AudioCodes Large Enterprise and Carrier Class Media Gateways

Release Notes

Mediant™ 8000

Version 6.6

Document #: LTRT-90924

Table of Contents

1 Hardware Platforms 9

2 New Features and Enhancements 11

2.1 Management Features 11

2.1.1 New Action "Clone Board" 11
2.1.2 Improved Media Gateway Boards' Configuration Backdoor 11
2.1.3 New Actions for Inserting and Moving Rows in Large SBC Tables 11
2.1.4 Session Quality Experience Reports 12
2.1.5 New Performance Monitoring Functionality 13

2.2 IP Networking Features 14

2.2.1 Board Network Settings 14
2.2.2 Improved Media Realm Table 14
2.2.3 Support for DNS Server Configuration at Board level 14
2.2.4 Support for ‘Logical link failure detection’ (relevant for ES-2 only) 14
2.2.5 Support for ES-2 (PMs and Filtering) 15

2.3 MEGACO Features 16

2.3.1 Support for AMR Payload Format – Bandwidth-Efficient / Octet-Aligned 16
2.3.2 Support for Transrating Between Different Ptime Values 16
2.3.3 Support for NB-IP Interfaces on the IP Multimedia Subsystem (IMS) System 16

2.4 SIP Call Control Features 17

2.4.1 Support for Larger SIP Tables 17
2.4.2 SIP General Features 17
2.4.2.1 Support for Proxy Redundancy Mode 17
2.4.2.2 Support for NAT Translation Table 17
2.4.2.3 Support for Fax Transmission behind NAT 18
2.4.2.4 Support for SIP T38 Version 18
2.4.2.5 Support for Advanced Syslog Message Facility Level 18
2.4.2.6 Support for Syslog Debug Level for Multiple SIP Boards 18
2.4.2.7 Support for IPV6 in SIP DNS Table 18
2.4.2.8 Support for QoS Statistics in SIP Release Call 18
2.4.2.9 Support for SIP Message Manipulations Table 19
2.4.2.10 Improved SIP IP Group Table 19
2.4.2.11 Support for SIP Least Cost Routing (LCR) 19
2.4.2.12 Support for SIP Message Policy Table 20
2.4.2.13 Support for Syslog and Debug Recording Filters 20
2.4.2.14 Support for LDAP 21
2.4.2.15 TCP Keep-Alive Mechanism per SIP Interface 22
2.4.2.16 Support for Simultaneous Negotiation-Fax (T.38) and Modem (V.150.1) Relay CED 22
2.4.2.17 Support for Gateway Name in SIP Contact Header 22
2.4.2.18 Support T.38 re-INVITE upon Detection of V.34 / Super G3 V8-CM Signals 23
2.4.2.19 Support for Re-Negotiation of Coders in re-INVITE for Unhold Calls .23
2.4.2.20 Support for Re-using TCP/TLS Connections without "alias" Requirement 23
2.4.2.21 Support for TLS Mutual Authentication per SIP Interface 23
2.4.2.22 Increased Maximum Record-Route Headers in INVITE / 200 OK 23
2.4.3 SIP Gateway Features 24
2.4.3.1 Support for Tel to IP Forking Group 24
2.4.3.2 Support Line Transfer Mode 24
2.4.3.3 Improved GW SIP IP-to-Tel Calls Security 24

2.4.3.4 Improved IP2Tel Manipulation Table 24
2.4.3.5 Support for Redirect Number Manipulation 24
2.4.3.6 Support for SIP GW Message Manipulation 25
2.4.3.7 Improved Destination Phone Number Manipulation for Tel-to-IP 25
2.4.3.8 Improved 'Use Trunk Group Information' 25
2.4.3.9 Support for Calling Name ID Manipulation 25
2.4.3.10 Improved SIP IP to Tel Routing table 25
2.4.3.11 Support for ISDN Facility Trace 25
2.4.3.12 Support for Replacing Calling Number with Redirect Number 25
2.4.3.13 Support for Early Media 26
2.4.3.14 Support for 'Enable Early 183' Feature 26
2.4.3.15 Improved SIP PSTN Settings 26
2.4.3.16 AudioCodes ELIN Gateway for Lync Server 2010 E9-1-1 Calls to PSTN 27
2.4.3.17 Connected Number Sub-Address Added to Connect Message 27
2.4.3.18 Interworking User-to-User Header with Text Format to UUIE IA5 Characters in Q.931 Messages 27
2.4.3.19 Improved Trunk Group Setting Table 28
2.4.3.20 Support of IP-to-Tel Routing based on Source SRD 28
2.4.3.21 Support for SIP Gateway3xx Redirect Responses 28
2.4.3.22 Support 183 for Early Media per IP Profile 28
2.4.4 SIP SBC Features 29
2.4.4.1 No Answer Timeout [Sec] 29
2.4.4.2 P-Asserted-Identity Handle 29
2.4.4.3 Refer Behavior 29
2.4.4.4 SBC Xfer Prefix 30
2.4.4.5 3xx Behavior 30
2.4.4.6 GRUU Mode 30
2.4.4.7 Max Forwards Limit 30
2.4.4.8 Minimum Session-Expires 30
2.4.4.9 User Registration Time 30
2.4.4.10 Proxy Registration Time 30
2.4.4.11 Survivability Registration Time 30
2.4.4.12 Keep Original User in Register 30
2.4.4.13 SBC Coders Preferences Mode 31
2.4.4.14 Bye Authentication 31
2.4.4.15 Improved SIP Proxy Server Table 31
2.4.4.16 Improved SIP IP to IP Routing Table 31
2.4.4.17 Support for SIP IP to IP Transcoding Mode 31
2.4.4.18 Support for Adding initial Route Header 32
2.4.4.19 Session Expires Mode 32
2.4.4.20 Support for SBC Allowed Coders Group Table 32
2.4.4.21 Support for SBC Condition Table 32
2.4.4.22 Support for Message Condition Association 32
2.4.4.23 Improved Classification Table - SIP Access List Using Classification 33
2.4.4.24 Support for Manipulation of SIP REGISTER Messages 33
2.4.4.25 Enhanced Anti-Tromboning for LAN User Agents (UAs) and WAN IP PBX 33
2.4.4.26 Interworking SIP Early Media 34
2.4.4.27 Interworking Re-INVITE Messages 34
2.4.4.28 Interworking SIP UPDATE Requests 34
2.4.4.29 Interworking Re-INVITE to UPDATE Requests 35
2.4.4.30 Interworking Delayed Offer 35
2.4.4.31 Interworking SIP REFER (Call Transfer) 35
2.4.4.32 Interworking SIP 3xx Redirect Responses 35
2.4.4.33 Advanced CAC Reserved Number of Calls per Customer 36
2.4.4.34 Support for SIP Call Forking 36
2.4.4.35 Support for SIP Forking by SIP Proxy Server 36

2.4.4.36 Support for User Registration Time per IP Profile 37
2.4.4.37 Support for Media (RTP) Normalization 37
2.4.4.38 Interworking Session Timer Mismatches...37
2.4.4.39 Support for MKI Length Negotiation for SRTP-to-SRTP Calls 37

2.5 Voice Features 38

2.5.1 Support for Minimum Gap Size..38
2.5.2 Support for RTCP XR Collection Server 38
2.5.3 Support for ESC Transport Type 38
2.5.4 Support for Acoustic Echo Cancellation..38
2.5.5 Support for Disabling RTCP when RTP is Inactive 38
2.5.6 Support for Five-Level RTP Redundancy 38
2.5.7 Support for Flexible Combinations of DSP Templates 38

2.6 Security Features 39

2.6.1 Improved Firewall Rules Table 39
2.6.2 Support for ARIA Encryption Algorithm for SRTP 39

2.7 PSTN Features 39

2.7.1 B-channels Status Indications for PRI 39
2.7.2 Improved ISDN Behavior...39
2.7.3 Manual D-Channel Switch Over 39

3 Known Constraints 41

3.1 Management Constraints...41

3.2 IP Networking Constraints...41

3.3 PSTN Constraints...42

3.4 Call Control Constraints 44

3.5 Voice Constraints...48

3.6 Security Constraints 49

3.7 High-Availability and Infrastructure Constraints.....................................49

3.8 Hardware Constraints 50

List of Tables

Table 3-1: Maximum Loads (Number of Boards) for Mediant 8000 Media Gateway............................50

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: May-28-2018

Trademarks

WEEE EU Directive

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

Customer Support

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

Document Revision Record

LTRT	Description
99022	Initial document release for Version 6.6
99024	Corrected the maximum supported number of entries in the Account Group (SIP > SIP General > Account Group) to 64.

Documentation Feedback

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

This page is intentionally left blank.

1 Hardware Platforms

The following hardware platforms are supported by Version 6.6 of the AudioCodes high availability Media Gateways software:

- Mediant 8000 with TP-6310 or TP-8410 TP boards.

This release supports the following hardware versions of the SC boards:

- SC Rev.1 – the first-generation SC board, based on the SUN CP2300 SBC, running on the SUN Solaris platform.
- SC Rev.2 – the second-generation SC board based on Intel CPU, running on the Linux platform.

The SC-Rev.2 board is supported, starting from Software version 5.8 of the Mediant 8000 software.

Note: On each Mediant 8000 system, the same revision of the SC board should be installed, i.e. either an SC Rev.1 + SC Rev.1 pair or an SC-Rev.2 + SC-Rev.2 pair. A mixture of an SC Rev.1+ SC-Rev.2 board is not supported.

The following hardware versions of the SA-1/RTM boards are supported:

- SA-1/RTM boards – boards without a Timing module.
- SA-1/RTM boards with a Timing module – for customers who wish to implement TDM clock synchronization using the BITS Generator or PSTN Line Sync capabilities.

This release supports the following hardware versions of the ES boards:

- ES/6600 – the first-generation ES board
- ES-2 – the second-generation ES board

The ES-2 board is supported starting from Software version 6.6 of the Mediant 8000 software.

Note: On each Mediant 8000 system, the same ES hardware board should be installed, i.e. either a ES/6600+ ES/6600 pair or a ES-2 + ES-2 pair. A mixture of an ES/6600 + ES-2 board is not supported.

The following hardware versions of the ES /RTM boards are supported:

- ES/6600/RTM boards – for ES/6600 use only.
- ES-2/RTM boards– for ES-2 use only.

This page is intentionally left blank.

2 New Features and Enhancements

The following new features have been introduced in the Version 6.6 release of the AudioCodes high availability Media Gateways software.

Note: Some of the features listed in this document are enabled only after purchasing the relevant software license keys from AudioCodes. For a list of software license keys that can be purchased, consult your AudioCodes sales representative.

2.1 Management Features

2.1.1 New Action "Clone Board"

A new action “clone TP board” simplifies the copying of VoP boards (TP-6310 / TP-8410) from an existing slot to a free slot. This feature may be used for copying a configuration from a working board.

2.1.2 Improved Media Gateway Boards' Configuration Backdoor

The user can now remove the backdoor configuration, even though there are still affected Media Gateway boards in the list. In the EMS, an appropriate warning popup window is displayed.

2.1.3 New Actions for Inserting and Moving Rows in Large SBC Tables

New table maintenance actions have been implemented for specific SBC tables – 'Move row up', 'Move row down', 'Insert row'. These actions make it easier for provisioning updates. For tables such as ‘IP- to-IP routing’, the sequence of the provisioned rows is important. The new feature allows the customer to add a new rule (provisioning row) in the middle of the table without redefining those rules provisioned in the previous rows. These new actions are available for the following large SBC tables:

- Classification
- IP to IP Routing
- SBC Manipulation
- SBC Message Manipulation
- SBC Condition

2.1.4 Session Quality Experience Reports

Mediant 8000 SIP boards can now be monitored using the Session Experience Manager (SEM). Session Quality Experience reports can be generated based on the data retrieved by the SEM for each SIP board. This feature enables VoIP network administrators to do the following:

- Quickly identify the metric or metrics responsible for degradation in the quality of any VoIP call made over the network.
- Accurately diagnose voice quality problems in response to VoIP user criticism
- Optimize quality of experience for VoIP users

The following important metrics are calculated when measuring the voice quality of calls made over a VoIP network:

- **Mean Opinion Score (MOS)** (specified by ITU-T recommendation P.800) is the average grade on a quality scale of Good to Failed, given by the SEM to voice calls made over a VoIP network after testing.
  MOS-LQ = listening quality, i.e., the quality of audio for listening purposes; it doesn't take bi-directional effects, such as delay and echo into account.
  MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects.
- **Jitter**, measured by the SEM, can result from uneven delays between received voice packets. To space evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality.
- **Packet Loss**, measured by the SEM, can result in choppy voice transmission. Lost packets are RTP packets that aren't received by the voice endpoint for processing.
- **Delay** (or latency), calculated by the SEM, is the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth.

2.1.5 New Performance Monitoring Functionality

The following new PMs have been added:

- New History PMs:
    - IP group level PMs:
        - MAX number of IPGroup Invite Dialogs
        - Avg Number of IPGroup Invite Dialogs
        - Min number of IPGroup Invite Dialogs
- New Real-Time PMs:
    - Media Realm PMs (QoE):
        - Tx traffic rate
        - RX traffic rate
        - Tx number of packets
        - Rx number of packets
        - Packet Jitter
        - Packet Delay
        - Rx Packet loss
        - Tx packet loss
        - Media realm QOS (measured by MOS method)
    - IP Group PMs:
        - Number of Dialogs of specific IP Group
        - Number of IP Group Invite dialogs
        - Number of IP Group Subscribe dialogs
        - Number of IP Group Other dialogs
    - SRD PMs:
        - Number of SRD Dialogs
        - Number of SRD Invite Dialogs
        - Number of SRD Subscribe dialogs
        - Number of SRD Other Dialogs

2.2 IP Networking Features

2.2.1 Board Network Settings

- DNS Request Timeout Seconds - Determines the time (in seconds) to wait before retransmitting a DNS request.
- Number of DNS Request Retries - Determines the number of times to retransmit DNS requests. After this number of retries, the gateway tries the Secondary DNS server IP.

2.2.2 Improved Media Realm Table

The "Is Default" parameter is used when configuring a Media Realm to indicate whether a Media Realm is default.

2.2.3 Support for DNS Server Configuration at Board level

The primary and secondary DNS server can now be configured at the board interface level.

2.2.4 Support for 'Logical link failure detection' (relevant for ES-2 only)

Logical link failure detection is now supported by the ES-2 based systems. This feature is relevant for ES-2 based systems only. This is implemented instead of the (LACP) mechanism supported only by ES/6600 based systems:

The Logical link failure detection mechanism does the following:

- Recognizes a logical link failure within a 30 seconds time period.
- Performs ES switch over if the other ES is enabled and is in a better state.
- Generates a trap to EMS in reference to the problematic uplink.
- Detects that the problem was solved and clears the previously generated alarm.

2.2.5 Support for ES-2 (PMs and Filtering)

This load adds support on the ES-2 switch for features that were previously implemented on the ES6600 switch, such as PMs and filtering. The following table provides a feature support comparison between the ES6600 and ES-2 switches.

ES/6600-ES-2 Feature Support Comparison

Feature	ES6600	ES-2
OAM & Control Uplinks	100MB	1GB
Online VLAN Configuration	Not supported	Supported
Online Distribution Rule	Not supported	Supported
Maximum number of VLANs	12	100
LACP	Supported	Not Supported
Logical link failure detection	Not Supported	Supported
PM Counters	Supported	Supported
Mirroring by Filters	Supported	Supported

2.3 MEGACO Features

2.3.1 Support for AMR Payload Format – Bandwidth-Efficient / Octet-Aligned

Both octet-aligned and bandwidth efficient AMR modes are now supported. The required mode can be set per call using the SDP AMR coder parameter (octet-align).

The octet-align MUST be symmetric, therefore, if the remote SDP exists, the local side is set according to it.

2.3.2 Support for Transrating Between Different Ptime Values

When all call parameters are the same except for Packetization Time (ptime), they can now be configured without transcoding; therefore, voice quality is improved.

2.3.3 Support for NB-IP Interfaces on the IP Multimedia Subsystem (IMS) System

Support for Narrow Band (NB) IP interfaces has now been added. The transport supported is only IP. Both Narrowband and Wideband versions of 3GPP AMR are supported. The supported configurations are as follows:

- Gateway (IP to TDM)
- Transcoding (IP to IP): 3GPP AMR NB/WB to G.711/G.722/AMR RFC 3267 and vice versa

The following H.248 packages are now supported:

- Q.1950 Bearer Characteristics Package (BCP)
- Q.1950 Generic Bearer Connection
- Q.1950 Bearer Network Connection Cut Through
- Q.1950 Bearer Control Tunneling
- 3GUP Package (ThreeGUP)
- IPBCP tunneling for SDP delivery

2.4 SIP Call Control Features

2.4.1 Support for Larger SIP Tables

The number of entries that can be provisioned in the following SIP related tables has been increased as follows:

- Coder Group Table (SIP > SIP General -> Coder Groups) – the number of entries has been increased to 10.
- Trunk Group Table (SIP > GW/IP to IP > Trunk Groups) – the number of entries has been increased to 240.
- Trunk group settings Table (SIP > GW/IP to IP > Trunk group settings) – the number of entries has been increased to 240.
- NAT Translation (SIP > SIP General > NAT Translation) – the maximum number of supported entries has been increased to 32.
- Account Group (SIP > SIP General > Account Group) – the maximum number of supported entries has been increased to 64.
- Manipulation rules Dest IP2Tel and Tel2IP (SIP>GW/IP to IP>Manipulation) – the number of entries has been increased to 120. IP2IP Inbound and Outbound manipulation (SIP>SBC>SBC Manipulation) –the number of entries has been increased to120. Calling Name Manipulation IP2Tel and Tel2IP (SIP > GW/IP to IP>Manipulation> Calling Name Manipulation) - the number of entries has been increased to 120.
- IP Group (SIP>SIP General> SIP Control Network> IP Groups) the number of entries has been increased to 48.
- IP2IPRouting (SIP>SBC>SBC Routing> IP to IP Routing) – the number of entries has been increased to 200.
- Classification Table (SIP>SBC>Classification) – the number of entries has been increased to 100.

2.4.2 SIP General Features

2.4.2.1 Support for Proxy Redundancy Mode

This feature enables flexibility in the configuration of the ‘Proxy Redundancy Mode’ setting. In previous versions, the user was able to define the Proxy Redundancy Mode only at the TP level. In the current version, the user can configure different modes (either Parking or Homing) on a per-Proxy Set basis.

2.4.2.2 Support for NAT Translation Table

This feature enables you to add multiple NATs for SIP control and RTP media using Static NAT rules. This table creates NAT rules for translating source IP address per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses. This allows, for example, the separation of VoIP traffic between different ISTP’s, and topology hiding (of internal IP addresses to the “public” network).

2.4.2.3 Support for Fax Transmission behind NAT

Support for transmission from fax machines (connected to the Media Gateway) located inside (behind) a Network Address Translation (NAT). Generally, the firewall blocks T.38 (and other) packets received from the WAN, unless the gateway behind the NAT sends at least one IP packet from the LAN to the WAN through the firewall. If the firewall blocks T.38 packets sent from the termination IP fax, the fax fails. To overcome this, the gateway sends No-Op (“no-signal”) packets to open a pinhole in the NAT for the answering fax machine. The originating fax does not wait for an answer, however immediately starts sending T.38 packets to the terminating fax machine upon receipt of a re-INVITE with T.38 only in the SDP, or T.38 and audio media in the SDP.

2.4.2.4 Support for SIP T38 Version

This feature allows configuring T.38 fax relay version. The following T.38 versions are supported:

- Version 0
- Version 3 (V34 over T.38)

2.4.2.5 Support for Advanced Syslog Message Facility Level

This feature allows the user to implement the Advanced Debug facility level for Syslog messages that are collected from the SIP boards (in accordance with RFC 3164).

The advanced facility level is useful when the gateway handles 'heavy' traffic When the Advanced Debug facility level (debug level 7) is configured, the Syslog Debug level automatically changes between Debug levels, and Warning level and Emergency level, depending on the SIP board's CPU consumption so that VoIP traffic isn’t affected.

Syslog messages are bundled into a single UDP packet, after which they are sent to a Syslog server (bundling size is determined by the 'SIP Max Bundle Syslog Length' parameter). Bundling reduces the number of UDP Syslog packets, thereby improving CPU utilization.

2.4.2.6 Support for Syslog Debug Level for Multiple SIP Boards

You can now configure the Debug level for SIP messages globally for all SIP boards (by setting 'SIP Logging Level' in the gateway level Troubleshooting screen). This configuration will overwrite the board level configuration.

2.4.2.7 Support for IPV6 in SIP DNS Table

Up to four different IPV6 addresses can be assigned to the same host name in the internal DNS table.

2.4.2.8 Support for QoS Statistics in SIP Release Call

This feature determines whether the SIP board includes call quality of service (QoS) statistics in SIP BYE and SIP 200 OK response to BYE, using the proprietary SIP header, X-RTP-Stat.

2.4.2.9 Support for SIP Message Manipulations Table

SIP header manipulation provides insertion, removal, and/or modification of SIP headers and parameters. This manipulation is configured in the Message Manipulations table. This feature enables the normalization of SIP messaging fields between communicating network segments.

2.4.2.10 Improved SIP IP Group Table

The following SIP IP Group parameters are now supported:

- Inbound Message Manipulation Set–allows customers to configure the Message Manipulation Set (rule) to be assigned to this IP Group for the SIP message manipulation rule on the Inbound message.
- Outbound Message Manipulation Set –allows customer to configure the Message Manipulation Set (rule) to be assigned to this IP Group for SIP message manipulation on the Outbound message.
- Source URI – allows customer to configure the source URI input used in the (CMR) Classify-Manipulate-Route process in SBC.
- Destination URI - allows customer to configure the destination URI input, used in the (CMR) Classify-Manipulate-Route process in SBC.
- Enlarge 'Enable Survivability' to support 'Always Terminate Register'.
- Registration Mode - Defines the registration mode for an IP Group.
- Authentication Mode
- Authentication Method List - defines SIP methods that the SIP board must challenge.
- Enable SBC Client Forking - enables call forking for USER-type IP Groups.
- Contact Name - If configured, the gateway uses the Contact Name string in its Contact and Via headers as a host name. It should be used for working with a specific IP group.

2.4.2.11 Support for SIP Least Cost Routing (LCR)

The LCR feature enables the gateway to choose the Outbound IP destination routing rule based on the lowest call cost. This feature enables service providers to optimize routing costs for customers.

This feature is configured in the following tables:

- Routing Rule Groups Table - Enable LCR feature and configure the average call duration and default connection cost.
- Cost Group Table
- Time Band Table

2.4.2.12 Support for SIP Message Policy Table

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

2.4.2.13 Support for Syslog and Debug Recording Filters

This feature provides support for setting filters for Syslog and debug recordings (DR) messages sent by a designated SIP board to a Syslog server with a packet capturing application (such as Wireshark). The feature helps to ensure that CPU consumption is reduced and an adverse impact upon VoIP performance is minimized.

The Syslog / DR filtering feature supports the configuration of up to 30 filtering rules using different filtering criteria. Each filtering criteria can be configured within a range. For example, you can filter Syslog messages for IP Groups 1 through 4.

The following Syslog filter criteria can be specified (configured in the gateway level 'SIP Logging Filter' screen):

- Specific Trunk Group (applicable only to the Gateway/IP-to-IP application)
- Specific Trunk (applicable only to the Gateway application)
- Specific Trunk/B-channel (applicable only to the Gateway application)
- Specific Tel-to-IP routing rule listed in the Outbound IP Routing table (applicable only to the Gateway/IP-to-IP application)
- Specific IP-to-Tel routing rule listed in the Inbound IP Routing table (applicable only to the Gateway/IP-to-IP application)
- Specific IP Group
- Specific SRD
- Specific Classification rule listed in the Classification table (applicable only to SBC application)
- Specific IP-to-IP routing rule listed in the IP-to-IP Routing table (applicable only to the SBC and SAS applications)
- Specific user, defined by username or user@host

Once the customer has configured the above filters, they can in addition choose to capture specific Debug recording packets for the filter criteria. For example, it is possible to capture SIP signaling or signaling and media for IP Groups 1 through 4. The following debug recording criteria can be filtered (configured in the gateway level 'SIP Logging Filter' screen):

- None (default)
- Signaling – contains all information related to signaling such as SIP signaling messages, Syslog, and CDR
- Signaling and media (RTP/RTCP/T.38)
- Signaling, media, and PCM - voice signals from and to TDM

- PSTN (ISDN and CAS) traces - applicable only for Trunk-related filters

When the parameter 'Enable Syslog' is disabled in the 'SIP Logging Filter' screen, no filtering occurs and therefore all messages are sent to the Syslog server.

2.4.2.14 Support for LDAP

LDAP (Lightweight Directory Access Protocol) is an Internet protocol programs used to look up information from a server.

The device supports Lightweight Directory Access Protocol (LDAP), enabling call routing decisions based on information stored on a third-party LDAP server (or Microsoft's Active Directory™ Enterprise Directory server). This feature enables the usage of a single common, popular database to manage and maintain information regarding user's availability, presence, and location.

The basic LDAP mechanism is described below:

- **Connection:** The SIP board connects and binds to the remote LDAP server either during the service's initialization (upon SIP board start-up) or whenever the LDAP server's IP address and port is changed. The service makes 10 attempts to connect and bind to the remote LDAP server with a timeout of 20 seconds between attempts. If the connection fails, the service remains in the disconnected state until either the LDAP server's IP address or port is changed.

  If the connection to the LDAP server later fails, the service attempts to reconnect, as described previously. M5k/8k will send SNMP alarm when the connection is broken. Upon successful reconnection, the alarm is cleared.

  Upon successful reconnection, the alarm is cleared.

  Binding to the LDAP server can be anonymous. For anonymous binding, the 'LDAP Bind DN' and 'LDAP Password' parameters must not be defined or set to an empty string.

  The address of the LDAP server can be a DNS name (using the 'LDAP Server Domain Name' parameter) or an IP address (using the 'LDAP Server IP' parameter).

- **Search:** To run a search using the LDAP service, the path to the directory's sub tree where the search is to be performed must be defined (using the 'LDAP Search DN' parameter). In addition, the search key (known as "filter" in LDAP references), which defines the exact DN to be found and one or more attributes whose values should be returned, must be defined. The SIP board supports up to 80 LDAP search requests.

  If the connection to the LDAP server is disrupted during the search, all search requests are dropped and an alarm indicating a failed status is sent to client applications.

- **Local LDAP Cache for LDAP Query Results:**

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

  The benefits of this feature include:

  - Improved routing decision performance using local cache for subsequent LDAP queries

- Reduced number of queries performed on an LDAP server and consequently reduced bandwidth consumption
- Partial survivability in case of intermittent LDAP server failure (or network isolation)

- **LDAP Cache actions:**

  The following new actions have been implemented:

  - LDAP Refresh Cache By Key-The action refreshes cache info related to specific key (AD attribute)
  - LDAP Clear All Cache-The action allows deleting all cache info.
  - LDAP Refresh all Cache - This action allows refreshing all cache info

2.4.2.15 TCP Keep-Alive Mechanism per SIP Interface

This feature provides support for a TCP keep-alive mechanism with a remote SIP entity (UAS or UAC) per SIP interface. A TCP keep-alive packet is an ACK (acknowledge) flag with the sequence number set to one less than the current sequence number for the connection. A host receiving one of these ACKs will respond with an ACK for the current sequence number. TCP keep-alive can be used, for example, to keep a NAT entry open for clients located behind the NAT server or simply to check that the connection to a remote network entity is still available.

The TCP keep-alive mechanism is configured per SIP interface.

2.4.2.16 Support for Simultaneous Negotiation-Fax (T.38) and Modem (V.150.1) Relay CED

This feature provides support for negotiating fax relay (T.38) and modem relay (V.150.1) sessions in the same already established call channel. Fax relay sessions require bypass answering tone (CED) while the modem relay requires RFC 2833 answering tone. As the SIP board is not always aware at the start of the session whether the answering tone is for fax or modem, it uses both methods for CED tone transfer.

Up until this release, the SIP board could only be configured for either fax relay or modem relay. Now both can be configured per SIP board.

Note that this feature applies to the answering tone that is sent simultaneously; only the fax or modem (depending on what is detected) is sent afterwards.

To support this feature, options [2] and [3] have been added to the existing parameter ‘CED Transfer Mode’. :

Note: For V.150 support, the V.150.1 feature must be present in the installed Feature Key.

2.4.2.17 Support for Gateway Name in SIP Contact Header

This feature provides support for adding the 'Gateway Name' (SIPGatewayName) parameter value to the SIP Contact header. Up until now, the SIP board set the Contact header's value to the board's IP address.

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

This feature provides support for enhanced fax-relay handling upon detection of V.34/Super G3 V8-CM (Call Menu) signals. If the SIP board detects V8-CM signals (or a fax CNG tone) from the originating fax, it sends a SIP re-INVITE with T.38 parameters in the SDP to the terminating fax. Up until this release, the sending of a T.38 re-INVITE was only possible upon detection of fax CNG tones. Detection of the CNG tone is done only if enabled (using the 'CNGDetectorMode' parameter).

2.4.2.19 Support for Re-Negotiation of Coders in re-INVITE for Unhold Calls

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

2.4.2.20 Support for Re-using TCP/TLS Connections without "alias" Requirement

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

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

2.4.2.21 Support for TLS Mutual Authentication per SIP Interface

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

2.4.2.22 Increased Maximum Record-Route Headers in INVITE / 200 OK

This feature provides support for an increase in the maximum number of SIP Record-Route headers supported by the SIP board in received INVITE requests or 200 OK responses. If the SIP board receives an INVITE containing more than 20 Record-Route headers, it responds with a SIP 513 response, indicating that the message is too large for processing.

2.4.3 SIP Gateway Features

2.4.3.1 Support for Tel to IP Forking Group

An incoming Tel call with multiple matched routing rules (e.g., all with the same source prefix numbers) can be sent (forked) to multiple IP destinations if the rules are defined with a Forking Group in the SIP Routing Tel2IP table.

The SIP board sends simultaneous INVITE messages and handles multiple SIP dialogs until one of the calls is answered. When a call is answered, the other calls are dropped.

The parameter 'Forking Group ID' allows the user to define a forking group ID for the routing rule. To enable the Tel2IP call forking feature, the user must set the 'Tel2IP Call Forking Mode' parameter to 'Enable'.

2.4.3.2 Support Line Transfer Mode

This feature allows defining the call transfer method used by the SIP GW when a SIP REFER message was received

The following methods are supported:

- None
- PBX blind transfer
- PBX semi-supervised transfer
- PBX Supervised transfer

2.4.3.3 Improved GW SIP IP-to-Tel Calls Security

Determines the gateway's policy on accepting or blocking SIP IP-to-Tel calls. This is useful in preventing unwanted SIP calls, SIP messages, and/or VoIP spam

This feature is configured by the "Secure Calls from IP" parameter in the SIP General 'Security Settings' pane.

2.4.3.4 Improved IP2Tel Manipulation Table

The 'Source Host Prefix' and the 'Destination Host Prefix' parameters have been added to the following tables:

- IP to Telephone / Inbound Routing Table 'Matching Rules'
- Telephone to IP / Outbound Routing Table 'Matching Rules'
- Number Manipulation Table Parameters

2.4.3.5 Support for Redirect Number Manipulation

This feature enables the customer to add a Redirect Number manipulation rule for IP-to-Tel and Tel-to-IP calls in the GW/IP to IP application.

The feature provides support for manipulating the value of the SIPDiversion, HistoryInfo, or Resource-Priority SIP message headers (including the reason the call was redirected).

2.4.3.6 Support for SIP GW Message Manipulation

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

The 'GW Inbound Manipulation Set' and 'GW OutboundManipulation Set' parameters are configured to support this feature.

2.4.3.7 Improved Destination Phone Number Manipulation for Tel-to-IP

The parameter 'Dest IPGroup ID' allows the customer to set different manipulation rules per destination IP group.

2.4.3.8 Improved 'Use Trunk Group Information'

The following Use Trunk Group Information is now provided:

- 'URC 2008' - the hotline 'Off Hook Indicator' parameter between SIP and ISDN.
- 'Hotline Extended' - Interworks the ISDN Setup message’s hotline 'OffHook Indicator' Information Element (IE) to SIP INVITE’s Request-URI and Contact headers.

2.4.3.9 Support for Calling Name ID Manipulation

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

2.4.3.10 Improved SIP IP to Tel Routing table

The parameter 'Dest Trunk ID' can be defined as a Destination Rule when routing an incoming SIP call to a specific trunk for IP-to-Tel SIP calls.

2.4.3.11 Support for ISDN Facility Trace

The ISDN Facility Trace is now supported. This trace allows customers to trace all of the parameters contained in the Facility IE and to view them in the Syslog.

2.4.3.12 Support for Replacing Calling Number with Redirect Number

This feature enables customer to replace the calling number with the redirect number in ISDN-to-IP calls. In this case, the calling name is deleted and left blank. The outgoing INVITE message does not include the redirect number that was used to replace the calling number. The replacement is performed only if a redirect number is present in the incoming call.

2.4.3.13 Support for Early Media

The feature enables the SIP board to send a 18x response with SDP allowing the establishment of the media stream prior to the answering of the call.

The inclusion of the SDP in the 18x response depends on the ISDN Progress Indicator (PI). The SDP is sent only if PI is set to '1' or '8' in the received Proceeding, Alerting, or Progress PRI messages. This feature also depends on the 'ProgressIndicator2IP' parameter, which if set to '1' or '8', the SIP board behaves as if it received the ISDN messages with the PI.

2.4.3.14 Support for 'Enable Early 183' Feature

The feature enables the gateway to send SIP 183 responses with SDP to the IP upon receipt of INVITE messages. This parameter is applicable to IP-to-Tel (ISDN) and IP-to-IP calls, and applies to all calls.

- IP-to-Tel calls: By sending the 183 response, the gateway opens an RTP channel before receiving the "progress" tone from the ISDN side. The gateway sends RTP packets immediately upon receipt of an ISDN Progress, Alerting with Progress indicator, or Connect message according to the initial negotiation without sending the 183 response again, thereby saving response time and avoiding early media clipping.
- IP-to-IP calls: Sending the 183 response enables SIP servers that require a stream of early media, to keep sessions open

2.4.3.15 Improved SIP PSTN Settings

The following parameters have been added to the SIP PSTN Settings table:

- Use EndPoint Number As Calling Number Tel2IP - enables the use of the B-channel number as the calling number (sent in the 'From' field of the INVITE) instead of the number received in the Q.931 Setup message (for Tel-to-IP calls).
- Use EndPoint Number As Calling Number IP2Tel - enables the use of the B-channel number as the calling party number (sent in the Q.931 Setup message) instead of the number received in the 'From' header of the INVITE, for IP-to-Tel calls.
- Add new parameter to PSTN tunneling – 'QSIG Path Replacement Mode' so the SIP board can interwork consultation call transfer requests for ISDN QSIG-to-IP calls.

2.4.3.16 AudioCodes ELIN Gateway for Lync Server 2010 E9-1-1 Calls to PSTN

The Microsoft Mediation Server sends the location information of the E9-1-1 caller in the XML-based PIDF-LO body contained in the SIP INVITE message. However, this content cannot be sent on the PSTN network using ISDN PRI due to protocol limitations. To solve this issue, Lync Server 2010 requires a PSTN Gateway (*ELIN Gateway*) to send the E9-1-1 call to the PSTN. When Lync Server 2010 sends the PIDF-LO to the PSTN Gateway, it parses the content and translates the calling number to an appropriate ELIN. This ensures that the call is routed to an appropriate PSAP, based on ELIN-address match lookup in the Emergency Services provider's ALI database.

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

2.4.3.17 Connected Number Sub-Address Added to Connect Message

This feature provides support for adding the connected number sub-address to the ISDN Connect message (i.e. the message sent when a call is answered). This feature is supported only for E1 EURO ISDN, QSIG and NTT protocols. This sub-address provides additional information in a phone number for identifying extensions (i.e., the same number may have several extensions).

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

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

2.4.3.19 Improved Trunk Group Setting Table

The Trunk Group Name parameter has been added to the SIP Trunk Group Settings Parameters table.

The 'Channel Select Mode' option has been enhanced with the following values:

- According To Source Number Select
- Trunk Cyclic Ascending
- ISDN Supp Serv Table
- Dest Number Ascending

2.4.3.20 Support of IP-to-Tel Routing based on Source SRD

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

2.4.3.21 Support for SIP Gateway3xx Redirect Responses

The gateway, upon receipt of a 3xx response, should try all contacts in the 3xx response until a successful route is obtained. However, the network SIP board should cease trying additional contacts upon receipt of a 6xx (negative response). It tries the first contact that succeeds in reaching the subscriber; however, the subscriber is busy. The BroadWorks Application Server then returns a 600 Busy Everywhere to indicate that no other contacts should be attempted in trying to reach this specific subscriber.

A new parameter has been added to gateway configuration 'Use Alt Route Reasons for 3xx' in the 'Alternative Routing and Manipulation' pane in the SIP Protocol Settings screen.

2.4.3.22 Support 183 for Early Media per IP Profile

This feature provides support for configuring SIP 183 for early media per IP Profile, thereby allowing early media to be configured for specific calls (Gateway and IP-to-IP application). This is done by associating the IP Profile with a relevant configuration entity such as an IP Group or a routing rule. Up until this release, early media could only be enabled for all calls, using the global parameter, EnableEarly183. Similar to the global parameter, when enabled, the SIP board sends a SIP 183 with SDP response immediately upon receipt of an INVITE request.

2.4.4 SIP SBC Features

2.4.4.1 No Answer Timeout [Sec]

This feature allows the user to define the timeout (in seconds) for SBC outgoing SIP INVITE messages. If the called IP party does not answer the call within this user-defined interval, the SIP board disconnects the session. The SIP board starts the timeout count upon receipt of a SIP 180 Ringing response from the called party. If no other SIP response (for example, 200 OK) is received thereafter within this timeout, the call is released. The valid range is 0 to 3600 seconds (default - 600).

2.4.4.2 P-Asserted-Identity Handle

This feature allows the user to define the SIP board's privacy handling of the P-Asserted-Identity header. This indicates how the outgoing SIP message handles identity. You can configure the following values:

- **[0]** Don't Care (default) = P-Asserted Identity header is not affected.
- **[1]** Add P-Asserted-Identity Header = Adds a P-Asserted-Identity header. The header's values are taken from the source URL.
- **[2]** Remove P-Asserted-Identity Header = Removes the P-Asserted-Identity header.

2.4.4.3 Refer Behavior

This feature determines handling of REFER requests. You can configure the following values:

- **[0]** Transparent = (Default) Refer-To header is unchanged and the gateway forwards the REFER as is.
- **[1]** DB URL = Changes the Refer-To header so that the re-routed INVITE is sent through the SBC:
  - Before forwarding the REFER request, the gateway changes the host part to the gateway's IP address and adds a special prefix ("T~&R_") to the Contact user part.
  - The incoming INVITE is identified as a REFER-resultant INVITE according to this special prefix.
  - The gateway replaces the host part in the Request-URI with the host from the REFER contact. The special prefix remains in the user part for regular classification, manipulation, and routing. The special prefix can also be used for specific routing rules for REFER-resultant INVITEs.
  - The special prefix is removed before the resultant INVITE is sent to the destination.

2.4.4.4 SBC Xfer Prefix

This feature allows the user to replace the prefix with the value defined for the SBCXferPrefix parameter, if the SIP board receives an INVITE with such a prefix.

2.4.4.5 3xx Behavior

This feature determines the handling of SIP 3xx responses. When enabled, the SIP board handles SIP redirections between different subnets (e.g., between LAN and WAN sides). This is required where the new address provided by the redirector (Redirect sever) may not be reachable by the far-end user (FEU) located in another subnet. For example, a far-end user (FEU) in the WAN sends a SIP request via the gateway to a Redirect server in the LAN, and the Redirect server replies with a SIP 3xx response to a PBX in the LAN in the Contact header. If the gateway sends this response as is (i.e., with the original Contact header), the FEU is unable to reach the new destination.

2.4.4.6 GRUU Mode

This feature allows the user to define the Globally Routable User Agent (UA) URI (GRUU) support (according to RFC 5627).

2.4.4.7 Max Forwards Limit

This feature allows the user to define the value of the Max-Forwards SIP header.

2.4.4.8 Minimum Session-Expires

This feature allows the user to define the minimum amount of time (in seconds) between session refresh requests in a dialog, before the session is considered timed out.

2.4.4.9 User Registration Time

This feature allows the user to define the duration of the periodic registrations between the user and the SBC (SBC responds with this value to user).

2.4.4.10 Proxy Registration Time

This feature allows the user to define the duration for which the user is registered in the proxy database (after the SIP board forwarded the REGISTER).

2.4.4.11 Survivability Registration Time

This feature allows to define the duration of the periodic registrations between the user and SBC, when the SBC is in Survivability State (i.e., when REGISTER requests cannot be forwarded to the proxy, and is terminated by the SBC).

2.4.4.12 Keep Original User in Register

This feature allows the user to determine whether the gateway replaces the Contact user with a unique Contact user in the outgoing message in response to a REGISTER request.

2.4.4.13 SBC Coders Preferences Mode

This feature determines the order of the Extension coders (coders added if there are no common coders between SDP offered coders and Allowed coders (defined in the Allowed Coders Group table) in the outgoing SIP message (in the SDP).

2.4.4.14 Bye Authentication

This feature enables the authentication of a SIP BYE request before a call is disconnected.

2.4.4.15 Improved SIP Proxy Server Table

This feature allows the user to define how the SIP board classifies an IP call to the Proxy Set. The call can be classified to the Proxy Set according to its IP address only or according to its IP address, port, and transport type.

This feature is configured by the parameter 'Classification Input' in the SIP Proxy Set Settings table.

2.4.4.16 Improved SIP IP to IP Routing Table

A new parameter 'destinationSRD' allows the customer to determine which SRD they wish to route the call.

A new parameter 'Request Type' in the SBC IP-to-IP Routing Settings Matching Rules pane allows customers to determine the type of incoming SIP request. For example, REGISTER or SUBSCRIBE.

2.4.4.17 Support for SIP IP to IP Transcoding Mode

SIP SBC transcoding mode is now supported. This mode defines the voice transcoding mode (media negotiation) between two user agents for the SBC application. For example, you can restrict the incoming SDP offer. In this case, the SIP board uses only Allowed coders (i.e., only coders common between those in the received SDP offer and the Allowed coders are used). This feature is configured by the parameter 'SBC Coders Mode' in the SIP SBC IP Profile Settings screen.

2.4.4.18 Support for Adding initial Route Header

This feature enables the inclusion of the SIP Route header in initial registration or re-registration (REGISTER) requests sent by the SIP board

When the gateway sends a REGISTER message, the Route header includes either the Proxy's FQDN, or IP address and port according to the configured Proxy Set, for example:

```
Route: <sip:10.10.10.10;lr;transport=udp>
```

or

```
Route: <sip: pcscf-gm.ims.rr.com;lr;transport=udp>
```

2.4.4.19 Session Expires Mode

This feature enables a customer to ignore a new SDP re-offer (from the media negotiation perspective) when a SDP session expires. According to RFC 3264, once an SDP session is established, a new SDP offer is considered only when the origin SDP value is incremented. For scenarios such as session expires, SDP negotiation is irrelevant and thus, the origin field is not changed. This feature is managed by the 'SBC Session Expires Mode' parameter in the SBC IP Profile.

2.4.4.20 Support for SBC Allowed Coders Group Table

The Allowed Coders (Coders Restriction) feature determines the coders that can be used for a specific SBC leg. In other words, the SIP board's SBC application can enforce the use of specific coders, while preventing the use of restricted coders. Coders excluded from the Allowed Coders Group list (restriction list) are removed from the SDP offer (only common coders between SDP offered coders and Allowed Coders are used).

2.4.4.21 Support for SBC Condition Table

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

2.4.4.22 Support for Message Condition Association

The SBC classification table and the SBC IP-to-IP Routing Table 'Matching Rules' table now support the 'Message Condition' parameter, which defines the index of the condition to associate (as defined in the SBC Conditions table). The classification is used only if the classification rule and its associated condition rule are matched.

2.4.4.23 Improved Classification Table - SIP Access List Using Classification

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

2.4.4.24 Support for Manipulation of SIP REGISTER Messages

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

2.4.4.25 Enhanced Anti-Tromboning for LAN User Agents (UAs) and WAN IP PBX

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

By default, media packets traverse the SBC in order to achieve the following:

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

Since media packets traverse the SBC, media quality may degrade (due to, for example, delay). In some setups, specific calls do not require media anchoring, for example, when there is no need for NAT, security, or transcoding. This is typical for calls between users in the LAN:

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

2.4.4.26 Interworking SIP Early Media

This feature provides support for handling SIP early media.

- Early Media Enabling - support for interworking early media between SIP UAs (IP Groups) that support and do not support receipt of early media.
- Early Media Response Type - support for determining the SIP provisional response type – 180 or 183 – to forward the early media to the caller.
- Multiple 18x - support for determining whether multiple 18x responses (including 180 Ringing, 181 Call is Being Forwarded, 182 Call Queued, and 183 Session Progress) are forwarded to the caller.
- Early media RTP- support for interworking with remote clients that send 18x responses with early media; however, consequent RTP is delayed (e.g. Lync), while others do not support this and require RTP to follow the 18x response immediately.

2.4.4.27 Interworking Re-INVITE Messages

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

- Interworking re-INVITE:

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

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

2.4.4.28 Interworking SIP UPDATE Requests

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

2.4.4.29 Interworking Re-INVITE to UPDATE Requests

This feature provides support for enabling communication between endpoints (IP groups) that do not support re-INVITE requests; however support the UPDATE method, and vice versa. The SBC translates the re-INVITE request to the UPDATE request, and vice versa. Note that if a re-INVITE request arrives without SDP, the SBC generates SDP and adds it to the outgoing UPDATE request. To enable this feature, each IP group needs to be configured with its capabilities by associating it with a relevant IP Profile. For example, an IP group that supports UPDATE requests; however not re-INVITEs, would be configured as follows:

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

If a re-INVITE request needs to be forwarded to this IP group, it is translated to an UPDATE request.

2.4.4.30 Interworking Delayed Offer

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

2.4.4.31 Interworking SIP REFER (Call Transfer)

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

This feature enables the configuration of IP groups that do not support REFER. For such IP groups, when the SBC receives a REFER request, instead of forwarding it to the IP Group it handles it locally. The SIP board generates a new INVITE to the alternative destination according to the rules in the IP-to-IP Routing table. The IP-to-IP Routing table has been enhanced to route such "re-route" INVITEs differently to regular INVITE routing. For the SBC to route INVITEs triggered by REFER, the new 'Call Trigger' field in this table must be set to "REFER".

2.4.4.32 Interworking SIP 3xx Redirect Responses

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

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

2.4.4.33 Advanced CAC Reserved Number of Calls per Customer

This feature enables operator to define a 'reserved' number of calls per customer.

SBC will share only resources that weren’t reserved per customers (IP Groups or SRDs).

The sum of the Reserved CACs should be lower than session capacity. The reservation can be configured for the INVITE or REGISTER SIP message type.

2.4.4.34 Support for SIP Call Forking

The SBC supports call forking of an incoming call to multiple SBC users (destinations). Call forking is supported by the SBC capability of registering multiple SIP client user phone contacts (mobile and fixed-line extensions) under the same Address of Record (AOR) in its registration database. This feature can be implemented in the following example scenarios:

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

SBC supports various modes of call forking. For example, in Parallel call forking mode, the gateway sends the INVITE message simultaneously to all the users registered under the same AOR, resulting in the ringing of all extensions; the first extension to pick up the call receives the call, and all other extensions stop ringing. The Call Forking feature is configured by creating a User-type IP Group and configuring the IP Group table's parameter, 'SBC Client Forking Mode'.

2.4.4.35 Support for SIP Forking by SIP Proxy Server

The SBC can handle SIP forking responses received from a proxy server in response to an INVITE forwarded by the gateway from a UA. In other words, received responses with a different SIP To header 'tag' parameter for the request forwarded SIP board. This occurs in scenarios, for example, where a proxy server forks the INVITE request to several UAs, and therefore, the SBC device may receive several replies for a single request. Forked SIP responses may result in a single SDP offer with two or more SDP answers during call setup. The SBC handles this scenario by "hiding" the forked responses from the INVITE-initiating UA. This is achieved by marking the UA that responded first to the INVITE as the active UA, and only requests/responses from that UA are subsequently forwarded. All other requests/responses from other UAs are handled by the SBC (SDP offers from these users are answered with an 'inactive' media).

The SBC supports two forking modes, configured by the SBC Forking Handling Mode parameter:

- Latch On First - only the first received 18x response is forwarded to the INVITE initiating UA, and disregards any subsequently received 18x forking responses (with or without SDP).
- Sequential - all 18x responses are forwarded to the INVITE initiating UA, one at a time in a sequential manner. If 18x arrives with an offer only, only the first offer is forwarded to the INVITE initiating UA.

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

2.4.4.36 Support for User Registration Time per IP Profile

This feature provides support for configuring user registration time for an IP Profile in the IP Profile table. This enables assigning different user registration times between specific calls. Up to now, registration time could only be configured for all calls.

2.4.4.37 Support for Media (RTP) Normalization

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

- Sequence number
- SSRC
- Timestamp

2.4.4.38 Interworking Session Timer Mismatches

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

2.4.4.39 Support for MKI Length Negotiation for SRTP-to-SRTP Calls

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

2.5 Voice Features

2.5.1 Support for Minimum Gap Size

Voice quality monitoring - minimum gap size (number of frames) is now supported.

2.5.2 Support for RTCP XR Collection Server

The SIP Media Settings table includes a new parameter for configuring the RTCP-XR Report Mode IP address of the Event State Compositor (ESC). The VoP board sends RTCP XR reports to the Collection server using SIP PUBLISH messages. The address can be configured as a numerical IP address or as a domain name.

2.5.3 Support for ESC Transport Type

The ESC Transport Type is now supported. This transport layer is used for outgoing SIP dialogs initiated by the SIP board to the RTCP XR Collection server, such as UDP, TCP and TLS.

2.5.4 Support for Acoustic Echo Cancellation

This feature provides support for acoustic echo cancellation (ACE).

These echoes are composed of undesirable acoustical reflections (non-linear) of the received signal (i.e., speaker) which find their way from multiple reflections, such as walls and windows into the transmitted signal (i.e., microphone). Therefore, the party at the far end hears their echo. The VoP board's ACE removes these echoes and sends only the near-end’s desired speech signal to the network (i.e., to the far-end party).

2.5.5 Support for Disabling RTCP when RTP is Inactive

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

2.5.6 Support for Five-Level RTP Redundancy

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

2.5.7 Support for Flexible Combinations of DSP Templates

Up until this release, each VoP board could be configured to use up to two DSP templates, where each DSP template was used by 50% of the calls. As of this version, any combination of DSP templates can be configured for each VoP board. For example, a VoP board can be configured to use DSP Template 1 for 20% of calls and DSP template 2 for 80% of the calls.

2.6 Security Features

2.6.1 Improved Firewall Rules Table

You can now define the source UDP or TCP port (on the remote host) from where packets are sent to the VoP board in the Firewall Rules table.

2.6.2 Support for ARIA Encryption Algorithm for SRTP

This feature provides support for the ARIA algorithm cipher encryption for Secure Real-time Transport Protocol (SRTP). This is an alternative option to the existing support for the AES algorithm. ARIA is a symmetric key-block cipher algorithm standard developed by the Korean National Security Research Institute. The ARIA offered suite supports 128-bit and 192-bit key encryption sizes with HMAC SHA-1 cryptographic hash function.

ARIA encryption is configured by the following parameter:

- 'Aria Media Security' – enables ARIA encryption

For ARIA encryption of SRTP, the VoP board must also be installed with the relevant Feature Key.

2.7 PSTN Features

2.7.1 B-channels Status Indications for PRI

B-channels status indications for PRI enable customer to view when an individual B-channel is 'Out-of-Service' and 'In-service'. Two types of B-channel status indications are provided:

- Alarm generated on the B-channel that are 'In Service' or those that are 'Out of Service' (set and clear alarm)
- Status of B-channels in the Viewing Trunk Channels Status.

2.7.2 Improved ISDN Behavior

The parameter 'ISDN Q931 Layer Response Behavior' has a new bit value 'NS_ACCEPT_ANY_CAUSE'. When this bit is set, the VoP board accepts any Cause information element (IE) value. This behavior bit is applicable only to the ETSI protocol.

2.7.3 Manual D-Channel Switch Over

This feature enables the user to perform switch over from a primary enabled NFAS trunk to its backup enabled NFAS trunk. Both should be unlocked, enabled and in the same NFAS Group.

This page is intentionally left blank.

3 Known Constraints

This section lists the known limitations of Version 6.6 of the carrier class Mediant Media Gateways.

3.1 Management Constraints

This version includes the following management constraints:

- Auxiliary file names provided to the system for loading to TP boards should not contain spaces.
- The 'Graceful Lock' feature does not function correctly when applied to the Redundant TP board when it is backing up for a failed active TP.
- Starting from v6.2, the '-v' option of the tpPing CLI command is deprecated. The command was used to perform PING from a specific interface (where the interface was specified by its type - OAM/media/control). Instead, a new option "-I" is supported by tpPing command:
    - -I interface address. Set source address to specified interface address. Argument may be numeric IP address (e.g. 10.7.9.210)

3.2 IP Networking Constraints

This version includes the following IP networking constraints:

- CALEA termination with UDP checksum does not function correctly. CALEA calls with UDP checksum enabled (either IPv4 or IPv6) will cause the VoP board to restart.
  Workaround: Do not add a CALEA termination if you are working with IPv6 or IPv4 with the UDP Checksum enabled.
- Enabling the UDP checksum calculation is not applied to CALEA and IP-to-IP calls with UDP connections. The UDP checksum field is set to zero in these cases.
- Enabling the UDP checksum calculation is not applied to ‘IP-to-IP’ connections without transcoding. In these cases, the UDP checksum field is set to zero.
- A call cannot be modified between IPv4 and IPv6. Calls that were opened as IPv6 cannot be reactivated to IPv4 and vice-versa.
  Workaround: In order to change a call between IPv4 and IPv6, the call must be closed and reopened with the new IP protocol.
- Debug Recording:
    - Only one IP target is allowed.
    - No more than 50 trace rules are allowed at any one time.
    - No more than 5 media stream recordings are allowed at any one time.

3.3 PSTN Constraints

This version includes the following PSTN constraints:

- All trunks in one blade should belong to the same Trunk Type (either E1 or T1).
- V5.2 Access Gateway Constraints:
  - Only V5.2 LE side (and not AN side) is supported.
  - The V.5.2 Access Gateway application is available for TP-8410 based systems only
  - Only PSTN (POTS) user ports are currently supported (and not ISDN PRI or BRI ports).
  - Only V5.2 is supported (not V5.1).
  - Only Protection Group 1 is supported.
  - Any other trunk in the TP-8410 board, which does not belong to any V5 interface, must be configured as 'E1Transparent'.
  - If the board has no V5.2 trunk configured, the first V5.2 trunk configured on- the-fly necessitates a Lock/Unlock on the TP board.
  - Only V5 trunks have voice capability. Other trunks (e.g. E1transparent) do not have this capability; the user can use these trunks as a clock source.
  - V5.2 re-provisioning procedures as defined in section 14.5 in ETS 300 324-1, are not supported.
  - In order to update the last port configuration of each V.52 Interface, the customer should use the ‘entire’ (complete) file option and not apply the ‘additional’ option. Configuration updates for the other ports can be applied using either method.
- Sometimes (on a very rare occasions), the BIT voice path test running on the Redundant TP board can fail when using the DS3 interface. As a result, an alarm indication is issued to the EMS. In this case, it is suggested to wait until the next periodic BIT test on the Redundant board passes successfully (the next test will run in a one hour’s time).
- When the DS3 interface is not connected, a trunk under this DS3 interface can appear in either a LOF or AIS alarm.
- The BIT voice path can fail when using the DS3 interface.
- The DS3 external clock is not relevant for Asynchronous mapping of DS3 in OC3.
- For SDH/SONET and DS3 interfaces: If a trunk was in LOF alarm and then cleared, the trunk tends to revert to an RAI alarm for a short period before changing to 'clear' (no alarm) state.
- In STM1 and OC3 configurations, path alarms do not display the real state if the higher level is not synchronized. For example, if there is no LOS on both PSTN Port A and Port B, the path level is shown as 'No Alarm'.
- After performing TP switchover, the Trunk RAI alarm is inappropriately cleared, even though the alarm still raised on the far end.

- SS7 Capacity Limitations:
  - Up to two SS7 Nodes can be configured per MTP3 Group (when using Shared-Point Code, only one SS7 Node is supported.)
  - Up to two Alias Point Codes can be configured per SS7 Node; however only one SS7 Node can be configured with Alias Point Codes.
  - Up to 64 SS7 Data Links can be configured per TP board.
  - Up to 32 SS7 Linksets can be configured per SS7 Node.
  - Up to 8 SS7 Linkset Links can be configured per SS7 Linkset.
  - Up to 30 SS7 Routesets can be configured per SS7 Node.
  - Up to 4 SS7 Routes can be configured per SS7 Routeset.
  - Redundant SS7 MTP3 Group: up to two TP boards can be associated with a single redundant MTP3 Group. Multiple MTP3 Groups may be defined in the system.
  - SS7: In order to activate the newly defined SS7 Node, the TP board should be reset.
  - An M3UA Sigtran group cannot be deleted if it is defined on an SCTP port with Active Association
- SIGTRAN (IUA, DUA, M2UA and M3UA) constraints:
  - Only SIGTRAN “Override” mode is supported
  - Textual Interface Identifier is not supported
  - Up to 32 interface groups may be configured per TP board
  - Up to 84 interface IDs can be configured per TP board
  - Up to 32 M3UA Routing Contexts can be configured per Media Gateway board
  - By default, up to three different SCTP ports can be configured per Media Gateway board (It can be increased to up to eight different SCTP ports. For further information, contact AudioCodes).
  - M3UA DAUD messages can contain up to 32 point codes
  - It is not possible to delete entries from the UAL Group table when the corresponding SCTP association is established.
  - Multiple interface groups can be configured on the same SCTP port only for the M3UA application.

3.4 Call Control Constraints

This version includes the following call control constraints:

- The MGCP and MEGACO control protocols are not concurrently supported on the same TP board
- The maximum MKI length in an SRTP packet is 4 bytes.
- The combination of the 'UNAUTHENTICATED_SRTP' SRTP session parameter with either 'UNENCRYPTED_SRTP' and/or 'UNENCRYPTED_SRTCP' is not supported.
- SBC RTP call forwarding using the SRTP tunneling feature cannot provide RTCP XR monitoring parameters (such as MOS) required for the QoE feature on the following variable bit rate coders: G.723, GSM FR, GSM EFR, MS RTA, EVRC, AMR, QCELP, SILK, and Speex. A workaround is to use SRTP full encryption / decryption on the forwarding calls.
- Ethernet packets received on the RTP side of SRTP-RTP SBC sessions must not exceed 1500 bytes. Packets exceeding this size are dropped.
- The Enhanced G.711 vocoder is no longer supported.
- Acoustic Echo Suppression cannot be used together with wideband transcoding. When Acoustic Echo Suppression is enabled, IP-to-IP calls using wideband coders, such as G.722 or AMR-WB do not maintain the wideband quality and consequently, is degraded to narrowband quality.
- If the initial transcoding session has one side using a narrowband coder (e.g. G.711), modifying the transcoding connection to wideband coders still results in narrowband voice quality. A workaround for this constraint is to ensure that the entire session uses wideband coders.
- When performing an IP-to-IP call with a wideband (WB) coder on each leg, if the Fax/Modem Transport type for one of the legs is not Transparent, the interconnection is made using a narrowband coder; therefore, the wideband quality of the call is not maintained. The user should avoid setting any Fax/Modem enhanced capabilities on wideband IP-to-IP calls for which the user wants to maintain wideband quality.
- Announcements and streaming cannot be performed on IP-to-IP wideband calls.
- To change the DSP template, either the Mixed Template table or the DSP Template single values can be used.
- For the Tel-to-IP Call Forking feature (supported by the Gateway application), if a domain name is used as the destination in the Outbound IP Routing table, the maximum number of resolved IP addresses supported by the VoP board's internal DNS that the call can be forked to is three (even if four IP addresses are defined for the domain name).

- For the IP-to-IP application, since the back-to-back user agent (B2BUA) mode is based on full termination at each leg, some SIP requests, headers and URI parameters and message bodies are omitted or changed while traversing the VoP board. Responses to requests within a SIP dialog are always sent independently at each leg, regardless of the other leg's response.
  - The following SIP Methods are omitted by the IP-to-IP application:
    - MESSAGE
    - PUBLISH
    - SUBSCRIBE
    - NOTIFY
    - Out-of-dialog REFER
    - Any other proprietary Method
  - The following SIP message components are omitted by the IP-to-IP application:
    - Message body (other than SDP)
    - Specific parameters in the SIP headers handled by the VoP board (such as To, From, P-Asserted, Diversion, Remote Party ID, and Contact)
    - Specific parameters in the SDP – these parameters may affect the RTP flow at each leg independently
- SIP - Publishing of RTCP XR is sent only at call termination.
- For the MEGACO Call Control protocol:
  - When the fax is set to 'Transparent' mode and fax events are requested, the call must be closed and opened if the fax ended while in this mode and no change to T.38 or Bypass occurred.
  - When sending an empty *eventBuffer* descriptor, the collected events are not erased.
  - The MEGACO descriptors *ModemDescriptor* and *MuxDescriptor* are not supported.
  - The auditCapabilities command returns only part of the parameter values
  - When creating a BCT context, there is no legality check on the topology, i.e., a case in which one termination has two inputs is not handled. Therefore, this might result with one-way voice.
  - Call Agent legality checking according to profile. Any request from an MGC listed in the provisioned Call Agent is executed ('Primary Call Agent IP' and 'Redundant Agents' in the EMS Call Control Settings screen).
  - If the values of 'PCM Input Gain' and 'Echo Canceler' parameters (in EMS 'Media Settings' screen) are changed, this does not affect the next call, only subsequent calls.
  - The **Move** command is not supported on the RTP termination in the 'IP-to-IP' context.
  - The IPv6 media type is not supported in CALEA terminations. CALEA packets are sent in IPv4 format only. The original RTP media type connected to the CALEA termination may be configured with the IPv6 media type.

  - Protocol/size limitations:
    - Maximum contexts in reply to *auditValue* of ALL contexts and Root termination is 2000.
    - Maximum command length is 35000 bytes.
    - Maximum number of transactions per message is 10.
    - Maximum number of actions per transaction is 150.
    - Maximum number of command requests per action is 10.
    - Maximum number of command replies per action is 100.
    - Maximum number of signals in a signal descriptor is 2.
    - Maximum number of signals in a signal list descriptor is 30.
    - Maximum number of reported signals is 50.
    - Maximum number of events in an event descriptor is 16.
    - Maximum number of reported events is 50.
    - Maximum number of observed events is 10.
    - Maximum number of event parameters is 5.
    - Maximum number of audit return parameters is 100.
    - Maximum number of DigitMap alternatives is 32.
    - Maximum length of DigitMap is 150.
    - Maximum dial string length is 30.
    - Maximum length of DigitMap name is 30.
    - Maximum number of the terminations in a BCT/‘IP-to-IP’/PoC context is 20

- The following constraints are applicable when three-level Termination Naming is used in the V5.2 Access Gateway (user configures in EMS- Call Control’ > MGCs > Endpoint names the parameter ‘Physical Termination type’ to the 'V.5.2 SubRack Card Port' value):
  - The Subrack ID ('Interface') MUST be mapped to the internal Interface ID in the V5.2 Interface Table.
  - All TP8410 belonging to the same subrack MUST have the same number of ports.
  - The number of TP boards in a subrack is limited to 253.
- Only one virtual gateway is supported in the following configurations:
  - V5.2 access gateway
  - AMS feature package
  - The gateway controller address is a domain name address.
- Domain Names and IP addresses cannot be mixed in the controllers list (in EMS Call Control > MGCs > CA Address Settings. The parameter ('Address format'). When the controller list contains a domain name, only one row (controller) is allowed to be provisioned in the group.
- The 'Service Change profile' parameter (in EMS Call Control > Virtual GWs > Virtual GW Settings) is limited to 29 characters.

- Auditing a Secured Media Agnostic stream does not return the SRTP Key.
  A Media agnostic stream can use the SRTP encryption. However, an Audit command will only return that the RTP/SAVP is used; however will not return the specific key.
- A warning message may appear in the Syslog while creating an SRTP call.
  During the call setup for an SRTP call, there may be a period in which the key exchange has not finished; however RTCP packets have already been sent from the remote side.
  In this case, the Syslog contains the following warning:
  'WARNING :SRTP_PCK_DROP_AUTH:1'

  The call, however, continues normally.
- When using multiple SDP sessions (starting with “v=0”), the local SDP information is saved only for the first session. This might cause an error in the Syslog in case only the second session of the local SDP matches any session of the remote SDP. Another issue would be if a new remote SDP is received without re-sending the local SDP. **Workaround:** If the call is using multiple SDP sessions, it is recommended to always include the local SDP in future modifications of the call.
- In some cases, the *ServiceChange* command for non-ROOT termination includes the Address field. The address field should be included in the *ServiceChange* command only for the ROOT termination.
- The AMR coder cannot be used for mediation calls. Creating a mediation call using an AMR coder results with no voice and errors appearing in the Syslog.
- The following characters must not be included in the ‘Media Realm Name’ parameter in MEGACO (in EMS Network > Media Realms > Board Realm Settings):
  - ‘/’
  - ‘$’
  - ‘*’.

  Also, the maximum length of the ‘Media Realm Name’ is 39 characters, even though the EMS/CLI Interface allows for entry of 64 characters.
- The following BGF constraints exist in Version 6.6:
  - The dir (direction) parameter of the adid/ipstop signal allows the MGC to determine which direction the data flow should be monitored by the Media Gateway. Currently only the "IN" (default) value is supported.
  - If the “OUT” value is used, an error is generated. If the “BOTH” value is used, no error will be generated and it will be considered as “IN”.
  - When the stream is in SendOnly mode, no adid/ipstop event is generated to the MGC upon connection break.
  - This feature is not supported when no DSP is allocated.

3.5 Voice Constraints

This version includes the following voice constraints:

- When performing an ‘IP-to-IP’ call using a Wide Band (WB) coder on each leg, if the Fax / Modem Transport Type for one of the legs is not 'Transparent', the interconnection does not preserve the WB quality of the call, and instead uses a Narrow Band (NB) interconnection. Therefore, to maintain WB call quality, avoid setting any Fax/Modem enhanced capabilities on WB ‘IP-to-IP’ calls.
- Announcement and Streaming cannot be performed on ‘IP-to-IP’ WB calls.
- RFC 2198 Redundancy mode with RFC 2833 is not supported (i.e., if a complete DTMF digit was lost, it is not reconstructed). The current RFC 2833 implementation does support Redundancy for lost inter-digit information. Since the channel can construct the entire digit from a single RFC 2833 end packet, the probability of such inter-digit information loss is very low.
- The duration resolution of the On and Off time digits when dialing to the network using RFC 2833 relay is dependent on the basic frame size of the coder being used.
- The 'CNG detector Mode' parameter (Media > Media Settings > Fax/Modem Settings screen in the EMS) must be set to ‘disable’ (*Transparent* mode) in order to detect a fax CNG tone received from the TDM, using the Call Progress Tone detector.
- According to RFC 3558, EVRC interleaving is supported only on the receiving side. Support for this mode on the transmitting side is not mandatory.
- 30 msec RTP frames using the EG.711 coder is not supported.
- Playback with Duration set to less than 20 msec is not supported.
- The RTP payload size on RTP forwarding in SBC applications cannot exceed 1000 bytes.
- When an initial transcoding session has one of the sides using an NB coder (e.g. G.711), modifying the transcoding connection to WB coders still results in NB voice quality.
  Workaround: Restart the whole session using WB coders.
- Transparent Coder (RFC 4040) limitations:
  - The coder can be used only when using a physical termination.
  - No detection IBS (e.g. DTMF)
  - Generation of IBS only towards the network
  - No fax/modem detection/generation. i.e. no support for T.38 & Bypass as well.

    Workaround: Use G.711 coder instead.
- The 'NetCoder' vocoder is not supported.

3.6 Security Constraints

This version includes the following security constraints:

- This version supports up to four IPSEC/IKE proposals for each SC IPSEC rule (previously eight proposals could be configured). The conversion of legacy configurations where encryption was set to “any”, causes the loss of specific encryption/authentication permutations. Consequently, it is converted to the following proposals:
    - modp768, DES, MD5
    - modp768, DES, SHA1
    - modp1024, 3DES, MD5
    - modp1024, 3DES, SHA1

The risk of an inappropriate conversion is considered low, since the new configuration encompasses the most commonly used permutations.

3.7 High-Availability and Infrastructure Constraints

This version includes the following HA and infrastructure constraints:

- Systems utilizing IPSec for control protocol transport, may experience a large bulk of Syslog error messages during TP board switchover. These messages can be ignored as they do not affect the switchover and the connection with the SSW is restored.
- During the TP board HA switchover process; the APS active interface status is not preserved. For example, prior to switchover, the PSTN-B is currently “Active” and PSTN-A is 'Inactive'. Following the switchover, the status for each PSTN interface is not updated (i.e. PSTN A should display 'Active' and PSTN B should display “Inactive”).
- When boards with different application types (such as Gateway and 'IP-to-IP') are added to the same Redundancy Group, the 'Redundancy mode' may be degraded to 'None'.

3.8 Hardware Constraints

The following tables describe the supported TP board loads for the Mediant 8000 Media Gateways.

Table 3-1: Maximum Loads (Number of Boards) for Mediant 8000 Media Gateway

Supported Protocol	Maximum Number of Boards	
	TP-6310	**TP-8410**
SIP	7+1	6+1
MEGACO/MGCP	8+1	6+1

This version includes the following additional hardware constraints:

- This load does not support the TP-1610 platform. TP-1610 hardware platform users should not upgrade their system to Version 6.6.
- This load does not support a mixture of the TP-6310 and TP-8410 hardware platforms in the same chassis using the Multiple Redundancy groups feature.
- The only combination of different hardware platforms supported in the Mediant 8000 chassis using the Multiple Redundancy groups feature is for the OC3/STM1 and T3 based TP boards.
- This load does not support IPmedia 5000/IPmedia 8000 systems. IPmedia users should not upgrade their system to Version 6.6.
- **ES-2 Ethernet Switch:**
  - Link Aggregation Control Protocol (LACP) protocol is not supported; therefore customer should not configure link aggregation on the Switch/Router side using this protocol. For example, configuration of CISCO L3 switch should be 'c 1 mode on' instead of 'channel-group 1 mode active'. Instead ES-2 supports logical link failure detection feature (for details, see Section 2.2.4 on page 14).

This page is intentionally left blank.

AudioCodes Large Enterprise and Carrier Class Media Gateways

Release Notes

Mediant™ 8000

Version 6.6

Document #: LTRT-90924