running-config`) and hidden in Syslog messages.

**Applicable Products:** MSBR.

#### 2.29.1.2 IKE Version 2 for ISAKMP

The device now supports Internet Key Exchange (IKE) Version 2 (in addition to the already supported IKEv1) for IPsec, which is configured for an Internet Security Association Key Management Protocol (ISAKMP) policy used for IPsec.

For example:

```
conf data
access-list ipsec permit ip 192.168.0.0 0.0.0.255 10.0.0.0
0.0.0.255
crypto isakmp policy 1
  enc aes 128
  authentication pre-share
  hash sha
  group 2
  lifetime 3600
ike v2
```

**Applicable Products:** MSBR.

### 2.29.1.3 Delay Time for Resending Failed SIP OPTIONS Keep-Alive Messages

The device can now be configured to wait a specific duration (in seconds) before re-sending a SIP OPTIONS keep-alive message to the SIP proxy server after receiving a failed SIP response from the previously sent keep-alive message. The feature is configured by the new ini file parameter, FailedOptionsRetryTime.

**Applicable Application:** All.

**Applicable Products:** All.

## 2.30 Version 7.20A.254.026

This version includes resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.254.006.
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
  - Mediant 800C MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-069 customers.

### 2.30.1 Resolved Constraints

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

**Table 40: Resolved Constraints for Version 7.20A.254.026**

Incident	Description
MSBR-8755	The Mediant 800 MSBR supports up to 10 SRDs. (Now, it supports up to 15.)
MSBR-8693	A new CLI command has been added -- configure voip > gateway digital settings > pstn-compatibility-profile (PstnCompatibilityProfile).
MSBR-8611	The device doesn't support the receipt of TR-069 redirect links that contain many characters. (Now, it supports up to 256 characters.)
MSBR-8599	The device doesn't save port mirroring configuration after device reset. (Now, it does if configured by the new command configure data > port-monitor-save-after-reset.)
MSBR-8568	The login password interval (WebPassChangeInterval) can now be configured through CLI using the new command web-password-change-interval.
MSBR-8550	No data transmission possible due to short connection timeout.
MSBR-8423	In some scenarios, the device doesn't periodically send the ACS inform messages.
MSBR-8398	The device uses a different TCP port (resets socket connection) from the one used for registering with the SIP proxy, for subsequent INVITE messages. As a result, calls fail.
MSBR-8376	The NTP server is unreachable when SNMP is disabled.
MSBR-8356	IPSec (PSK and RSA) on the device's (Mediant 500L) LTE interface doesn't function in branch office scenarios.

## 2.31 Version 7.20A.252.192

This version includes new features and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.252.023.
- This version is applicable to all MSBR devices.
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS

### 2.31.1 Resolved Constraints

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

**Table 41: Resolved Constraints for Version 7.20A.252.192**

Incident	Description
MSBR-9181	Changing an access VLAN (e.g., <code>switchport access vlan 11</code> to <code>12</code> ) on a gigabitethernet port (for example, <code>giga 1/4</code> ), causes a PPP session disconnect, which never comes up again.
MSBR-9203	Signal doesn't display in <code>show data cellular status</code> in QMI mode cellular.
MSBR-9246	Noise heard on FXO port.
MSBR-8930	Connectivity problems to the device due to memory leak.
MSBR-9091	Auto-provisioning not functioning due to DBS issue over IPv6.

## 2.32 Version 7.20A.252.183

This version includes new features and resolved constraints only.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.252.053.
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500C MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
  - Mediant 800C MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
- This version is not released for customers with T1 and SHDSL WAN flavors.

### 2.32.1 New Features

This section describes the new features introduced in this version.

#### 2.32.1.1 PPPoE Connection Process Started after Layer-2

The device's underlying interfaces (e.g., Gigabit Ethernet) using PPPoE can now be configured to start the establishment of the PPPoE connection after Layer 2 of the underlying interface (e.g., when cable connected), instead of waiting for the PPPoE process to start after Layer 3 of the underlying interface established.

This feature is enabled using the new CLI command, `layer_2_only`, as shown in the example below:

```
interface pppoe 0
  firewall enable
  napt
  underlying GigabitEthernet 0/0
  layer_2_only
  no shutdown
exit
```

**Applicable Products:** MSBR.

#### 2.32.1.2 Proxy Keep-Alive for Active Proxy Server Only

Up until now, when the device was enabled to send keep-alive SIP OPTIONS messages to proxy servers belonging to a Proxy Set, it sent them to all the proxies, regardless of the configured redundancy mode (parking or homing), configured by the 'Redundancy Mode' parameter. Now, the

device can be configured to regard the redundancy mode, using the new optional value **Using OPTIONS on Active Server** for the existing 'Proxy Keep-Alive' parameter in the Proxy Sets table:

- Parking mode: The device sends keep-alive OPTIONS messages only to the currently active proxy server.
- Homing mode: The device sends keep-alive OPTIONS messages to the currently active proxy server as well as to all servers (offline) with higher priority than the active server. Once a higher priority server comes online, the device stops sending OPTIONS to the previously active server and connects to the higher priority server. The device now sends keep-alive messages to it and all servers (offline) with higher priority.
- If the 'Redundancy Mode' parameter is not specified and the 'Proxy Load Balancing Method' parameter is configured to any value other than **Disable**, the device sends keep-alive OPTIONS messages to all active proxy servers (same behavior as if the Proxy Keep-Alive parameter was configured to **Using OPTIONS**).

**Applicable Products:** MSBR.

## 2.32.2 Resolved Constraints

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

**Table 42: Resolved Constraints for Version 7.20A.252.183**

Incident	Description
MSBR-8569	The device doesn't install static routes correctly in the routing table that were received through DHCP.
MSBR-8583	The device's IPv6 DNS relay doesn't function.
MSBR-8785	The device doesn't raise alarms correctly for busy out scenarios (e.g., on D-channel) for BRI interfaces.
MSBR-8803	The device's busy out behavior has been enhanced, and can use the Trunk Group Settings table or Tel-to-IP Routing table to determine busy out for a Trunk Group (configured by ISDNBusyOutBasedOnTable).
MSBR-8816	The device's ISDN screening indicator doesn't function correctly when it includes two calling party numbers in the outgoing ISDN Setup message for IP-to-Tel ISDN calls. To resolve this constraint the following parameters were added: ScreeningInd2ISDN1 and ScreeningInd2ISDN2.
MSBR-8889	For the Auto-Update mechanism, the device doesn't always retrieve the configuration file (CLIScriptUrl), because traffic is not going over the default route.
MSBR-8919	TLS handshake issues when the device resets and attempts to connect to the provisioning server for the Auto-Update mechanism.
MSBR-8928	The device cannot restrict IPv4/IPv6 addresses ( <i>access-list</i> ) from accessing its management interface.
MSBR-8949	The parameter 'Trunk Status Reporting Mode' (TrunkStatusReportingMode) doesn't function after a software upgrade.
MSBR-8955	When the device operates in Single Network Mode, the device doesn't attempt to resolve the FQDN of the manager hostname ( <i>manager-host-name</i> ) for SNMP trap destinations.
MSBR-8974	The device doesn't send IPv6 router solicitation for the fiber interface.

## 2.33 Version 7.20A.252.144

This version includes new features and resolved constraints.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.252.053.
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500C MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
  - Mediant 800C MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
- This version is not released for customers with T1 and SHDSL WAN flavors.

### 2.33.1 New Features

This section describes the new features introduced in this version.

#### 2.33.1.1 SNMP over IPv6 for Trap Destinations

The device now supports configuration of SNMP trap destinations (managers) as IPv6 addresses (in addition to already supported IPv4 addresses). This is configured by a new parameter/command:

- ini: SnmpTransportType
  - Web: 'SNMP Transport Type' (SNMP Community Settings page)
  - CLI: configure system > snmp settings > snmp-transport-type
- (Note that SNMP Trusted Managers still support only IPv4 addresses.)

**Applicable Products:** MSBR.

### 2.33.2 Resolved Constraints

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

**Table 43: Resolved Constraints for Version 7.20A.252.144**

Incident	Description
MSBR-8673	4G configuration for service provider isn't functioning.
MSBR-8845	The Trusted Managers table doesn't stay IPv4 independently of the SNMP Transport Type parameter.

Incident	Description
MSBR-8784	For TR-069, the device is missing Wi-Fi parameters.
MSBR-8743	When using DHCPv6 to assign a WAN IPv6 address to the device, any SSH session to the IPv6 address on the WAN freezes after about 30 seconds.
MSBR-8720	The device crashes with a HW Watchdog Signal 10 and 904.
MSBR-8714	TACACS servers and SIPS servers are not indexed 1 to N.
MSBR-8712	The device sends TR-069 RemoteAccess Boolean values to the ACS in upper case (e.g., "True"/"False") instead of all lower case.
MSBR-8696	The kernel route is sometimes missing after a device restart.
MSBR-8685	CLI configuration is missing "exit" on IPv6 dhcp server vendor-specific sub-option configurations.
MSBR-8684	Data Debug Capture files don't close properly after running the <b>debug capture data phy stop</b> command.
MSBR-8683	The device randomly crashes.
MSBR-8659	The device's private key for the TLS certificate doesn't "survive" a <b>write factory</b> .
MSBR-8628	The device's LAN interface periodically stops sending and receiving IPv6 packets.
MSBR-8622	The device fails to interpret line breaks ("\n") from the TR-069 Auto Configuration Server (ACS).
MSBR-8616	TR-069 IPv4 Inform message sends the device's Serial Number (not MAC address) for the WAN port (gig 0/0).
MSBR-8615	SIP SUBSCRIBE dialog sessions fail at random times.
MSBR-8601	NOTIFY messages sent to the WAN from the core SBC are not being processed by the MSBR SBC.
MSBR-8595	Access Point Name (APN) cannot be used without a username or password (device uses a default username/password even if not configured).
MSBR-8592	The console of the device fails to respond periodically.
MSBR-8591	The device's VoIP interface fails to bind correctly to the IPv6 WAN interface.
MSBR-8588	The default notification is not active for the TR-069 parameter Device.LAN.IPAddress.
MSBR-8586	The device doesn't support Device.Services.VoiceService.1.VoiceProfile.
MSBR-8585	The device is missing TR-069 parameters under Device.Services.VoiceService.1.VoiceProfile.1.SIP.
MSBR-8584	The device doesn't support some TR-069 VoiceProfile parameters after Device Activation on ACS.
MSBR-8573	The CLI <b>copy firmware</b> command incorrectly formats the Host header in IPv6 HTTP/S GET requests sent by the device.
MSBR-8502	The device doesn't have a TR-069 ACS provisioning sub-option when using IPv6 DHCP client on the WAN.
MSBR-8477	The device doesn't advertise concatenated Prefix Delegation (PD) prefixes on the LAN using stateful DHCPv6.

Incident	Description
MSBR-8417	The device forwards learned IPv6 DNS servers to only one DHCP server on a LAN VLAN.
MSBR-8401	There is no option to specify for the DHCPv6 client which prefix length to request for PD IA.
MSBR-8399	The DHCPv6 server doesn't advertise learned IPv6 DNS from the WAN.

## 2.34 Version 7.20A.252.078

This version includes new features and resolved constraints.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.252.053.
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
  - Mediant 800C MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
  - SHDSL
  - T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

### 2.34.1 Resolved Constraints

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

**Table 44: Resolved Constraints for Version 7.20A.252.078**

Incident	Description
MSBR-8499	When the device operates in Single Networking mode, it cannot send SIP messages to its own IP interface.
MSBR-8535	The BGP password is not encrypted in the CLI <b>show run</b> output.
MSBR-8540	When both copper WAN and fiber are connected, DHCP lease renewal from the copper WAN is not sent.

Incident	Description
MSBR-8553	Some voice parameters are in the ini file, but not in the CLI. The following CLI commands were added under configure voip > media voice: <ul style="list-style-type: none"> <li>■ <b>mf-transport-type</b> (MFTransportType)</li> <li>■ <b>mfr1-detector-enable</b> (MFR1DetectorEnable)</li> <li>■ <b>dtmf-detector-enable</b> (DTMFDetectorEnable)</li> </ul>
MSBR-8579	When the device connects to a third-party gateway, it doesn't receive GW Info from it.
MSBR-8590	The device tries to establish a TCP session using an internal IP address instead of the associated SIP Interface.
SBC-13728	The device locks (AdminState = 0) after a reset.

## 2.35 Version 7.20A.252.062

This version includes new features and resolved constraints.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.252.053.
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
  - Mediant 800C MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
  - SHDSL
  - T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

## 2.35.1 New Features

This section describes the new features introduced in this version.

### 2.35.1.1 Read-Only for LAN Guest-LAN Interface Page for Web End-Users

For Web End Users, the parameters on the LAN Interface page in the LAN Guest folder can be made read-only. In other words, this applies to the parameters under the LAN Interfaces Settings group and DHCP Settings group.

The feature is configured by the Administrator using the following new parameter:

- ini: EndUserAllowLanGuestSettings
- CLI: configure system > end-user > allow-lan-guest-settings enable|disable

**Applicable Products:** MSBR.

### 2.35.1.2 Hide and Read-Only for Multiple Subscriber Number Table for Web End-Users

For Web End-Users, the Voice folder (Monitor > Voice) can be hidden by the following new command:

```
(config-system)# end-user > allow-voice-settings enable|disable
```

This folder contains the Multiple Subscriber Number table and therefore, if the folder is hidden, the table will also be hidden.

In addition, when the folder is shown (enabled), the Administrator can apply the following security features to the table:

- 'User ID' parameter value is shown read-only
- The 'Password' parameter and value are hidden

This is configured by the following new parameter:

- ini: EndUserMsnSettings
- CLI: configure system > end user > allow-msn-authentication-settings enable|disable

**Applicable Products:** MSBR.

### 2.35.1.3 BFD for IPv6 BGP

The device supports Bidirectional Forwarding Detection (BFD) for a Border Gateway Protocol (BGP).

The feature includes the following new commands:

- BFD for a BGP AS (autonomous system) is enabled by a new command:

```
(config-data)# router bgp <as-id>
(bgp-router) # neighbor <neighbor ip> fall-over bfd interval
<value> min_rx <value> multiplier <value>
```

Where:

- *interval*: interval (in msec) for outgoing BFD messages. The interval is increased if the remote system requires it.
- *min\_rx*: minimum interval (in msec) between BFD messages. The remote system uses this interval for sending messages in case its interval is lower.
- *multiplier*: maximum number of packets that can be missed before the session status is considered down.

**Applicable Products:** MSBR.

### 2.35.1.4 MD5 Password for IPv6 BGP Sessions

An MD5 password can now be configured for IPv6 BGP network interfaces, using the following existing command:

```
(config-data)# router bgp 1
(conf-router)# neighbor 2010:18::200:200 password 0101010101
```

**Applicable Products:** MSBR.

### 2.35.1.5 OVOC Floating License Support via VRF

The device supports the Floating License application when communication with OVOC is through one of the device's VRF.

**Applicable Products:** MSBR.

## 2.35.2 Resolved Constraints

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

**Table 45: Resolved Constraints for Version 7.20A.252.062**

Incident	Description
MSBR-1486	IPv6 PD (Prefix Delegation) doesn't function with Stateful DHCPv6 mode.
MSBR-8218	WAN SIP address gets wrong loopback IP address as source.
MSBR-8275	Vulnerability in shell command injection in sysupgrade.sh in .cmp firmware file.
MSBR-8328	In some scenarios, a problem in configuration is experienced when it is loaded using the Auto-Update mechanism.
MSBR-8340	Cross scripting vulnerability on JSON pages in Web interface.
MSBR-8341	Console accessible via Telnet (exposing security risk).
MSBR-8347	The login password cannot be changed by the End User.
MSBR-8356	IPSec via LTE is not functioning on the cellular interface.
MSBR-8380	The device crashes (resets) when changing MTU on the cellular interface.
MSBR-8390	High data CPU experienced during 200 concurrent voice calls.
MSBR-8398	The device changes the TCP port and resets the socket connection.
MSBR-8409	The Save button in the Web interface is erroneously displayed in red after a Startup Script file is loaded successfully.
MSBR-8438	For DHCPv6, there is no option to configure a DHCPv6 server on the LAN to advertise IPv6 NTP servers dynamically learned on the WAN,
MSBR-8445	When the device uses IPv6, it connects LAN media streams to an internal IPv6 address, which causes incorrect SBC signaling on the device.
MSBR-8446	For DHCPv6, NTP servers advertised on DHCP Option 31 instead of Option 56.

## 2.36 Version 7.20A.250.028

This version includes new features and resolved constraints.



- This MSBR version corresponds to SBC-Gateway Version 7.20A.250.012.
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
  - Mediant 800C MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
  - SHDSL
  - T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

### 2.36.1 New Features

This section describes the new features introduced in this version.

#### 2.36.1.1 WAN Status and Performance Monitoring Display

The device's Web interface now displays the following WAN interface information:

- WAN status (Monitor menu > Monitor tab > Data Status folder > Network Status)
- WAN statistics (Monitor menu > Monitor tab > Data Status folder > Network Statistics)
- WAN performance statistics (Monitor menu > Monitor tab > Data Status folder > Network Performance Monitors)

**Applicable Products:** All.

#### 2.36.1.2 Copper WAN through SFP

The small form-factor pluggable (SFP) optical module, typically used for WAN fiber interface, can also be used for WAN copper interface. This new feature provides support by the device's management interfaces to display the duplex mode (full or half) of this WAN copper connection type.

**Applicable Products:** All.

### 2.36.1.3 Display of DSL Transmission Statistics

A new CLI command has been introduced that displays historical statistics of upstream and downstream transmission properties (speed, power, SNR margin and attenuation) of the DSL interface:

```
show data interface dsl <Slot>/<Port> history
```

For example:

```
# sh d in dsl 0/2 history
Time: 03/01/2018 11:11:03
Downstream: Actual speed 112636000, power 13.9, SNR margin 26.2,
Attenuation 0.1
Upstream: Actual speed 83680000, power 8.1, SNR margin 5.3,
Attenuation 1.6
Time: 03/01/2018 11:09:53
Downstream: Actual speed 112636000, power 13.9, SNR margin 25.9,
Attenuation 0.1
Upstream: Actual speed 83680000, power 8.1, SNR margin 5.2,
Attenuation 1.6
```

**Applicable Products:** All.

### 2.36.1.4 DHCPv4 Option 82 Support

The device supports DHCP Option 82. When this feature is enabled and a DHCP relay agent forwards client-originated DHCP packets containing Option 82 to the device (acting as a DHCP server), the device "echos" the information of Option 82 back to the DHCP client. The feature is enabled for the interface on which the DHCPv4 server is configured, using the following new CLI command:

```
ip dhcp-server option82
```

**Applicable Products:** All.

### 2.36.1.5 LTE WWAN Support

The device supports Long-Term Evolution (LTE) wireless WAN (WWAN). This is supported by an integrated 4G LTE cellular modem, two cellular antennas, and a slot for inserting a Subscriber Identity Module (SIM) card to connect with the 4G cellular network.

**Applicable Products:** Mediant 500L MSBR.

### 2.36.1.6 QoS on L2TP Interfaces

The device supports the configuration of Quality of Service (QoS) on Layer 2 Tunneling Protocol (L2TP) interfaces.

**Applicable Products:** All.

### 2.36.1.7 TR-069 Annex F

The device supports TR-069 Annex F. Annex F is relevant when the Gateway and the Device (CPE) are managed by the same ACS. According to Annex F, the Device and the Gateway (to which the Device is connected) pass their private information to one another, and the ACS identifies the Device as being under the Gateway. The MSBR can be the Device or the Gateway. When the MSBR uses TR-181 Data Model, it functions as the Device; when the MSBR uses TR-098 Internet Gateway Device, it functions as the Gateway.

As a result of this feature, the following new TR-069 objects and parameters are now supported:

- Device.GatewayInfo object (TR-181 Device Data Model)
- ManageableDeviceNumberOfEntries parameter to InternetGatewayDevice.ManagementServer. object (TR-098 Device Data Model)
- nternetGatewayDevice.ManagementServer.ManageableDevice object and its parameters (TR-098 Device Data Model)

**Applicable Products:** All.

## 2.36.2 Resolved Constraints

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

**Table 46: Resolved Constraints for Version 7.20A.250.028**

Incident	Description
MSBR-1434	The subnet mask is not displayed in the <b>show data ip interface</b> command when the IP address mode is DHCP.
MSBR-1447	In Single Network Mode, Debug Recording packets show the internal WAN IP address instead of the WAN interface IP address.
MSBR-7947	Configuration is not saved to flash under MSN configuration in the End User Web GUI.
MSBR-8072	The device doesn't create a default route when using DHCP IPv6.
MSBR-8100	The device crashes upon a JSON output of configuration through TR-069.
MSBR-8141	Configuration cannot be backed up in OVOC when VRF is configured on the WAN interface.
MSBR-8212	When an SNMP trap destination is configured, it appears twice in the CLI script.
MSBR-8248	The device reboots after running the <b>show run</b> command through TR-069.
SBC-9536 (VI-155449)	When the device operates with the CRP application, it has invalid default configuration, which prevents the CRP from being configured correctly (IP Group and IP-to-IP Routing tables).

## 2.37 Version 7.20A.202.307

This version includes new features and resolved constraints.



- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
  - Mediant 800C MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
  - SHDSL
  - T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

### 2.37.1 New Features

New features introduced in this version include the following:

- Support for an integrated LTE modem.
- New debug log commands:
  - Displays the device's syslog of exceptions:  
`debug exception-syslog-history`
  - Displays the device's syslog of resets:  
`debug reset-syslog-history`
- End-User Web Interface:
  - DHCP Settings has been moved to the LAN Interface page.
  - Configuration of multiple PPPoE interfaces (configure system > end-user > wan-if pppoe auto).
  - Display of the connected (active) PPPoE interface, even when multiple PPPoE interfaces have been configured.
  - New configuration table has been added "Multiple Subscriber Number" (Voice folder > Multiple Subscriber Number) for FXS and BRI interfaces.

## 2.37.2 Resolved Constraints

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

**Table 47: Resolved Constraints for Version 7.20A.202.307**

Incident	Description
152228	In the End User Web interface, the pages under the LAN Guest folder display incorrect DHCP information.
153838	A CLI command has been added ( <b>ipv6 dhcp-client prefix-len-128</b> ), which changes the prefix length of a received IPv6 address through DHCP to 128 bit (instead of the default 64). This has been done to comply with RFC 5942.
153921	In the End-User Web interface, the login password is not saved after a device reset.
153977	DNS resolution with NAPTR is not functioning.
153996	In the End-User Web interface, an error occurs when assigning a static IP address for the WAN Backup interface.
154240	When the WAN cable is unplugged and then plugged in again, no connection is experienced to the management interfaces (HTTP, telnet, etc..).
154292	After a Media Realm is configured, it cannot be edited.
154296	In the End-User Web interface, the Apply button doesn't function for LAN Guest interfaces.
154769	TLS configuration is not saved to the device's CLI.
154859	In IPv6 PD configuration, the default route to the LAN subnet appears in the Routing table to its own address.
154912	The <b>show run</b> command displays an unwanted DynDNS configuration after each device reset.
155104	After upgrading from Version 6.8 to 7.20A.202, the device reports a different hardware version through TR-069.
155106 / 154404 / 154463	Uploading the CLI Script file through the Web interface fails and only part of the script is applied. This occurs when some of the configuration is not accepted.

## 2.38 Version 7.20A.202.112

This version includes new features and resolved constraints.



- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
  - Mediant 800C MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
  - SHDSL
  - T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

### 2.38.1 New Features

New features introduced in this version include the following:

- Static WAN IP address configuration through the End User Web interface.
- The `InternetGatewayDevice.Time` object is now supported for TR-098.
- The `InternetGatewayDevice.Time` object is now supported for TR-069, allowing NTP to be enabled or disabled. The `Device.Time` object is now supported for TR-069.
- The Debug Capture feature now allows the naming of the captured files and sending them to specific folders on TFTP servers.
- Support for DHCPv4 Option 66 to obtain the TFTP server name and Option 67 to obtain the configuration file name, when the MSBR is a DHCP client. The output of the CLI commands **show system alarms** and **show system alarms-history** can now be displayed in JSON format, using the following new CLI command:

```
output-format json
```

The output is returned to plain text format using the following command:

```
output-format plain
```

## 2.38.2 Resolved Constraints

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

**Table 48: Resolved Constraints for Version 7.20A.202.112**

Incident	Description
141040	The settings of the <b>web-restrict</b> CLI command does not save after a device reset.
142368	Rate counters don't show fast-path and non fast-path traffic.
148811	WiFi "Krack" vulnerability: PTK rekeying to generate a new ANonce.
148909	Hostname resolution for VRFs is not supported. Access list is not binding to a single VRF. Hostname resolution for IPv6 is not supported. Access list FQDN does not support multiple VRFs.
148983	Automatic switching from EFM to ATM for SHDSL interfaces does not function.
148992	Access list IPv6 rule has no 'precedence' option.
149652	The Auto Provisioning process doesn't complete configuration file load.
150110	Bind to WAN - the internal LAN IP address appears in the <b>show run data</b> output (and should not).
150432	The <b>show data interface pppoe</b> CLI command does not show the subnet mask in its output.
150518	IPv6 cannot be enabled or disabled through TR-181.
150707	In TR-069, no support for MTU fragmentation.
150755	The NTP server IP address cannot be obtained from DHCP.
150763	The device doesn't renew its' IP address after a DHCP server configuration change.
150904	The device doesn't bind VLAN 100 and higher in Single Networking Mode.
150931	The device doesn't accept BGP configuration of peers in peer-group.
150932	CLI <b>show</b> commands for the Wi-Fi interface do not display "connected" status.
150963	Multiple VRRP IDs (per interface) doesn't support DHCPv4.
151017	The <b>copy</b> command fails first time with the error "(6) Could not resolve host".
152270	The configuration by the <b>coders-and-profiles</b> command is displayed in the wrong location in the CLI script, which causes an error when applying the script to the device.
152395	The <b>show data ip igmp proxy groups</b> command displays an error.
152875	A WAN IPv6 cannot be assigned to a Media Realm in the Web interface.
152930	When DHCPv4 is configured with a static IPv6 address, the <b>show data ipv6 interface brief</b> command does not display IPv6 status properly. DHCP client configuration on WAN copper disables IPv6 protocol.
152974	The license for the Zero Configuration feature is not retained after a hardware (button) reset.
152984	After clicking the Edit button in the SIP Interfaces table, the network interface doesn't appear even though it is configured.

Incident	Description
153155	Debug Recording cannot be sent to the WAN over a non-default VRF.
153235	For the configuration of <b>sip-definition account</b> , no space appears before "obscured" in the obscured password (e.g., password /cnHyzQwOzo9NjY/OA==obscured").
153545	The <b>show data interface &lt;Interface Name&gt;</b> command does not show the subnet mask when the IP address is obtained through DHCP.

## 2.39 Version 7.20A.200.038

This version includes new features and resolved constraints.



- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
  - SHDSL
  - T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

### 2.39.1 New Features

New features introduced in this version include the following:

- DNS lookup queries for a specific VRF. To support this feature, the following new command has been added:
 

```
nslookup [Hostname] source data vrf [VRF Name]
```
- Configuration of a specific protocol bind (snmp|http|https|telnet|ssh) per management server.
 

```
bind source-address interface [Interface] management-servers [http|https|snmp|ssh|telnet]
```
- Support for multicast in VRFs, using the new 'pim' command:
 

```
ip vrf <VRF Name> enable pim
```

- Configuration of Gratuitous ARP (GARP) per interface with timer, using the following new commands:

```
(config-data)# garp timer <Seconds 1-3600, Default 60>
(conf-if-GE 0/0)# garp enable | no garp enable
```

The feature is applicable only to Gigabit and fiber WAN interface types (VLAN 1 only).

- Support for Y.1731.
- Loading License Key file through CLI (from HTTP, HTTPS, FTP, TFTP, or NFS server), using the following new command:

```
# copy feature-key from [URL]
```

- Web-based management interface (Web End-User) for end users, allowing basic configuration, for example, LAN ports settings, WAN ports settings, Wi-Fi settings, and port forwarding settings. For more information, refer to the *Mediant MSBR Basic System Setup CLI Configuration Guide*.
- Configuration of maximum path for BGP, using the following new command:

```
(config-data)# router bgp [AS Number] maximum-paths [Number]
```

## 2.39.2 Resolved Constraints

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

**Table 49: Resolved Constraints for Version 7.20A.200.038**

Incident	Description
147996	Incorrect order of SNMP configuration through CLI prevents configuration to be applied.
148592	For TR-069 management, digest authentication messages are sent in the wrong format.
149101	When the WAN interface is configured on VRF, the Auto-Update and copy features do not function if DNS resolution is required.

## 2.40 Version 7.20A.154.078

This version includes new features and resolved constraints.



- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - A/VDSL ISDN
  - A/VDSL POTS
  - SHDSL
  - T1 WAN
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

### 2.40.1 New Features

New features introduced in this version include the following:

- Support for DNS with VRRP.
- Support for disabling the DHCP "dynamic" mode. When the command **no ip dhcp-server dynamic** is run, the DHCP server only answers to statically configured hosts.
- Support for the ZTE MF833V cellular dongle.

### 2.40.2 Resolved Constraints

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

**Table 50: Resolved Constraints for Version 7.20A.154.078**

Incident	Description
146911	IPSec does not function when <b>ipsec access list destination</b> is set to "any".
147776	DHCP client does not renew its DHCP lease if the device undergoes an unplanned reset. DHCP lease renewal is possible only if the device is restarted during DHCP client lease time.
147955	Under some conditions, the ini file cannot be loaded using the Automatic Update mechanism (IniFileURL parameter).
148218	When VRRP backup becomes operational, it erases dynamic leases. To prevent this, the VRRP backup device uses ARP to keep the lease of active IPs.

## 2.41 Version 7.20A.154.061

This version includes new features and resolved constraints.



- This version is based on MSBR Version 6.80A.347.001 (released in July 2017). In other words, all data capabilities of this MSBR 7.2 version are fully aligned to the above mentioned 6.8 version (with a few exceptions, as listed in the document *MSBR Data Feature Additions from 6.8 to 7.2*).
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - VDSL ISDN
  - VDSL POTS
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

### 2.41.1 Resolved Constraints

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

**Table 51: Resolved Constraints for Version 7.20A.154.061**

Incident	Description
146955	Device crashes on rare occasions when SNMP is used to GET QoS information.
147706	AAA TACACS configuration is not saved to configuration.
147732	Issue with saving configuration of Access List with SNMP community.
147776	The device's DHCPv4 server now supports fast revival after reset, using DHCPREQUEST messages.
147781	TR-181 operations cause the device's CLI to freeze.

## 2.42 Version 7.20A.154.025

This version includes new features and resolved constraints.



- This version is based on MSBR Version 6.80A.347.001 (released in July 2017). In other words, all data capabilities of this MSBR 7.2 version are fully aligned to the above mentioned 6.8 version (with a few exceptions, as listed in the document *MSBR Data Feature Additions from 6.8 to 7.2*).
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - VDSL ISDN
  - VDSL POTS
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.

### 2.42.1 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.
- 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*.
- 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.

## 2.42.2 Resolved Constraints

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

**Table 52: Resolved Constraints for Version 7.20A.154.025**

Incident	Description
138373	In some cases, the Huawei 4G USB stick does not receive an IP address after a device reset.
139561	New command has been added to view DDNS status ( <b>show data ddns</b> ).
141714	Unable to display L2 hosts in the TR hosts table (but now possible (InternetGatewayDevice.LANDevice.{i}.Hosts.Host.{i})).
142257	No option to configure dynamic learning of IPv6 NTP addresses on a PPPoE interface.
142487	Configuration of GRE tunnel without a source interface is not allowed in order to prevent a mismatch with the other side of the tunnel.
142488	The configuration <b>qos match-map</b> input "NAME" VLAN 4001 appears as <b>qos match-map</b> input "NAME" internal-LAN when the <b>show</b> command is run.
142836	LAN-based host feature doesn't show all hosts.
142981	The RTP port is different than that advertised in the SDP body of the SIP 200 OK.
143282	For DHCPv6 NTP, the <b>ipv6 dhcp-client ntp-server</b> command is not displayed by the <b>show run</b> command under the PPPoE interface.
143933	Upload of files through TR-069 via HTTPS fails.
144063	Single Network Mode - no RTP between local extensions (FXS and IP Phone / FXS and FXS) when using the loopback interface.
144064	Single Network Mode - no RTP between local extensions (FXS and IP Phone) when using VRF.
144197	Configuring "cellular-backup" in the backup-group when IPSec crypto map is configured, causes the cellular interface to remain in non-operational mode.
144486	TR-069 change of PPPoE credentials terminates too early and causes transaction error.
144974	The <b>show run</b> command does not display IPSec, PFS or metric parameters under the crypto map if the crypto map is not associated with the interface.
145066	The OSPF <b>max-metric router-lsa</b> command has no effect when the OSPF process is closed.
145342	TR-069 provisioning code is lost after device reset and reverts to default ("VOIP.DATA").
145463	Single Network Mode – ringback tone from PRT file is not played.
145580	InternetGatewayDevice.LANDevice.1.LANEthernetInterfaceConfig.4 is not displayed in the TR-069 ACS.
145636	The cellular, dynamic option driver is not saved after a device reset.
146255	Statically configured IPv6 route does not function when a dynamic IP address is configured.
146327	IPv6 addresses on the PPPoE interface does not function with IPv4 addresses.
146430	PPPoE interface cannot be underlying to an ATM interface.
146575	QoS calibration on VDSL/EFM lines.

## 2.43 Version 7.20A.150.004

This is the initial version of the 7.2 Software Release for the MSBR product series.



- This version is based on MSBR 6.8 Version **6.80A.335.005**, released in March 2017. In other words, all data capabilities of this MSBR 7.2 version are fully aligned to the above mentioned 6.8 version (with a few exceptions, as listed in the document *MSBR Data Feature Additions from 6.8 to 7.2*).
- This version is introduced as a controlled release and is not backward compatible with Version 6.8 concerning some of the management interfaces and mainly the command-line interface. For more details, please refer to the relevant documents released together with this document.
- This version is not recommended for migrating existing MSBR fleets from Version 6.8, but rather for new customers, and for existing customers for evaluation and preparation for future upgrades from Version 6.8.
- If the MSBR device is running a software version that is earlier than 6.80A.286.002, to upgrade the device to Version 7.2, the device must first be upgraded to Version 6.80A.286.002 and only then upgraded to Version 7.2.
- This version is applicable only to the following MSBR devices:
  - Mediant 500 MSBR
  - Mediant 500L MSBR
  - Mediant 800B MSBR
- This version is applicable only to the following physical WAN interfaces:
  - Copper
  - Cellular
  - Fiber
  - VDSL ISDN
  - VDSL POTS
- This version is not released for customers with T1 and SHDSL WAN flavors.
- This version is not released for TR-181 customers.
- This version is compatible with AudioCodes EMS/SEM Version 7.2.3083.

### 2.43.1 Known Constraints

This section lists known constraints.

**Table 53: Known Constraints in Version 7.20A.150.004**

Incident	Description
-	TR-181 is not supported. <b>Applicable Products:</b> MSBR.
141108	Running speed tests through TR-069 is not supported.
143283	DHCPv6 NTP "Current Dynamic NTP Server" information is not displayed in the CLI when running the CLI command <b>show system ntp-status</b> . <b>Applicable Products:</b> MSBR.
143295	The CL command <b>debug reset-history</b> saves only the last three reset reasons. <b>Applicable Products:</b> MSBR.
144076	The CLI command <b>show data interfaces cellular 0/0</b> fails. <b>Applicable Products:</b> MSBR.

---

Incident	Description
144181	The device does not support 802.1X. <b>Applicable Products:</b> MSBR.
144214	The CLI command <b>debug capture data physical clear</b> is not supported. <b>Applicable Products:</b> MSBR.

## 3 Capacity

This section provides capacity figures per product.

### 3.1 SIP Signaling and Media Capacity

The following below lists maximum, concurrent SIP signaling sessions, concurrent media sessions, and registered users per product.

**Table 54: SIP Signaling and Media Capacity per MSBR Product**

Product	Signaling Capacity		Media Sessions			
	SIP Sessions	Registered Users	Session Type	RTP Sessions	SRTP Sessions	Detailed Media Capabilities
Mediant 500 MSBR	60	500	Hybrid	60	60	See Table 55
			GW-Only	30	30	Transcoding: n/a
Mediant 500L MSBR	60	200	Hybrid	60	60	See Table 56
			GW-Only	8	8	Transcoding: n/a
Mediant 500Li MSBR	30	100	Hybrid	30	15	GW & Transcoding: See Table 58
			GW-Only	8	8	
Mediant 800A MSBR	60	200	Hybrid	60	60	GW & Transcoding: See Table 59
Mediant 800B MSBR	60	500	Hybrid	60	60	GW & Transcoding: See Table 59
Mediant 800C MSBR	150	600	Hybrid	150	100	GW & Transcoding: See Table 59
MediaPack 50x (502 / 504 / 508)	30	100	Hybrid	30	15	GW & Transcoding: See Table 62
			GW-Only	8	8	
MediaPack 5xx (516 / 524 / 532)	30	100	Hybrid	30	15	GW & Transcoding: See Table 62
			GW-Only	32	32	



- The figures listed in the table 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.
- "GW" refers to Gateway functionality.
- The "SIP Sessions" column displays the maximum concurrent signaling sessions for both SBC and Gateway (when applicable). Whenever signaling sessions is above the maximum media sessions, the rest of the signaling sessions can be used for Direct Media.
- The "Session Type" column refers to Gateway-only sessions, SBC-only sessions, or Hybrid sessions which is any mixture of SBC and Gateway sessions under the limitations of Gateway-only or SBC-only maximum values.
- The "RTP Sessions" column displays the maximum concurrent RTP sessions when all sessions are RTP-RTP (for SBC sessions) or TDM-RTP (for Gateway sessions).
- The "SRTP Sessions" column displays the maximum concurrent SRTP sessions when all sessions are RTP-SRTP (for SBC sessions) or TDM-SRTP (for Gateway sessions).

- The "Registered Users" column displays the maximum number of users that can be registered with the device. This applies to the supported application (SBC or CRP).
- 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 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 G.729, one signaling resource, one media session resource, and one transcoding session resource is used.

## 3.2 Detailed Capacity

This section provides detailed capacity figures.

### 3.2.1 Mediant 500 MSBR

The channel capacity and SBC session capacity for Mediant 500 MSBR are shown in the table below.

**Table 55: 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	30/36
4 x BRI	8	52
1/2/3 x BRI	2/4/6	58/56/54
4 x FXS or 4 x FXO	4	56
FXS, FXO, and/or BRI, but none in use	0	60



- 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.

### 3.2.2 Mediant 500L MSBR

The channel capacity and SBC session capacity for Mediant 500L MSBR are shown in the table below.

**Table 56: 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



- 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.

### 3.2.3 Mediant 500Li MSBR

The DSP channel capacity and SBC session capacity for Mediant 500Li is shown in the table below.

**Table 57: Mediant 500Li MSBR Capacity per PSTN Assembly and Capabilities**

Telephony Interface Assembly	DSP Channels Allocated for PSTN	Max. SBC Sessions
2 x BRI and 2 x FXS	6	24
4 x BRI	8	22
8 x FXS	8	22
FXS, FXO, and/or BRI, but not in use	0	30

**Table 58: Mediant 500Li MSBR Transcoding Capacity**

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions						Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities					To Profile		To Profile
		Detectors	IPM	G.722	AMR WB	SILK NB / ILBC	SILK WB		1
FXS and/or BRI, but <b>not</b> in use	0	-	√	-	-	-	6	6	30



- 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.

### 3.2.4 Mediant 800 MSBR

This section provides DSP channel capacity and SBC session capacity for Mediant 800 MSBR.

#### 3.2.4.1 Mediant 800/B MSBR

The DSP channel capacity and SBC session capacity for Mediant 800/B MSBR are shown in the table below.

**Table 59: 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 800A	Mediant 800B
		AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB	SILK-WB	Opus-NB	Opus-WB	V.150.1					
2 x E1/T1	60/48	-	-	-	-	-	-	-	3/15	2/13	-	0/12	0/12
2 x T1	48	-	-	-	-	-	-	√	11	9	-	12	12
1 x E1/T1	38/32	-	-	-	-	-	-	-	22/28	18/22	-	22/28	22/28
8 x FXS/FXO Mix	38/32	-	-	√	-	-	-	-	8/12	7/11	-	22/28	22/28
1 x E1/T1	30/24	-	-	√	-	-	-	√	14/18	12/16	-	30/36	30/36
1 x E1 4 x BRI	38	-	-	-	-	-	-	-	22	18	-	22	22
1 x E1& 4 x FXS	34	-	-	-	-	-	-	-	26	21	-	26	26
2 x E1 4 x FXS	64	-	-	-	-	-	-	-	0	0	-	0	0
4 x BRI 4 x FXS 4 x FXO	16	-	-	-	-	-	-	-	5	4	-	44	44
8 x BRI 4 x FXS	20	-	-	-	-	-	-	-	1	1	-	40	40
8 x BRI	16	-	-	-	-	-	-	-	5	4	-	44	44
12 x FXS	12	-	-	√	-	-	-	√	3	3	-	48	48
4 x FXS 8 x FXO	12	-	-	√	-	-	-	-	3	3	-	48	48
8 x FXS 4 x FXO	12	-	-	√	-	-	-	-	3	3	-	48	48
4 x BRI 4 x FXS	12	-	-	√	-	-	-	-	3	3	-	48	48

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 800A	Mediant 800B
		AMR-NB / G.722	AMR-WB (G.722.2)	SILK-NB	SILK-WB	Opus-NB	Opus-WB	V.150.1					
4 x FXS	8	-	-	-	-	-	-	-	7	5	6	52	52
4 x FXO	8	-	-	√	-	-	-	-	6	6	-	52	52
4 x BRI	8	-	-	-	-	-	-	-	7	5	6	52	52
	8	-	-	√	-	-	-	-	6	6	-	52	52
1/2/3 x BRI	2/4/6	-	-	-	-	-	-	-	17/15/14	14/13/11	-	58/56/54	58/56/54
	2/4/6	-	-	√	-	-	-	-	11/10/8	10/8/7	-	58/56/54	58/56/54
4 x FXS or 4 x FXO	4	-	-	√	-	-	-	√	10	8	-	56	56
	4	√	-	-	-	-	-	-	12	10	4	56	56
	4	-	-	√	-	-	-	-	6	6	4	56	56
	4	-	√	√	-	-	-	-	4	4	4	56	56
	4	-	√	√	√	-	-	-	3	3	4	56	56
	4	-	-	-	-	√	-	-	1	0	4	56	56
	4	-	-	-	-	-	√	-	0	0	3	56	56
FXS, FXO, and/or BRI, but not in use	0	-	-	-	-	-	-	-	19	16	-	60	60



- **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 (A / AB), 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.

### 3.2.4.2 Mediant 800C MSBR

The DSP channel capacity and SBC session capacity for Mediant 800C MSBR are shown in the table below.

**Table 60: Mediant 800C MSBR Channel Capacity per PSTN and Capabilities**

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions						Max SBC Sessions
		From Profile 2	From Profile 2 with SILK NB/iLBC	From Profile 2 with Opus NB	From Profile 2 with Opus WB	To Profile 1	To Profile 2	
4 x E1/T1 + 4 x FXS	124/100	√	-	-	-	2/23	2/18	26/50
2 x E1/T1 + 4 x FXS	64/52	√	-	-	-	0/10	0/8	86/98
Not in use	-	√	-	-	-	114	96	150
		-	√	-	-	78	66	150
	-	-	-	√	-	54	48	150
	-	-	-	-	√	42	42	150



- *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 (A / AB), 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.

## 3.2.5 MediaPack 5xx

### 3.2.5.1 MediaPack 50x (MP-502, MP-504 and MP-508)

The DSP channel capacity and SBC session capacity for MediaPack 50x is shown in the table below.

**Table 61: MP-502, MP-504 and MP-508 Capacity per PSTN Assembly and Capabilities**

Telephony Interface Assembly	DSP Channels Allocated for PSTN	Max. SBC Sessions
MP-502 2 x FXS	2	28
MP-504 4 x FXS	4	26
MP-508 8 x FXS	8	22

**Table 62: MP-502, MP-504 and MP-508 Transcoding Capacity**

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions					To Profile 1	To Profile 2	Max. SBC Sessions
		From Profile 2 with Additional Advanced DSP Capabilities							
		IPM Detectors	G.722	AMR WB	SILK NB / iLBC	SILK WB			
Not in use	0	-	-	-	-	-	6	6	30
		-	√	-	-	-	6	6	30



- For Profile 1 to Profile 1 using G.711, the maximum number of transcoding sessions is 10.
- 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.

### 3.2.5.2 MediaPack 5xx (MP-516, MP-524, and MP-532)

The DSP channel capacity and SBC session capacity for MediaPack 5xx is shown in the table below.

**Table 63: MP-516, MP-524, and MP-532 Capacity per PSTN Assembly and Capabilities**

Telephony Interface Assembly	DSP Channels Allocated for PSTN	Max. SBC Sessions
MP-516	16	14
MP-524	24	6
MP-532	32	0

**Table 64: MP-516, MP-524, and MP-532 Transcoding Capacity**

Telephony Interface Assembly	DSP Channels Allocated for PSTN	SBC Transcoding Sessions						Max. SBC Sessions	
		From Profile 2 with Additional Advanced DSP Capabilities					To Profile		To Profile
		IPM Detectors	G.722	AMR WB	SILK NB / iLBC	SILK WB	1		2
Not in use	0	-	-	-	-	-	20	16	30
		-	√	-	-	-	18	14	30
		-	-	-	√	-	13	11	30



- 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.

### 3.3 Session Capacity per Feature

The table below lists maximum capacity per feature, per product:

**Table 65: Maximum Capacity per Feature for MSBRs**

Product	SIPREC Sessions	TLS Connections
Mediant 500Li	10	50
Mediant 500L MSBR	30	50
Mediant 500 MSBR	30	50
Mediant 800B MSBR	30	50
Mediant 800C MSBR	30	-
MediaPack 5xx	10	50



The figures in the table above for SIPREC capacity assume that there are no other concurrent, regular (non-SIPREC) voice sessions.

## 4 Supported SIP Standards

This section lists SIP RFCs and standards supported by the device.

### 4.1 Supported SIP RFCs

The table below lists the supported RFCs.

**Table 66: Supported RFCs**

RFC	Description	Gateway	SBC
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2	√	√
RFC 2806	URLs for Telephone Calls	√	√
draft-choudhuri-sip-info-digit-00	SIP INFO method for DTMF digit transport and collection	√	√
draft-ietf-bfcpbis-rfc4583bis-12	Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams	×	√ (forwarded transparently)
draft-ietf-sip-connect-reuse-06	Connection Reuse in SIP	√	√
draft-ietf-sipping-cc-transfer-05	Call Transfer	√	√
draft-ietf-sipping-realtimifax-01	SIP Support for Real-time Fax: Call Flow Examples	√	√ (forwarded transparently)
draft-ietf-sip-privacy-04.txt	SIP Extensions for Network-Asserted Caller Identity using Remote-Party-ID header	√	√
draft-johnston-sipping-cc-uui-04	Transporting User to User Information for Call Centers using SIP	√	√ (forwarded transparently)
draft-levy-sip-diversion-08	Diversion Indication in SIP	√	√
draft-mahy-iptel-cpc-06	The Calling Party's Category tel URI Parameter	√	√ (forwarded transparently)
draft-mahy-sipping-signaled-digits-01	Signaled Telephony Events in the Session Initiation Protocol	√	√
draft-sandbakken-dispatch-bfcp-udp-03	Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport	×	√ (forwarded transparently)
ECMA-355, ISO/IEC 22535	QSIG tunneling	√	√ (forwarded transparently)
RFC 2327	SDP	√	√
RFC 2617	HTTP Authentication: Basic and Digest Access Authentication	√	√
RFC 2782	A DNS RR for specifying the location of services	√	√
RFC 2833	Telephone event	√	√

RFC	Description	Gateway	SBC
RFC 2976	SIP INFO Method	√	√
RFC 3261	SIP	√	√
RFC 3262	Reliability of Provisional Responses	√	√
RFC 3263	Locating SIP Servers	√	√
RFC 3264	Offer/Answer Model	√	√
RFC 3265	(SIP)-Specific Event Notification	√	√
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)	√	×
RFC 3311	UPDATE Method	√	√
RFC 3323	Privacy Mechanism	√	√
RFC 3325	Private Extensions to the SIP for Asserted Identity within Trusted Networks	√	√
RFC 3326	Reason header	√	√ (forwarded transparently)
RFC 3327	Extension Header Field for Registering Non-Adjacent Contacts	√	×
RFC 3361	DHCP Option for SIP Servers	√	×
RFC 3362	Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration	√	√
RFC 3372	SIP-T	√	√ (forwarded transparently)
RFC 3389	RTP Payload for Comfort Noise	√	√ (forwarded transparently)
RFC 3420	Internet Media Type message/sipfrag	√	√
RFC 3455	P-Associated-URI	√	√ (using user info \ account)
RFC 3489	STUN - Simple Traversal of UDP	√	√
RFC 3515	Refer Method	√	√
RFC 3550	RTP: A Transport Protocol for Real-Time Applications	√	√
RFC 3578	Interworking of ISDN overlap signalling to SIP	√	×
RFC 3581	Symmetric Response Routing - rport	√	√
RFC 3605	RTCP attribute in SDP	√	√ (forwarded transparently)
RFC 3608	SIP Extension Header Field for Service Route Discovery During Registration	√	×
RFC 3611	RTCP-XR	√	√
RFC 3665	SIP Basic Call Flow Examples	√	√

RFC	Description	Gateway	SBC
RFC 3666	SIP to PSTN Call Flows	√	√ (forwarded transparently)
RFC 3680	A SIP Event Package for Registration (IMS)	√	×
RFC 3711	The Secure Real-time Transport Protocol (SRTP)	√	√
RFC 3725	Third Party Call Control	√	√
RFC 3824	Using E.164 numbers with SIP (ENUM)	√	√
RFC 3842	MWI	√	√
RFC 3891	"Replaces" Header	√	√
RFC 3892	The SIP Referred-By Mechanism	√	√
RFC 3903	SIP Extension for Event State Publication	√	√
RFC 3911	The SIP Join Header	Partial	×
RFC 3960	Early Media and Ringing Tone Generation in SIP	Partial	√
RFC 3966	The tel URI for Telephone Numbers	√	√
RFC 4028	Session Timers in the Session Initiation Protocol	√	√
RFC 4040	RTP payload format for a 64 kbit/s transparent call - Clearmode	√	√ (forwarded transparently)
RFC 4117	Transcoding Services Invocation	√	×
RFC 4235	Dialog Event Package	Partial	Partial
RFC 4240	Basic Network Media Services with SIP - NetAnn	√	√ (forwarded transparently)
RFC 4244	An Extension to SIP for Request History Information	√	√
RFC 4320	Actions Addressing Identified Issues with SIP Non-INVITE Transaction	√	√
RFC 4321	Problems Identified Associated with SIP Non-INVITE Transaction	√	√
RFC 4411	Extending SIP Reason Header for Preemption Events	√	√ (forwarded transparently)
RFC 4412	Communications Resource Priority for SIP	√	√ (forwarded transparently)
RFC 4458	SIP URIs for Applications such as Voicemail and Interactive Voice Response	√	√ (forwarded transparently)
RFC 4475	SIP Torture Test Messages	√	√
RFC 4497 or ISO/IEC 17343	Interworking between SIP and QSIG	√	√ (forwarded transparently)
RFC 4566	Session Description Protocol	√	√
RFC 4568	SDP Security Descriptions for Media Streams for SRTP	√	√
RFC 4582	The Binary Floor Control Protocol (BFCP)	×	√ (forwarded transparently)

RFC	Description	Gateway	SBC
RFC 4715	Interworking of ISDN Sub Address to sip isub parameter	√	√ (forwarded transparently)
RFC 4730	A SIP Event Package for Key Press Stimulus (KPML)	Partial	×
RFC 4733	RTP Payload for DTMF Digits	√	√
RFC 4904	Representing trunk groups in tel/sip URIs	√	√ (forwarded transparently)
RFC 4960	Stream Control Transmission Protocol	×	√
RFC 4961	Symmetric RTP and RTCP for NAT	√	√
RFC 4975	The Message Session Relay Protocol (MSRP)	×	√
RFC 5022	Media Server Control Markup Language (MSCML)	√	×
RFC 5079	Rejecting Anonymous Requests in SIP	√	√
RFC 5627	Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP	√	√ (forwarded transparently)
RFC 5628	Registration Event Package Extension for GRUU	√	×
RFC 5806	Diversion Header, same as draft-levy-sip-diversion-08	√	√
RFC 5853	Requirements from SIP / SBC Deployments	-	√
RFC 6035	SIP Package for Voice Quality Reporting Event, using sip PUBLISH	√	√
RFC 6135	An Alternative Connection Model for the Message Session Relay Protocol (MSRP)	×	√
RFC 6140	Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)	√	√
RFC 6337	Session Initiation Protocol (SIP) Usage of the Offer/Answer Model	-	√
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)	√	√
RFC 6442	Location Conveyance for the Session Initiation Protocol	-	√
RFC 7245	An Architecture for Media Recording Using the Session Initiation Protocol	√	√
RFC 7261	Offer/Answer Considerations for G723 Annex A and G729 Annex B	√	√
RFC 7865	Session Initiation Protocol (SIP) Recording Metadata	√	√
RFC 7866	Session Recording Protocol	√	√
RFC 8068	Session Initiation Protocol (SIP) Recording Call Flows	√	√



## 4.2 SIP Message Compliancy

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

### 4.2.1 SIP Functions

The device supports the following SIP Functions:

**Table 67: 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

### 4.2.2 SIP Methods

The device supports the following SIP Methods:

**Table 68: 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	-

### 4.2.3 SIP Headers

The device supports the following SIP headers:

**Table 69: Supported SIP Headers**

SIP Header	SIP Header
Accept	Proxy- Authenticate
Accept-Encoding	Proxy- Authorization
Alert-Info	Proxy- Require
Allow	Prack
Also	Reason
Asserted-Identity	Record- Route
Authorization	Refer-To
Call-ID	Referred-By
Call-Info	Replaces
Contact	Require
Content-Disposition	Remote-Party-ID
Content-Encoding	Response- Key
Content-Length	Retry-After
Content-Type	Route
Cseq	Rseq
Date	Session-Expires
Diversion	Server
Expires	Service-Route
Fax	SIP-If-Match
From	Subject
History-Info	Supported
Join	Target-Dialog
Max-Forwards	Timestamp
Messages-Waiting	To
MIN-SE	Unsupported
P-Associated-URI	User- Agent
P-Asserted-Identity	Via
P-Charging-Vector	Voicemail
P-Preferred-Identity	Warning
Priority	WWW- Authenticate
Privacy	-



The following SIP headers are not supported:

- Encryption
- Organization

#### 4.2.4 SDP Fields

The device supports the following SDP fields:

**Table 70: Supported SDP Fields**

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

#### 4.2.5 SIP Responses

The device supports the following SIP responses:

**Table 71: Supported SIP Responses**

Response Type		Comments
<b>1xx Response (Information Responses)</b>		
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.

Response Type		Comments
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
<b>2xx Response (Successful Responses)</b>		
200		OK
202		Accepted
<b>3xx Response (Redirection Responses)</b>		
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.
<b>4xx Response (Client Failure Responses)</b>		
400	Bad Request	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
401	Unauthorized	Authentication support for Basic and Digest. Upon receiving this message, the device issues a new request according to the scheme received on this response.
402	Payment Required	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
403	Forbidden	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
404	Not Found	The device generates this response if it is unable to locate the callee. Upon receiving this response, the device notifies the User with a Reorder Tone.
405	Method Not Allowed	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
406	Not Acceptable	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
407	Proxy Authentication Required	Authentication support for Basic and Digest. Upon receiving this message, the device issues a new request according to the scheme received on this response.
408	Request Timeout	The device generates this response if the no-answer timer expires. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.

Response Type		Comments
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.
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.

Response Type		Comments
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.
<b>5xx Response (Server Failure Responses)</b>		
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	
<b>6xx Response (Global Responses)</b>		
600	Busy Everywhere	Upon receipt of any of these responses, the device releases the call, sending an appropriate release cause to the PSTN side.
603	Decline	
604	Does Not Exist Anywhere	
606	Not Acceptable	

**International Headquarters**

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

**AudioCodes Inc.**

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

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

Website: <https://www.audiocodes.com>

©2026 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: **LTRT-27790**

