Release Notes

AudioCodes Multi-Service Business Router Series of Integrated Voice & Data Routers

Mediant 500Li MSBR

Version 7.2

Table of Contents

List of Tables

Notice

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

This document is subject to change without notice.

Date Published: March-18-2021

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

Throughout this manual, unless otherwise specified, the term *device* refers to the AudioCodes Mediant 500 MSBR.

Related Documentation

Document Name
Mediant 500Li MSBR Hardware Installation Manual
Mediant 500Li MSBR User's Manual
Mediant 500Li MSBR CLI Reference Guide

Document Revision Record

LTRT	Description
27445	Initial document release
27531	Ver. 7.20AN.456.516
27539	Ver. 7.20AN.456.539 (R5.1)

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 AudioCodes Mediant 500Li MSBR Version 7.2. This includes new features, known constraints, and resolved constraints.

Note:

- 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, visit AudioCodes website at https://www.audiocodes.com/services-support/open-source or contact your AudioCodes sales representative.
- Updates to this document may be made due to significant information discovered after the release or too late in the release cycle to be otherwise included in this release documentation. You can check for an updated version on AudioCodes website at https://www.audiocodes.com/library/technical-documents.

1.1 Software Revision Record

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

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

Table 1-1: Software Revision Record

Software Version	Date
7.20AN.456.539 (R5.1)	18 March 2021
7.20AN.456.516 (R5)	11 February 2021
7.20AN.456.347 (R4)	1 November 2020
7.20AN.456.089 (R3)	15 September 2020
7.20AN.404.003	3 December 2019

This page is intentionally left blank.

2 Released Versions

This chapter describes new features, known constraints and resolved constraints relating to data-router functionality of Mediant 500Li MSBR.

Note: For supported session border controller (SBC) and media gateway functionality on the Mediant 500Li MSBR, refer to the *SBC-Gateway Series Release Notes Version 7.2*.

2.1 Version 7.20AN.456.539 (R5.1)

This version includes new features and resolved constraints only.

Note: This version corresponds to SBC-Gateway Version 7.20A.256.024.

2.1.1 New Features

This section describes the new features introduced in this version.

2.1.1.1 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)

2.1.1.2 L2TP over Cellular

The device now supports L2TP over cellular.

2.1.1.3 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.

2.1.1.4 Allowing Port Forwarding and DMZ Pages in End-User Web Interface

The availability of the following pages (hidden by default) in the End-User web interface is now configurable:

- Port Forwarding Settings page (Monitor > Advanced folder > Port Forwarding Settings):
  `conf system -> end-user -> allow-port-forwarding enable|disable`
  (EndUserAllowPortForwarding)
- DMZ Settings page (Monitor > Advanced folder > DMZ):
  `conf system -> end-user -> allow-dmz-settings enable|disable`
  (EndUserAllowDMZSettings)

2.1.2 Resolved Constraints

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

Table 2-1: Resolved Constraints for Version 7.20AN.456.539

Incident	Description
NGC-3823	TR-069 doesn't refresh after the IP address is changed.

2.2 Version 7.20AN.456.516 (R5)

This version includes new features and known constraints only.

Note: This version corresponds to SBC-Gateway Version 7.20A.256.024.

2.2.1 New Features

This section describes the new features introduced in this version.

2.2.1.1 Transcoding Support

The device now provides call transcoding (coder, DTMF and SRTP-RTP) capabilities. It supports up to 20 transcoding sessions.

2.2.1.2 Increased SBC Sessions

The device now supports up to 30 concurrent SBC sessions.

2.2.1.3 Tracking Enhancements

This version introduces the following tracking enhancements:

- A static route can now be configured to depend on two tracking objects. In this case, the route is 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]
```

- The following `track` command options have been added for track retries:
  - `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".
- Clearing track minimum RTT values:

```
# clear counters track [<track id>
```

- Minimum / 60sec, average and target have been added to the output of the following command:

```
show data track brief
```

- The show of the track now 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
```

2.2.1.4 Multicast in VRFs

The device now supports multicast in VRF, using the new `pim` command:

```
ip vrf <VRF Name> enable pim
```

2.2.1.5 DNS Resolution for IPv6

The device now supports obtaining IPv6 addresses from DNS resolutions.

2.2.1.6 TR-069 over IPv6

The device now supports IPv6 for TR-069 communication with the TR-069 Auto-Configuration Server (ACS). The device determines if an IPv4 or IPv6 interface should be used 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}.

TR-069 over IPv6 is enabled (disabled, by default) by the new parameter, 'IPv6' (`configure system > cwmp > ipv6 enable`). If not enabled, the device only uses IPv4 for TR-069.

2.2.1.7 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.)

2.2.1.8 End-User Web Interface

The device now provides a 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*.

The following has also 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

2.2.2 Resolved Constraints

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

Table 2-2: Resolved Constraints for Version 7.20AN.456.516

Incident	Description
NGC-3398	The device freezes every few hours (power off is required to resolve).
NGC-3507	QoS match-map isn't configurable.
NGC-3705	Device failure upon DTMF transcoding.
NGC-3815	QoS configuration is identical to Mediant 500L.
NGC-3818	Internet browsing is not possible when the device has ADSL.
NGC-3824	TR-069 shows "500ng" instead of "500Li".
NGC-3921	The Wi-Fi interface cannot be recovered.
NGC-3923	BRI interfaces are not fully configurable.
NGC-3925	The 4G interface is not displayed in the device string.

2.3 Version 7.20AN.456.347 (R4)

This version includes new features and known constraints only.

Note: This version corresponds to SBC-Gateway Version 7.20A.256.024.

2.3.1 New Features

This section describes the new features introduced in this version.

2.3.1.1 Binding Applications to IPv6 Network Interfaces

The device now supports binding various applications to a source IPv6 network interface (VRF alias or IP address). Up until now, only IPv4 was supported.

- Web interface: `config-system > web > web-if <Index> > network-source`
- SSH: `config-system > cli-settings > ssh-network-source-ipv6 | ssh-network-source-ipv4`
- Telnet: `config-system > cli-settings > telnet-network-source-ipv6 | telnet-network-source-ipv4`
- Syslog: `config-troubleshoot > syslog > network-source`
- Automatic Update: `configure system > automatic-update > network-source`

Applicable Products: Mediant 500Li.

2.3.1.2 IEEE 802.11w Protection Management Frames for Wi-Fi

The device now supports the IEEE 802.11w-2009 wireless encryption standard, which is based on the 802.11i framework and protects against subtle attacks on wireless LAN (WLAN) management frames. Protection Management Frames (PMF) or also known as Management Frame Protection (MFP) is configured by the following new command:

```
(config-data)# interface dot11radio 1
(conf-if-dot11radio 1)# mfp {disabled|optional|required}
```

Where:

- *disabled* means disables the client for MFP support
- optional means that it sets PMF only with MFP -supporting clients
- *required* means that clients can associate only if MFP is negotiated. If the devices do not support MFP, they are not allowed to join the network

Applicable Products: Mediant 500Li.

2.3.1.3 TLS Version 1.3 Support

The device now supports TLS Version 1.3. As a result, the following configuration updates have been made to the existing TLS Contexts table:

- Additional optional 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 existing value Any - Including SSLv3 (0) has been renamed "Any TLS 1.x", which now indicates support for only TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3.

Note: SSLv3 is no longer supported as it's not sufficiently secure.

- New parameters for configuring a cipher list for TLSv1.3:
  - 'Cipher Server TLS1.3'
  - 'Cipher Client TLS1.3'
- New 'Key Exchange Groups' parameter for configuring groups that are supported for key exchange (applicable to all TLS versions):
  - X25519
  - P-256
  - P-384
- Existing 'DH Key Size' parameter updates:
  - Default has changed to 2048.
  - Value 1024 is now displayed as "1024 – Not Recommended" (1024 is only available in the Web interface.)

  Above also affects the existing ‘Private Key Size’ parameter on the Change Certificates page.

Note: If the old (obsolete) Auto-Update related ini file parameter [AupdCipherString] was used for defining the TLS 1.0-1.2 cipher string and the device is upgraded to this software version, this parameter is ignored (i.e., no backward compatibility). Therefore, after upgrade, the TLS 1.0-1.2 cipher string must be configured in the TLS Contexts table ('Cipher Client' parameter).

Applicable Products: Mediant 500Li.

2.3.2 Known Constraints

The following known constraints were discovered in this release:

Table 2-3: Known Constraints for Version 7.20AN.456.347

Incident	Description
NGC-3324	Only up to 1,000 IPv6 sessions are supported.

2.4 Version 7.20AN.456.089 (R3)

This version includes new features only.

Note:

- This version corresponds to SBC-Gateway Version 7.20A.256.024.
- IPv6 will be supported in the next applicable release.

2.4.1 New Features

This section describes the new features introduced in this version.

2.4.1.1 License Key for Advanced Bandwidth Performance

The License Key ("Enhanced-Performance") now specifies the maximum bandwidth supported by the device:

- If not defined (default), device is licensed for up to 200 Mbps traffic with QoS
- "AP500" license allows up to 500 Mbps traffic with QoS
- "AP1000" license allows up to 1 Gbps traffic with QoS

Applicable Products: Mediant 500Li.

2.4.1.2 Wi-Fi Support

The device now supports Wi-Fi router functionality.

Applicable Products: Mediant 500Li.

2.4.1.3 LTE WWAN Support

The device now supports Long-Term Evolution (LTE) wireless WAN (WWAN). This is provided 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 provider.

Note: QoS on LTE interfaces will be supported in a future release.

Applicable Products: Mediant 500Li.

2.4.1.4 FXS Out-of-Service Scenarios

The device can now take an FXS port interface out-of-service due to Serial Peripheral Interface (SPI) failure, elevated temperature, or ground fault.

Applicable Products: Mediant 500Li.

2.4.1.5 IPSec Support

The device now supports IPSec

Applicable Products: Mediant 500Li.

2.5 Version 7.20AN.404.003

This version includes new features only.

Note: This version corresponds to SBC-Gateway Version 7.20A.204.

2.5.1 New Features

This section describes the new features introduced in this version.

2.5.1.1 Enhanced Binding of Applications to Interfaces / Source Addresses

Alias names can be configured for the device's Virtual Routing and Forwarding (VRF) and IP address network interfaces. This is done using the new subcommands `alias` (IP addresses), `ipv4-alias` (VRF), and `ipv6-alias` (VRF), as shown in the examples below:

- Defines an IPv4 address with alias on interface VLAN 1:

```
(config-data)# interface vlan 1
(conf-if-VLAN 1)# ip address 10.4.4.61 255.255.0.0 alias
ip_vlan1
```

- Defines an IPv6 address with alias on interface VLAN 1:

```
(config-data)# interface vlan 1
(conf-if-VLAN 1)# ip address 2000:3000::10/64 alias ipv6_vlan1
```

- Defines a VRF with an IPv4 alias:

```
(config-data)# ip vrf voip ipv4-alias voip_v4
```

- Defines a VRF with an IPv6 alias:

```
(config-data)# ip vrf voip ipv6-alias voip_v6
```

The alias name (of the VRF table or IP address of network interface) is used to bind a specific management application (i.e. SIP, RADIUS, LDAP, SSH, SNMP, Telnet, Web Interfaces, or Syslog) to a source network interface. If the network interface name is not defined for one of these management interfaces, the default VRF named "main-vrf" (IPv4 or IPv6) is used by default. However, for the voice interface, SIP Interfaces and Media Realms must be assigned a network interface (i.e., alias name of VRF or IP address).

The following lists the new commands / parameters for binding each application:

- Binding the SSH application to a source network interface:
  - `ssh-network-source-ipv4` / SSHIPv4Interface_InterfaceName
  - `ssh-network-source-ipv6` / SSHIPv6Interface_InterfaceName
- Binding the Telnet application to a source network interface:
  - `telnet-network-source-ipv4` / TelnetIPv4Interface_InterfaceName
  - `telnet-network-source-ipv6` / TelnetIPv6Interface_InterfaceName
- Binding the SNMP application to a source network interface:`configure system > snmp settings > network-interface` / SNMPInterface.
- Binding the RADIUS application client to a source network interface: `configure system > radius servers > network-source` /

RadiusServers_InterfaceName.

- Binding the Syslog application to a source network interface: `configure troubleshoot > syslog > syslog-interface > network-source` / SyslogInterface_InterfaceName.
- Binding the Debug Recording (DR) application to a source network interface: `configure troubleshoot > logging settings > network-source` / DebugRecordingIpInterfaceName.
- Binding Web management interfaces to a source network interface, allowing access to the Web interface through different VRFs or IP addresses. Each Web interface can be secured by enforcing access over HTTPS. The feature is supported by the new Web Interface table (`configure system > web > web-if` / WebInterfaces).
- Specifying source network interface for the `copy from` command, using the new subcommand, `source`, for example:

```
copy web-logo from http://server.com/logo source main-vrf-ipv4
```

- Binding the Automatic Update mechanism to a source network interface to open a connection with the remote provisioning server: `configure system > automatic-update > network-source` / AUPDInterface.

The alias configuration is optional and must be done if the VRF or IP address is used by one of the above-mentioned management and SIP applications. If the interface is used for other purposes, such as data routing, the alias of the interface does not need to be configured.

All VRFs and IP addresses that are configured with alias names can be displayed using the new command, `show network available-app-interface`, as shown in the following example:

```
MP5XXNG(config-data)# do show network available-app-interfaces

VRF IFs:  VRF Alias          Address Family                 Vrf Name        IF Status
-------------------------------------------------------------------------------------
          "main-vrf-ipv4"    IPv4                           main-vrf        UP
          "main-vrf-ipv6"    IPv6                           main-vrf        UP
          "1234567890123456"      IPv4                           2               UP
          "voip"             IPv4                           vrf_voip        UP

IP  IFs:  IP Alias           IP Address          Device IF Name      Vrf Name        IF Status
-------------------------------------------------------------------------------------
          "1234567890123450"      10.2.2.2            VLAN 2          main-vrf        UP
          "vlan_1"           10.4.4.61           VLAN 1          2               UP


Applications binding: (Current source interface resolved in the vrf according to app. destination address)
        App name          VRF Alias                App Dst Address                  Source Address
        -------------------------------------------------------------------------------------
        SIP               "main-vrf-ipv4"          11.11.11.100                     10.10.10.1
```

Applicable Products: Mediant 500Li.

2.5.1.2 Restore to Factory Defaults after Three Failed Resets

The device automatically restores to factory default settings after three unsuccessful consecutive reset attempts. In the event of three additional consecutive failures (total of six failures), the BOOTP application is automatically activated to rescue the device (i.e., the device sends out BOOTP parameters to load a new firmware when in rescue mode).

Applicable Products: Mediant 500Li.

2.5.1.3 Enhanced Syslog (Rsyslog)

The device supports Rsyslog, which is an enhanced version of the standard Syslog protocol (RFC 3164). Rsyslog provides better logging performance, flexibility and filtering capabilities.

For example, the device can store logs in its flash memory (persistent), which remain (persist) even after a device reset (crash).

This feature introduces the following new commands:

- Maximum size of persistent log file:
  - Configure troubleshoot > syslog > system-persistent-log-size (SystemPersistentLogSize)
- Log display filter:
  - show system log no-sip: Displays all non-SIP logged messages.
  - show system log: Displays a specified persistent log file (0-9, where 0 is the latest file).
- Log files download (copy to command):
  - system-log: Downloads the system log file.
  - system-log-no-sip: Downloads the system log file without SIP-related information.
  - system-log-persistent: Downloads the persistent system log file.

  These downloaded files are compressed in tar.gz format.

Applicable Products: Mediant 500Li.

2.5.1.4 Flash Memory Dual Image

The device has a dual image in its flash memory. The key purpose of this architecture is to support a fallback mechanism to prevent downtime that may arise because of firmware related-issues occurring during every day operations and during a firmware upgrade. The dual image architecture includes separate flash memory segments for the active firmware image, redundant firmware image and another image for system-related data including the device's running configuration file. This mechanism is implemented for the following scenarios:

- System startup: Upon every successful system startup, the redundant .cmp file is checked, validated and restored if necessary (in case it's corrupted or different to the active .cmp file).
- Firmware Upgrade:
  - The new .cmp file is burnt to the active partition.
  - The device's existing running configuration file is backed up to the system partition.

  If during the firmware upgrade, one of the following occurs:
  - The upgrade process fails or the device doesn't fully complete the boot process.
  - The device's firmware is corrupted.

  Then the device restores it's backed up .cmp and running configuration files, thereby ensuring seamless operation.

  If the upgrade process succeeds, the backed-up files are deleted, the new .cmp file is copied to the redundant partition and the new running configuration file is backed up to the system partition.

Applicable Products: Mediant 500Li.

2.5.1.5 QoS

The QoS module is new. Please consult the QoS-specific configuration guide for more information.

2.5.2 Known Constraints

The following features are not supported in this release:

- Wi-Fi
- IPSec
- VPN
- IPv6
- Cellular
- DHCP relay
- DHCP client unicast
- WAN ingress policer
- LAN egress shaper
- Bridging
- Dynamic routing
- VRRP
- Layer-2 security features (802.1x and port security) and metro Ethernet features
- Multi-WAN copper and fiber aren't supported simultaneously. To enable the WAN interface, use the CLI command `conf data > wan mode <copper (default) | fiber>`, and then write and reload the unit for it to take effect.
- Zero Conf

3 Capacity

This section provides capacity figures per product.

3.1 Data Performance

The following lists the device's data-router capacity:

- 64 bytes UDP performance: up to 700 Mbps
- Internet Mix (IMIX) UDP (avg. 400 bytes) performance: up to wire speed
- PPS performance (aggregated): up to 2.3 million packets per second
- 5 simultaneous TCP sessions - wire speed
- Max. streams: 30,000
- Applying QoS classify/remark/shaper on the above benchmarks has no impact.

Note: Performance figures above are based on the presence of the AP1000 feature key.

3.2 SIP Signaling and Media Capacity

The following table lists the device's capacity for concurrent SIP signaling sessions, concurrent media sessions, and registered users.

Table 3-1: SIP Signaling and Media Capacity

Signaling Capacity		Media Sessions			
SIP Sessions	**Registered Users**	**Session Type**	**RTP Sessions**	**SRTP Sessions**	**Detailed Media Capabilities**
30	100	Hybrid	30	15	Transcoding: See Table 3-3
		GW-Only	8	8	

Notes:

- 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 and media 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.

3.2.1 Detailed Capacity

The DSP channel capacity and SBC session capacity for Mediant 500Li are shown in the table below.

Table 3-2: 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 3-3: 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 1	To Profile 2	
		IPM Detectors	G.722	AMR WB	SILK NB / iLBC	SILK WB			
FXS, FXO, and/or BRI, but not in use	0	-	-	-	-	-	20	16	30

Notes:

- All hardware assemblies also support the following DSP channel capabilities: echo cancellation (EC), CID (caller ID), RTCP XR reporting, and SRTP.
- Three-way conferencing is supported by the analog ports.
- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.

3.3 Session Capacity per Feature

The table below lists capacity per feature:

Table 3-4: Capacity per Feature

WebRTC Sessions	One-Voice Resiliency (OVR) Users	SIPRec Sessions
2	-	10

Note: 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 4-1: Supported RFCs

RFC	Description	Gateway	SBC
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-realtimefax-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 2976	SIP INFO Method	√	√
RFC 3261	SIP	√	√

RFC	Description	Gateway	SBC
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 3666	SIP to PSTN Call Flows	√	√ (forwarded transparently)
RFC 3680	A SIP Event Package for Registration (IMS)	√	×

RFC	Description	Gateway	SBC
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 4168	The Stream Control Transfer Protocol (SCTP) as a Transport for SIP	×	√
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 4-2: Supported SIP Functions

Function	Comments
User Agent Client (UAC)	-
User Agent Server (UAS)	-
Proxy Server	The device supports working with third-party Proxy Servers such as Nortel CS1K/CS2K, Avaya, Microsoft OCS, Alcatel, 3Com, BroadSoft, Snom, Cisco and many others
Redirect Server	The device supports working with third-party Redirection servers
Registrar Server	The device supports working with third-party Registration servers

4.2.2 SIP Methods

The device supports the following SIP Methods:

Table 4-3: Supported SIP Methods

Method	Comments
ACK	-
BYE	-
CANCEL	-
INFO	-
INVITE	-
MESSAGE	Supported only by the SBC application and send only
NOTIFY	-
OPTIONS	-
PRACK	-
PUBLISH	Send only
REFER	Inside and outside of a dialog
REGISTER	Send only for Gateway/IP-to-IP application; send and receive for SBC application
SUBSCRIBE	-
UPDATE	-

4.2.3 SIP Headers

The device supports the following SIP headers:

Table 4-4: 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	-

Note: The following SIP headers are not supported:

- Encryption
- Organization

4.2.4 SDP Fields

The device supports the following SDP fields:

Table 4-5: 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 4-6: Supported SIP Responses

Response Type		Comments
1xx Response (Information Responses)		
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.

Response Type		Comments
182	Queued	The device generates this response in Call Waiting service. When the SIP device receives a 182 response, it plays a special waiting Ringback tone to the telephone side.
183	Session Progress	The device generates this response if the Early Media feature is enabled and if the device plays a Ringback tone to IP
2xx Response (Successful Responses)		
200	OK	
202	Accepted	
3xx Response (Redirection Responses)		
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.
4xx Response (Client Failure Responses)		
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.

Response Type		Comments
407	Proxy Authentication Required	Authentication support for Basic and Digest. Upon receiving this message, the device issues a new request according to the scheme received on this response.
408	Request Timeout	The device generates this response if the no-answer timer expires. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
409	Conflict	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
410	Gone	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
411	Length Required	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
413	Request Entity Too Large	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
415	Unsupported Media	If the device receives a 415 Unsupported Media response, it notifies the User with a Reorder Tone. The device generates this response in case of SDP mismatch.
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.

Response Type		Comments
485	Ambiguous	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
486	Busy Here	The SIP device generates this response if the called party is off-hook and the call cannot be presented as a call waiting call. Upon receipt of this response, the device notifies the User and generates a busy tone.
487	Request Canceled	This response indicates that the initial request is terminated with a BYE or CANCEL request.
488	Not Acceptable	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
491	Request Pending	When acting as a UAS: the device sent a re-INVITE on an established session and is still in progress. If it receives a re-INVITE on the same dialog, it returns a 491 response to the received INVITE. When acting as a UAC: If the device receives a 491 response to a re-INVITE, it starts a timer. After the timer expires, the UAC tries to send the re-INVITE again.
5xx Response (Server Failure Responses)		
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	
6xx Response (Global Responses)		
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	

This page is intentionally left blank.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
200 Cottontail Lane,
Suite A101E,
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com/

Document #: LTRT-27539