AudioCodes CPE & Access Analog Gateways

SIP

MediaPack™ MP-124 & MP-11x

Release Notes

Version 5.6

Document #: LTRT-65611

September 2008

Table of Contents

List of Figures

List of Tables

Notice

This document describes the release of the AudioCodes MP-11x and MP-124 MediaPack Series of Voice over IP (VoIP) media gateways.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered customers at http://www.audiocodes.com/support.

This document is subject to change without notice.

Date Published: Sep-14-2008 Date Printed: Sep-15-2008

Tip: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press the **ALT** and ← keys

Trademarks

AC logo, Ardito, AudioCoded, AudioCodes, AudioCodes logo, CTI², CTI Squared, InTouch, IPmedia, Mediant, MediaPack, MP-MLQ, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, 3GX, TrunkPack, VoicePacketizer, VoIPerfect, What's Inside Matters, Your Gateway To VoIP, are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners.

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 service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used. Only industry-standard terms are used throughout this manual.

Related Documentation

Document #	Manual Name
LTRT-523xx (where *xx* denotes the document version)	Product Reference Manual
LTRT-665xx	CPE SIP Configuration Guide for IP Voice Mail
LTRT-654xx	MP-11x & MP-124 SIP User's Manual
LTRT-598xx	MP-11x & MP-124 SIP-MGCP Installation Guide

Notes:

- Throughout this manual, the terms *MediaPack* or *device* refer to the MP-124, MP-118, MP-114, and MP-112 VoIP gateways.
- Throughout this manual, the term *MP-11x* refers to the MP-118, MP-114, and MP-112 MediaPack series VoIP gateways.

1 What's New in Release 5.6

Note: This document uses a one-row table convention to indicate the products for which each feature is applicable. The products that don't support the feature are shaded (grayed). In the example below, the feature would be applicable only to MP-11x FXS.

MP-124	MP-11x	FXS	FXO

1.1 Supported Hardware Platforms

1.1.1 New Products Introduced in this Release

The following new product has been introduced in this release:

- MP-124 Rev. D for DC power.

1.1.2 Support of the Existing Hardware Platforms

The following existing hardware platforms are supported in this release:

- MP-11x combined FXS/FXO devices:
  - MP-114/FXS+FXO providing 2 FXS ports and 2 FXO ports
  - MP-118/FXS+FXO providing 4 FXS ports and 4 FXO ports
- MP-11x/FXO devices:
  - MP-118/FXO providing 8 analog FXO interfaces
  - MP-114/FXO providing 4 analog FXO interfaces
- MP-11x/FXS devices:
  - MP-118/FXS providing 8 analog FXS interfaces
  - MP-114/FXS providing 4 analog FXS interfaces
  - MP-112/FXS providing 2 analog FXS interfaces
- MP-124/FXS providing 24 analog FXS interfaces

1.1.3 Hardware Platforms No Longer Supported

Not applicable.

1.2 General Gateway New Features

The device supports the following new gateway features:

1. **Immediate Release of Tel-to-IP Call when Device Receives 401/407 Response:**

MP-124	MP-11x	FXS	FXO

If the device's default password has never been modified and an "Authentication Required" SIP response (401/407) is received, the call is immediately released (and a SIP Re-INVITE message is not sent).

2. **Play Busy Tone to IP Upon Call Failure (FXO):**

MP-124	MP-11x	FXS	FXO

In previous releases, when the FXO device operated in Automatic Dialing mode, there was no method to inform the caller that the Tel-to-IP call failed. The reason was that the FXO device does not seize the line until a SIP 200 OK response is received. A new option has been added which allows the device to play a Busy/Reorder tone to the TDM line if a SIP error response (4xx, 5xx or 6xx) is received. The FXO device seizes the line (off-hook) if a SIP error response is received and plays a Busy/Reorder tone to the TDM side for the duration defined by the TimeForReorderTone parameter. After playing the tone, the line is released (on-hook).

Relevant parameter: *FXOAutoDialPlayBusyTone*.

3. **Play Comfort Tone to FXS/FXO Endpoints:**

MP-124	MP-11x	FXS	FXO

The device now supports the option to play a Comfort Tone to the FXS or FXO endpoint. Typically, immediately after dialing is complete, a SIP INVITE message is sent and after a certain period of time, a SIP 18x response is received. During this time interval (i.e., after sending the INVITE and before receiving a 18x), the device plays a Comfort Tone to the endpoint.

Relevant parameter: *EnableComfortTone*.

4. **Hold Timeout:**

MP-124	MP-11x	FXS	FXO

The device now supports the option to keep a call on-hold for a user-defined time before disconnecting the call.. If a hold request (SIP Re-INVITE) is received from the IP side, a timer is started. Unless a Retrieve request is received, once the timer expires the call is disconnected.

Relevant parameter: *HeldTimeout*.

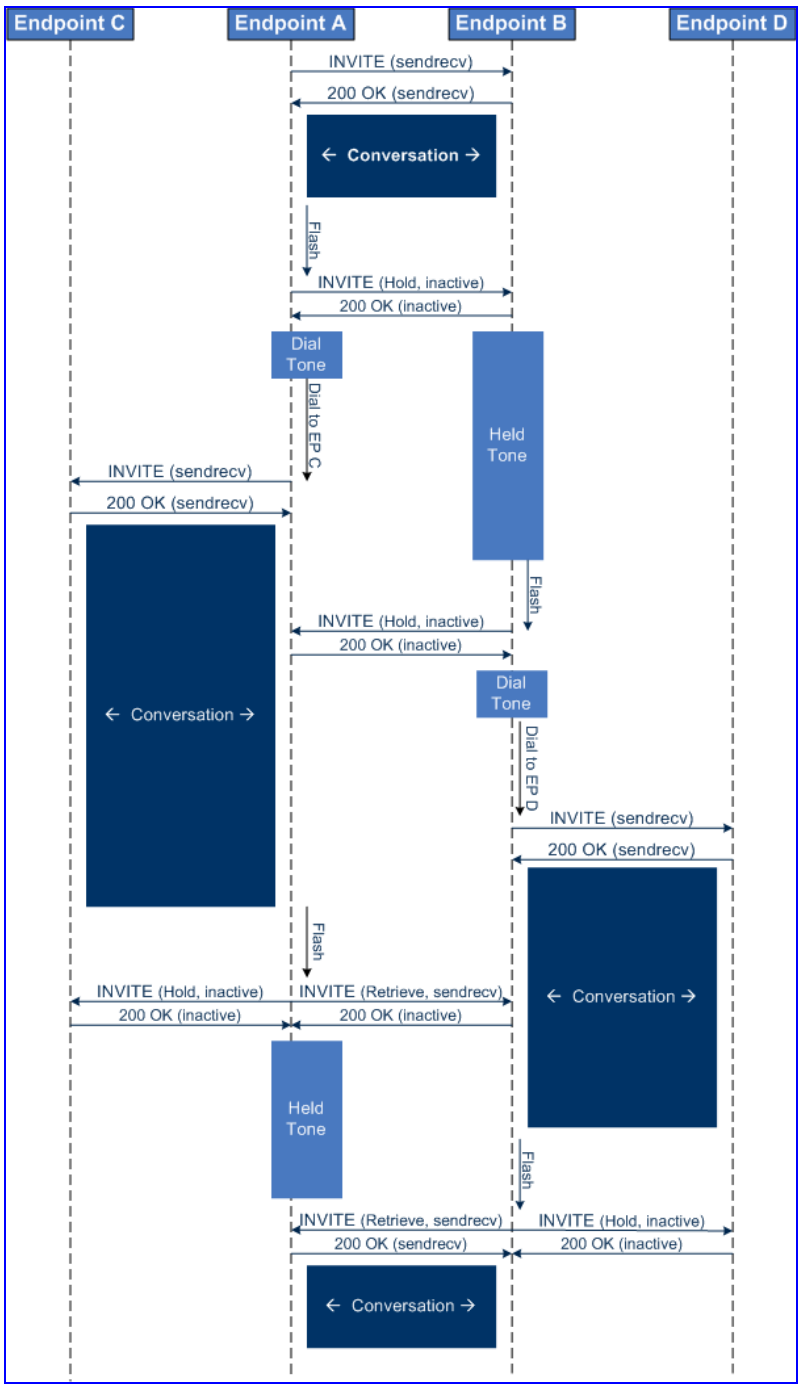
5. "Double Hold":

MP-124	MP-11x	FXS	FXO

The device now supports a “Double Hold” scenario where a Held party can send a Hold Re-INVITE to the other side.

Example call flow:

Figure 1-1: Double Hold SIP Call Flow



Notes:

- Call Transfer: while in a Double Hold state, placing the phone on-hook disconnects both calls (i.e. call transfer is not performed).
- Call Waiting: now supported while on-hold. The endpoint hears the Call Waiting tone instead of the Held tone.

6. Additional Parameters in IP and Tel Profile Pages:

MP-124	MP-11x	FXS	FXO

The IP and Tel Profile pages provide additional parameters to perform the following:

- IP Profile: Enables or disables the Broken Connection mechanism.
- Tel Profile:
  - Enables or disables DID Wink.
  - Selects the Dialing Mode (One-Stage or Two-Stage).
  - Enables or disables disconnection of the call upon detection of a Busy tone.

Relevant parameters: *IPProfile*; *TelProfile*.

7. Maximum Row Entries Increased in Destination Number Manipulation Tables:

MP-124	MP-11x	FXS	FXO

The maximum number of row entries in the Destination Number Manipulation tables has been increased to 100.

Relevant parameters: *NumberMapTel2IP*; *NumberMapIP2Tel*.

8. Maximum Row Entries Increased in Tel-to-IP Source Number Manipulation Table:

MP-124	MP-11x	FXS	FXO

The maximum number of row entries in the Tel-to-IP Source Number Manipulation table has been increased to 120 rows.

Relevant parameter: *SourceNumberMapTel2IP*.

9. Maximum Row Entries Increased in the Internal DNS Table:

MP-124	MP-11x	FXS	FXO

The maximum number of row entries in the Internal DNS table has been increased to 20. In addition, each row now supports up to four different IP addresses.

Relevant parameter: *DNS2IP*.

10. Fields 'Source Trunk Group and 'Source IP Group' Added to Manipulation Tables:

MP-124	MP-11x	FXS	FXO

New columns were added to the Destination and Source Number Tel-to-IP Manipulation tables to allow manipulation according to Source Trunk Group or Source IP Group.

Relevant parameters: *NumberMapTel2IP*; *SourceNumberMapTel2IP*.

11. SRTP Enhancements:

MP-124	MP-11x	FXS	FXO

The device now supports the following enhancements when using Secure Real-time Transport Protocol (SRTP):

- Generates and uses a Master Key Identifier (MKI) value on outgoing SRTP streams (in addition to existing support for incoming SRTP streams).
- Supports SRTP/SRTCP attributes as defined in RFC 4568 (SDP Security Descriptions for Media Streams) - UNAUTHENTICATED_SRTP, UNENCRYPTED_SRTCP, and UNENCRYPTED_SRTP.

Relevant parameters: *SRTPTxPacketMKISize*; *RTPAuthenticationDisableTx*; *RTPEncryptionDisableTx*, *RTCPEncryptionDisableTx*.

12. MLPP Enhancements:

MP-124	MP-11x	FXS	FXO

The device's support for the Multi-Level Precedence and Preemption (MLPP) protocol has been enhanced to support Supplementary Services scenarios such as:

- Call Hold
- Call Transfer
- Call Waiting
- 3-Way Conference (using an external Media Server)

For a detailed description of the MLPP implementation using SIP, please refer to the device's *User's Manual*.

13. Distinctive Ringback Tones:

MP-124	MP-11x	FXS	FXO

The device can now play a specific Ringback Tone defined in the Call Progress Tones file. This option enables an Application server to request the device to play a distinctive Ringback tone to the calling party, according to the destination of the call. The tone is played according to the Alert-Info header received in the 180 Ringing SIP response.

Relevant parameter: *FirstCallRBTId*.

14. Play Tone upon Alternative Routing:

MP-124	MP-11x	FXS	FXO

The device can now play a tone whenever Alternative Routing is used. Each time an alternate route is found, a tone is played for a user-defined duration. Once the tone has finished playing, the new SIP INVITE is generated toward the new destination.

Note: Tone Type #25 must be defined in the Call Progress Tones (CPT) file.

Relevant parameter: *AltRoutingToneDuration*.

15. New Re-Routing Options for Redirect / Transfer Scenarios:

MP-124	MP-11x	FXS	FXO

When a call initiated by the device is re-directed (i.e., a 3xx SIP response is received) or transferred (i.e., a SIP REFER request is received), several re-routing options can now be selected:

- Send INVITE messages directly to the URI (according to the Refer-To header in the REFER message or Contact header in the 3xx response).
- Send a new INVITE message to the Proxy.
- Use the Routing table to locate the destination and then send the new INVITE to this destination.

This feature can be applied per device or per IP Group.

Note: This feature replaces the existing SendINVITEToProxy parameter.

Relevant parameters: *SIPReroutingMode*; *IPGroup*.

16. Wildcards Support in TLS Certificates:

MP-124	MP-11x	FXS	FXO

The device now supports the receipt of wildcards ('*') in X.509 Certificates when establishing TLS connections. These wildcards can be part of the CN attribute of the Subject field or the DNSName attribute of the SubjectAltName field.

17. Multiple Digits in Dialing Plan Notation:

MP-124	MP-11x	FXS	FXO

Currently, the dialing plan for destination/source prefixes in the Routing and Manipulation tables support the following notations:

- [n-m] - represents a range of numbers.
- [n,m] - represents multiple numbers.
- [2,3,4]xxx# - pound sign (#) at the end of a number represents the end of a number.

In previous releases, the [n,m] format only supported single-digit numbers. From this release, it is now possible to use multiple digits (up to three digits) such as [11,22,33] or [111,222,333]. The Dialing Plan notation is applicable to all manipulation and routing tables.

18. **Time Interval between SIP OPTIONS Messages for IP Connectivity:**

MP-124	MP-11x	FXS	FXO

It is now possible to configure the time interval between SIP OPTIONS Keep-Alive messages used for the IP Connectivity application.

Relevant parameter: *AltRoutingTel2IPKeepAliveTime*.

19. **Add Prefix for Blind Transfer:**

MP-124	MP-11x	FXS	FXO

The device now supports the option to add a prefix to the number defined in the SIP Refer-To header for FXO Blind Transfer modes (LineTransferMode = 1, 2 or 3).

Relevant parameter: *XferPrefixIP2Tel*.

20. **Increased PRT Buffer Size:**

MP-124	MP-11x	FXS	FXO

The pre-recorded tone (PRT) buffer size has been increased from 100 to 200 Kbytes.

21. **Configurable T.38 Fax Maximum Buffer Value in SDP:**

MP-124	MP-11x	FXS	FXO

The device now supports specifying the maximum T.38 buffer size supported by the device. This value is included in the outgoing Session Description Protocol (SDP).

Relevant parameter: *T38FaxMaxBufferSize*.

22. **RSA Keys in SSH:**

MP-124	MP-11x	FXS	FXO

The device's internal Secure Shell (SSH) server now supports RSA public keys. By default, SSH uses the same user name and password as the Telnet and Web servers. In addition, SSH supports 1024-bit RSA public keys, which provide carrier-grade security. The device can now be configured with an administrator RSA key as a means of strengthening authentication. For information on implementing public keys for SSH, refer to the *Product Reference Manual*.

Relevant parameters: *SSHAdminKey; SSHRequirePublicKey*.

23. **Fax/Modem Bypass Output Gain Configuration:**

MP-124	MP-11x	FXS	FXO

It is now possible to determine fax and/or modem bypass output gain values by fine-tuning the level of appropriate output signals in bypass (VBD) mode.

Relevant parameters: *FaxBypassOutputGain*; *ModemBypassOutputGain*.

24. **Sends RFC 2833 ANS/ANSam Events Upon Fax/Modem Answer Tones:**

MP-124	MP-11x	FXS	FXO

The device can now be configured to send RFC 2833 ANS/ANSam events upon detection of fax and/or modem answer tones (i.e., CED tone).

Relevant parameter: *FaxModemNTEMode*.

1.3 SIP New Features

The device supports the following new SIP features:

1. **Different SAS Modes:**

MP-124	MP-11x	FXS	FXO

It is now possible to configure the device's Stand-Alone Survivability (SAS) application to operate in different Survivability modes:

- Immediately operate in Emergency Mode, by setting the parameter SASProxySet to -1. In this case, the SAS application does not send keep-alive messages to the configured Proxy server and handles the incoming REGISTER and INVITE messages according to the Emergency mode settings.
- Operate according to the regular Normal/Emergency logic, but while in Normal mode, REGISTER requests are ignored, thereby forcing registering endpoints to switch to the serving Proxy (instead of the SAS application).

Relevant parameter: *SASSurvivabilityMode*.

2. **Cascading SAS Servers:**

MP-124	MP-11x	FXS	FXO

The SAS application now supports cascading of several SAS servers. Each SAS application can use a Proxy Set as a redundancy mechanism. The SAS application uses the Proxy Keep-Alive mechanism to verify the status of each IP address defined in the Proxy Set (marks each server as Online or Offline).

Relevant parameter: *RedundantSASProxySet*.

Each time a new SIP request arrives, the SAS application checks whether the user is listed in the registration database. If the user is listed in the database, the request is sent to the specific user. If the user is not found, the request is forwarded to the next redundant SAS, defined in the Redundant SAS Proxy Set. If this specific SAS IP address appears in the SIP 'via' header of the request, it is not forwarded (this prevents loops in the request's course). If no such redundant SAS exists, the SAS sends the request to its default gateway (defined by the parameter SASDefaultGatewayIP).

Figure 1-2: Cascading SAS Example

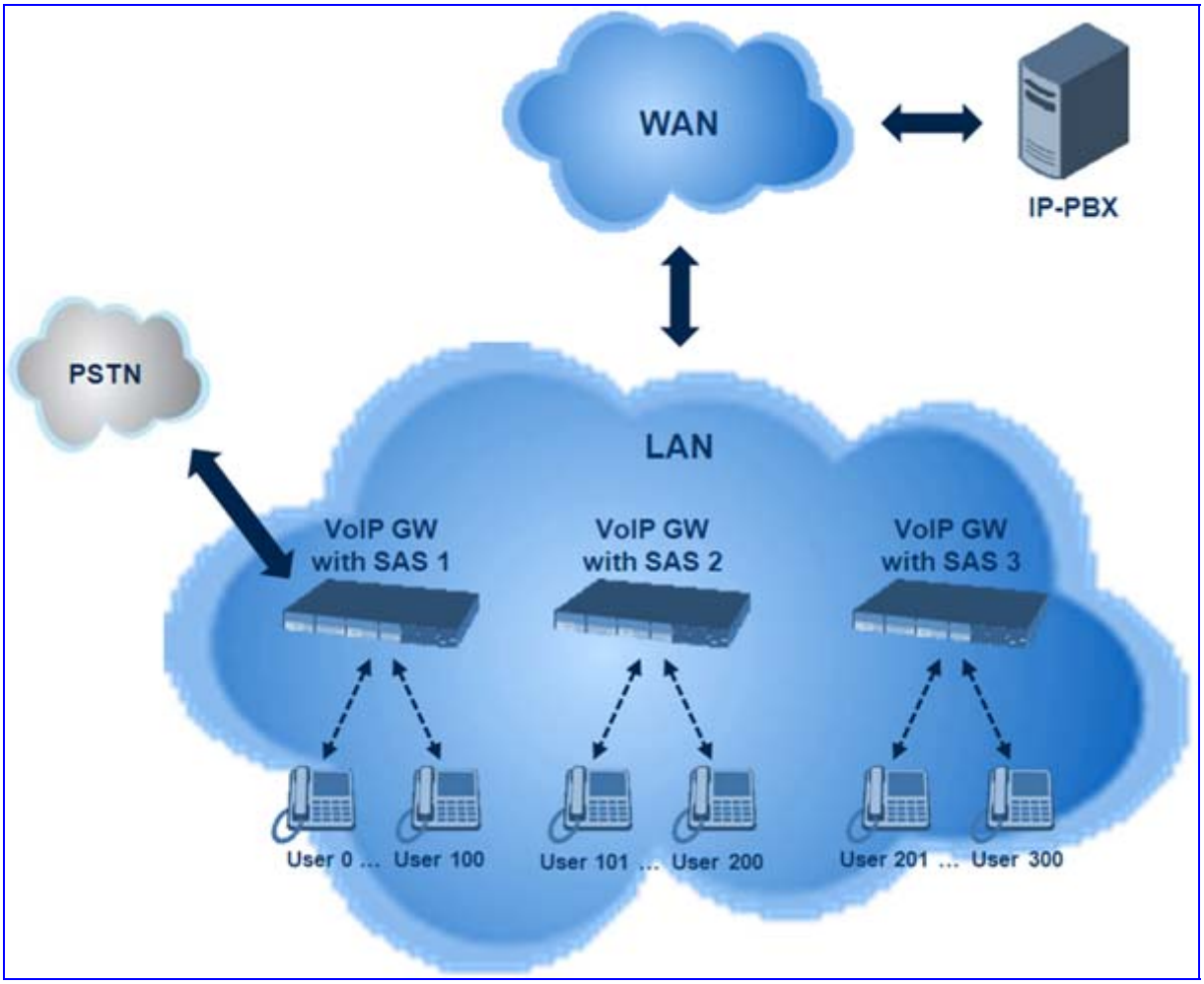
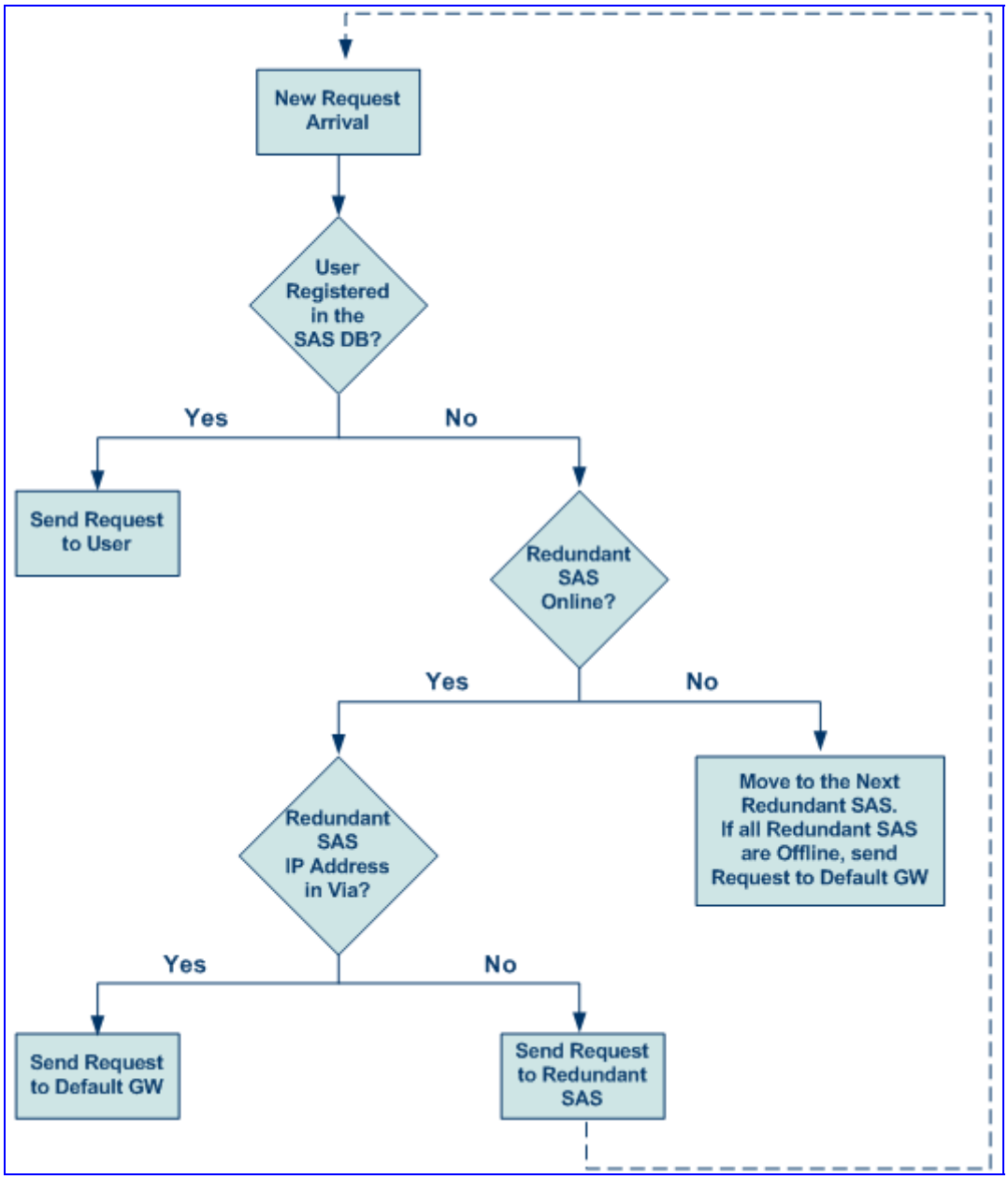


Figure 1-3: Flowchart of SAS Process

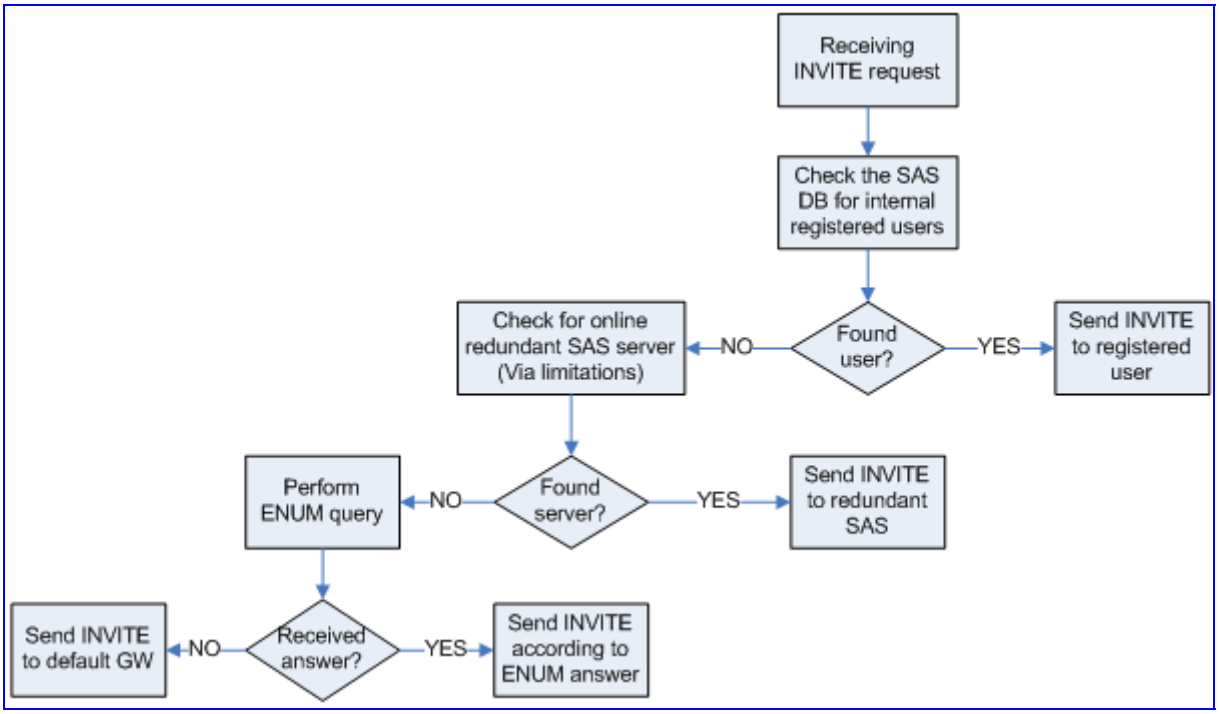


3. ENUM Support for SAS Application:

MP-124	MP-11x	FXS	FXO

A new option was added to the SAS application allowing Telephone Number Mapping (ENUM E.164) capabilities to route incoming INVITE requests. Once an INVITE is received in Emergency mode, the SAS database of registered users is searched for a matching Address-Of-Record (AoR). If not found, the Redundant SAS servers are searched. If there is still no match, an ENUM query is performed and the response is used to correctly route the INVITE.

Figure 1-4: ENUM Support for SAS Application



Note: The call flow depicted above is applicable only when SAS is in Emergency Mode.

Relevant parameter: *SASEnableENUM*.

4. Manipulation of AoR in Incoming REGISTER Requests for SAS Applications:

MP-124	MP-11x	FXS	FXO

The SAS application now supports an option to manipulate the User-Part of an incoming REGISTER request Address-Of-Record (AoR) before saving it to the registered users database. The manipulation can include removing a certain number of digits from the right end of the number (i.e., suffix) or alternatively, to keep only a certain number of digits from the right end of the number (referred to as “short numbering”). The registered database contains the AoR before and after the manipulation.

Note: The parameter SASShortNumberLength is now obsolete.

Relevant parameter: *SASRegistrationManipulation*.

1.4 Web New Features

The device supports the following new Web interface feature:

1. **Improved Interface for Manipulation Tables:**

MP-124	MP-11x	FXS	FXO

The Manipulation tables (Tel-to-IP and IP-to-Tel source and destination numbers) GUI interface has been enhanced to allow adding, deleting, and modifying of individual row entries.

1.5 SNMP New Features

The device supports the following new SNMP features:

1. **SNMP Alarm Raised when in SAS Emergency Mode:**

MP-124	MP-11x	FXS	FXO

The SAS application now generates an SNMP alarm when switching from “Normal" mode to “Emergency" mode. This alarm is cleared once the SAS returns to “Normal" mode.

2. **SNMP Actions for X.509 Certificates:**

MP-124	MP-11x	FXS	FXO

The following SNMP actions were added for X.509 certificates:

- acSysSecurityGenCsrSubjectName: Generates a certificate-signing request using the provided name
- acSysSecuritySelfSignedCertificateSubjectName: Generates a Self-Signed Certificate using the provided name.

1.6 New Parameters

The table below describes the new parameters for Release 5.6. Most of these new parameters can be configured using both the *ini* file (enclosed in square brackets) and the Web interface.

Table 1-1: Release 5.6 New Web / [ini File] Parameters

Parameter	Description
Held Timeout **[HeldTimeout]**	Determines the time interval that the device can allow a call to remain on hold. If a Resume (un-hold Re-INVITE) message is received before the timer expires, the call is renewed. If this timer expires, the call is released. ▪ **[-1]** = The call is placed on hold indefinitely until the initiator of on hold retrieves the call again(default). ▪ **[0 - 2400]** =Time to wait in seconds, after which the call is released.
[EnableComfortTone]	Determines whether the device plays a Comfort Tone (Tone Type #18) to the FXS/FXO endpoint after a SIP INVITE is sent and before a 18x response is received. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
[XferPrefixIP2Tel]	Defines the prefix that is added to the destination number received in the SIP Refer-to header (in IP-to-Tel calls). This parameter is applicable for FXO Blind Transfer modes (LineTransferMode = 1, 2 or 3). The valid range is a string of up to 9 characters. The default is an empty string.
Alt Routing Tone Duration **[AltRoutingToneDuration]**	Determines the time period (in milliseconds) that the device plays a tone on each Alternative Routing attempt. When the tone finishes playing, a new SIP INVITE message is generated toward the new destination. The tone played is the Call Forward Tone (i.e., Tone Type #25 in the CPT file). The valid range is 0 to 20,000. The default time is 0 (i.e., no tone is played).
SAS Proxy Set **[SASProxySet]**	Determines the Proxy Set (index number) used in SAS Normal mode to forward REGISTER and INVITE requests from the users that are served by the SAS application. The valid range is 0 to 5. The default value is 0 (i.e., default Proxy Set).
Redundant SAS Proxy Set **[RedundantSASProxySet]**	Determines the Proxy Set (index number) used in SAS Emergency mode for fallback when the user is not found in the Registered Users database. Each time a new SIP request arrives, the SAS application checks whether the user exists in the registration database. If the user is located in the database, the request is sent to the user. If the user is not found, the request is forwarded to the next redundant SAS defined in the Redundant SAS Proxy Set. If that SAS Proxy IP appears in the Via header of the request, it is not forwarded (so that loops are prevented in the request's course). If no such redundant SAS exists, the SAS sends the

Parameter	Description
	request to its default gateway (configured by the parameter SASDefaultGatewayIP). The valid range is -1 to 5. The default value is -1 (i.e., no redundant Proxy Set).
[SASSurvivabilityMode]	Determines the Survivability mode used by the SAS application. ▪ **[0]** Standard = All incoming INVITE and REGISTER requests are forwarded to the defined Proxy list in SASProxySet in Normal mode and handled by the SAS application in Emergency mode (default). ▪ **[1]** Always Emergency = The SAS application does not use Keep-Alive messages towards the SASProxySet and instead, always operates in Emergency mode (as if no Proxy in the SASProxySet is available). ▪ **[2]** Ignore REGISTER = Use regular SAS Normal/Emergency logic (same as option 0) but when in Normal mode, incoming REGISTER requests are ignored.
[SASBindingMode]	Determines the SAS application database binding mode. ▪ **[0]** URI = If the incoming AoR in the INVITE requests is using a 'tel:' URI or 'user=phone' is defined, the binding is performed according to the user part of the URI only. Otherwise, the binding is according to the entire URI, i.e., User@Host (default). ▪ **[1]** User Part only = The binding is always performed according to the User Part only.
[SASEnableENUM]	Determines whether the SAS application uses ENUM queries to route incoming INVITE requests when in Emergency mode. Once an INVITE is received in Emergency mode, the SAS database of registered users is searched for a matching AoR. If not found, the Redundant SAS servers are searched. If there is still no match, an ENUM query is performed and the response is used to correctly route the INVITE. If no response is received from the ENUM server, the INVITE is routed to the default gateway. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
[SASRegistrationManipulation]	This ini file table parameter is used by the SAS application to manipulate the User-Part of an incoming REGISTER request AoR (the To header), before saving it to the registered users database. The format of this table parameter is as follows: [SASRegistrationManipulation] FORMAT SASRegistrationManipulation_Index = SASRegistrationManipulation_RemoveFromRight, SASRegistrationManipulation_LeaveFromRight; [\SASRegistrationManipulation] ▪ RemoveFromRight = number of digits removed from the right side of the User-Part before saving to the registered user database.

Parameter	Description
	▪ LeaveFromRight = number of digits to keep from the right side. If both RemoveFromRight and LeaveFromRight are defined, the RemoveFromRight is applied first. The registered database contains the AoR before and after the manipulation. The range of both RemoveFromRight and LeaveFromRight is 0 to 30. **Note:** This table can include only one index entry.
SIP Rerouting Mode **[SIPReroutingMode]**	Determines the routing mode after a call redirection (i.e., a 3xx SIP response is received) or transfer (i.e., a SIP REFER request is received). ▪ **[0]** Standard = INVITE messages that are generated as a result of Transfer or Redirect are sent directly to the URI, according to the Refer-To header in the REFER message or Contact header in the 3xx response (default). ▪ **[1]** Proxy = Sends a new INVITE to the Proxy. **Note:** Applicable only if a Proxy server is used and the parameter AlwaysSendtoProxy is set to 0. ▪ **[2]** Routing Table = Uses the Routing table to locate the destination and then sends a new INVITE to this destination. **Notes:** ▪ When this parameter is set to [1] and the INVITE sent to the Proxy fails, the device re-routes the call according to the Standard mode [0]. ▪ When this parameter is set to [2] and the INVITE fails, the device re-routes the call according to the Standard mode [0]. If DNS resolution fails, the device attempts to route the call to the Proxy. If routing to the Proxy also fails, the Redirect / Transfer request is rejected. ▪ When this parameter is set to [2], the XferPrefix parameter can be used to define different routing rules for redirected calls. ▪ This parameter is disregarded if the parameter AlwaysSendToProxy is set to 1.
Master Key Identifier (MKI) Size **[SRTPTxPacketMKISize]**	Determines the size (in bytes) of the Master Key Identifier (MKI) in SRTP Tx packets. The range is 0 to 4. The default value is 0.
Disable Authentication On Transmitted RTP Packets **[RTPAuthenticationDisableTx]**	On a secured RTP session, this parameter determines whether to enable Authentication on transmitted RTP packets. ▪ **[0]** Enable (default) ▪ **[1]** Disable

Parameter	Description
Disable Encryption On Transmitted RTP Packets **[RTPEncryptionDisableTx]**	On a secured RTP session, this parameter determines whether to enable Encryption on transmitted RTP packets. ▪ **[0]** Enable (default) ▪ **[1]** Disable
Disable Encryption On Transmitted RTCP Packets **[RTCPEncryptionDisableTx]**	On a secured RTP session, this parameter determines whether to enable Encryption on transmitted RTCP packets. ▪ **[0]** Enable (default) ▪ **[1]** Disable
Alt Routing Tel to IP Keep Alive Time **[AltRoutingTel2IPKeepAliveTime]**	Defines the time interval (in seconds) between SIP OPTIONS Keep-Alive messages used for the IP Connectivity application. The valid range is 5 to 2,000,000. The default value is 60.
[RemoveToTagInFailureResponse]	Determines whether the device removes the 'to' header tag from final SIP failure responses to INVITE transactions. ▪ **[0]** = Do not remove tag (default). ▪ **[1]** = Remove tag.
[FXOAutoDialPlayBusyTone]	Determines whether the FXO device plays a Busy/Reorder tone to the TDM side if a Tel-to-IP call is rejected by a SIP error response (4xx, 5xx or 6xx). The FXO device seizes the line (off-hook) if a SIP error response is received and plays a Busy/Reorder tone to the TDM side for the duration defined by the parameter TimeForReorderTone. After playing the tone, the line is released (on-hook). ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
[SSHAdminKey]	Determines the RSA public key for strong authentication to logging in to the Secure Shell (SSH) interface (if enabled). The value should be a base64-encoded string. The value can be a maximum length of 511 characters. For additional information, refer to the *Product Reference Manual*.
[SSHRequirePublicKey]	Enables or disables RSA public keys for SSH. ▪ **[0]** = RSA public keys are optional, if a value is configured for the *ini* file parameter SSHAdminKey (default). ▪ **[1]** = RSA public keys are mandatory.
[FaxBypassOutputGain]	Defines the fax bypass output gain control. The range is -31 to +31 dB, in 1-dB steps. The default is 0 (i.e., no gain).
[ModemBypassOutputGain]	Defines the modem bypass output gain control. The range is -31 dB to +31 dB, in 1-dB steps. The default is 0 (i.e., no gain).
[T38FaxMaxBufferSize]	Defines the maximum size (in bytes) of a T.38 buffer supported by the device. This value is included in the outgoing SDP when T.38 is used for fax relay over IP. The valid range is 100 to 1,024. The default value is 1,024.

Parameter	Description
[FaxModemNTEMode]	Determines whether the device sends RFC 2833 ANS/ANSAM events upon detection of fax and/or modem answer tones (i.e., CED tone). ▪ **[0]** = Disabled (default). ▪ **[1]** = Enabled. **Note:** This parameter is applicable only when the fax or modem transport type is set to bypass or Transparent with Events.

1.7 Modified Parameters

The table below lists parameters from the previous release that have been modified for Release 5.6. The parameters enclosed in square brackets depict the *ini* file parameter; the other parameters depict the parameters in the Embedded Web Server.

Table 1-2: Release 5.6 Modified Web / [ini File] Parameters

Parameter	Description
[IPProfile]	(**Modification:** Addition of DisconnectOnBrokenConnection.) This *ini* file table parameter configures the IP profiles table. The format of this parameter is as follows: [IPProfile] FORMAT IPProfile_Index = IPProfile_**ProfileName**, IPProfile_**IpPreference**, IPProfile_**CodersGroupID**, IPProfile_**IsFaxUsed***, IPProfile_**JitterBufMinDelay***, IPProfile_**JitterBufOptFactor***, IPProfile_**IPDiffServ***, IPProfile_**SigIPDiffServ***, N/A, IPProfile_**RTPRedundancyDepth**, IPProfile_**RemoteBaseUDPPort**, IPProfile_**CNGmode**, IPProfile_**VxxTransportType**, IPProfile_**NSEMode**, N/A, IPProfile_**PlayRBTone2IP**, IPProfile_**EnableEarlyMedia***, IPProfile_**ProgressIndicator2IP***, IPProfile_**EnableEchoCanceller***, IPProfile_**MediaSecurityBehaviour**, IPProfile_**CallLimit**, IPProfile_ **DisconnectOnBrokenConnection**; [\IPProfile] For example: [IPProfile] IPProfile_1 = name1,2,1,0,10,13,15,44,1,1,6000,0,2,0,0,0,1,0,1,0,-1,1; IPProfile_2 = name2,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,$$,,$$,40,$$; [\IPProfile] **Notes:** ▪ This parameter can appear up to 9 times (i.e., indices 1-9). ▪ * Indicates common parameters used in both IP and Tel profiles. ▪ IpPreference = determines the priority of the Profile (1 to 20,

Parameter	Description
	where 20 is the highest preference). If both IP and Tel profiles apply to the same call, the coders and other common parameters (indicated with an asterisk) of the preferred Profile are applied to that call. If the Tel and IP profiles are identical, the Tel Profile parameters are applied. ▪ Two adjacent dollar signs ('$$') indicate that the parameter's default value is used. ▪ IPProfile can be used in the 'Tel to IP Routing' and 'IP to Hunt Group Routing' tables (Prefix and PSTNPrefix parameters). ▪ The 'Profile Name' assigned to a Profile index, must enable users to identify it intuitively and easily.
[TelProfile]	(**Modification:** Addition of EnableDIDWink, IsTwoStageDial, and DisconnectOnBusyTone parameters.) This *ini* file table parameter configures the Tel Profile Settings table. The format of this parameter is as follows: [TelProfile] FORMAT TelProfile_**Index** = TelProfile_**ProfileName**, TelProfile_**TelPreference**, TelProfile_**CodersGroupID**, TelProfile_**IsFaxUsed***, TelProfile_**JitterBufMinDelay***, TelProfile_**JitterBufOptFactor***, TelProfile_**IPDiffServ***, TelProfile_**SigIPDiffServ***, TelProfile_**DtmfVolume**, TelProfile_**InputGain**, TelProfile_**VoiceVolume**, TelProfile_EnableReversePolarity, TelProfile_EnableCurrentDisconnect, TelProfile_**EnableDigitDelivery**, TelProfile_**EnableEC**, TelProfile_MWIAnalog, TelProfile_MWIDisplay, TelProfile_**FlashHookPeriod**, TelProfile_**EnableEarlyMedia***, TelProfile_**ProgressIndicator2IP***, TelProfile_**TimeForReorderTone***, TelProfile_EnableDIDWink, TelProfile_IsTwoStageDial, TelProfile_DisconnectOnBusyTone; [\TelProfile] * = Indicates common parameters used in both IP and Tel profiles. TelPreference = determines the priority of the Profile (1 to 20, where 20 is the highest preference). If both IP and Tel profiles apply to the same call, the coders and other common parameters (indicated with an asterisk) of the preferred Profile are applied to that call. If the preference of the Tel and IP profiles is identical, the Tel Profile parameters are applied. For example: [TelProfile] TelProfile 1 = FaxProfile,1,1,1,40,13,22,33,$$,$$,$$,0,0,0,1,0,0,$$,0,$$,0,0,0; TelProfile 2 = ModemProfile,2,2,0,40,13,$$,$$,$$,$$,$$,$$,$$,$$,0,0,0,$$,0,$$,$$,$$,$$; [\TelProfile] **Notes:** ▪ This parameter can appear up to 9 times (i.e., indices 1-9). ▪ Two adjacent dollar signs ('$$') indicate that the parameter's default value is used.

Parameter	Description
	▪ The TelProfile index can be used in the Endpoint Phone Number table (TrunkGroup parameter). ▪ The 'Profile Name' assigned to a Profile index must enable users to identify it intuitively and easily.
[DNS2IP]	(**Modification:** Maximum number of table entries increased from 10 to 20; Maximum IP addresses increased from 2 to 4.) This *ini* file table parameter configures the internal DNS table for resolving host names to IP addresses. Four different IP addresses (in dotted-decimal notation) can be assigned to a host name. The format of this parameter is as follows: [Dns2Ip] FORMAT Dns2Ip_**Index** = Dns2Ip_**DomainName**, Dns2Ip_**FirstIpAddress**, Dns2Ip_**SecondIpAddress**, Dns2Ip_**ThirdIpAddress**, Dns2Ip_**FourthIpAddress**; [\Dns2Ip] Where, ▪ DomainName = Host name. ▪ FirstIpAddress, SecondIpAddress, ThirdIpAddress, FourthIpAddress = First, second, third, and fourth IP addresses respectively. For example: [Dns2Ip] Dns2Ip 0 = DnsName, 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4; [\Dns2Ip] **Notes:** ▪ This parameter can include up to 20 indices. ▪ If the internal DNS table is used, the device first attempts to resolve a domain name using this table. If the domain name isn't found, the device performs a DNS resolution using an external DNS server.
First Call Ringback Tone ID **[FirstCallRBTId]**	(**Modification:** Description and Web interface reference.) Determines the index of the first Ringback Tone in the CPT file. This option enables an Application server to request the device to play a distinctive Ringback tone to the calling party according to the destination of the call. The tone is played according to the Alert-Info header received in the 180 Ringing SIP response (the value of the Alert-Info header is added to the value of this parameter). The valid range is -1 to 1,000. The default value is -1 (i.e., play standard Ringback tone). **Notes:** ▪ It is assumed that all Ringback Tones are defined in sequence in the CPT file. ▪ In case of an MLPP call, the device uses the value of this parameter plus one as the index of the Ringback tone in the CPT file (e.g., if this value is set to 1, then the index is 2, i.e., 1 + 1).

Parameter	Description
[PeerHostNameVerificationMode]	(**Modification:** Support for the asterisk '*' wildcard.) Determines whether the device verifies the Subject Name of a remote certificate when establishing TLS connections. ▪ **[0]** = Disable (default). ▪ **[1]** = Verify Subject Name only when acting as a server for the TLS connection. ▪ **[2]** = Verify Subject Name when acting as a server or client for the TLS connection. When a remote certificate is received and this parameter is not disabled, the SubjectAltName value is compared with the list of available Proxies. If a match is found for any of the configured Proxies, the TLS connection is established. The comparison is performed if the SubjectAltName is either a DNS name (DNSName) or an IP address. If no match is found and the SubjectAltName is marked as 'critical', the TLS connection is not established. If DNSName is used, the certificate can also use wildcards ('*') to replace parts of the domain name. If the SubjectAltName is not marked as 'critical' and there is no match, the CN value of the SubjectName field is compared with the parameter TLSRemoteSubjectName. If a match is found, the connection is established. Otherwise, the connection is terminated.
[TLSRemoteSubjectName]	(**Modification:** Support for the asterisk '*' wildcard.) Defines the Subject Name that is compared with the name defined in the remote side certificate when establishing TLS connections. If the SubjectAltName of the received certificate is not equal to any of the defined Proxies Host names/IP addresses and is not marked as 'critical', the Common Name (CN) of the Subject field is compared with this value. If not equal, the TLS connection is not established. If the CN uses a domain name, the certificate can also use wildcards ('*') to replace parts of the domain name. The valid range is a string of up to 49 characters. **Note:** This parameter is applicable only if the parameter PeerHostNameVerificationMode is set to 1 or 2.
[NumberMapTel2IP]	(**Modification:** New parameters for Source Trunk Group and Source IP Group.) This *ini* file table parameter manipulates manipulates the destination number of Tel-to-IP calls. The format of this parameter is as follows: [NumberMapTel2Ip] FORMAT NumberMapTel2Ip_Index = NumberMapTel2Ip_**DestinationPrefix**, NumberMapTel2Ip_**SourcePrefix**, NumberMapTel2Ip_**SourceAddress**, NumberMapTel2Ip_**NumberType**, NumberMapTel2Ip_**NumberPlan**, NumberMapTel2Ip_**RemoveFromLeft**, NumberMapTel2Ip_**RemoveFromRight**, NumberMapTel2Ip_**LeaveFromRight**, NumberMapTel2Ip_**Prefix2Add**, NumberMapTel2Ip_**Suffix2Add**,

Parameter	Description
	NumberMapTel2Ip_**IsPresentationRestricted**, NumberMapTel2Ip_**SrcTrunkGroupID**, NumberMapTel2Ip_ **SrcIPGroupID**; [\NumberMapTel2Ip] Where, ▪ DestinationPrefix = Destination number prefix. ▪ SourcePrefix = Source number prefix. ▪ SourceAddress = **N/A.** ▪ NumberType = Number Type used in RPID header. ▪ NumberPlan = Number Type used in RPID header. ▪ RemoveFromLeft = Number of stripped digits from the left. ▪ RemoveFromRight = Number of stripped digits from the right. ▪ LeaveFromRight = Number of remaining digits from the right. ▪ Prefix2Add = String to add as prefix. ▪ Suffix2Add = String to add as suffix. ▪ IsPresentationRestricted = N/A (set to $$). ▪ SrcTrunkGroupID = Source Trunk Group ID. ▪ SrcIPGroupID = Source IP Group ID. For example: [NumberMapTel2Ip] NumberMapTel2Ip 0 = 01,$$,*,0,0,2,$$,$$,971,$$,$$,$$,$$; NumberMapTel2Ip 1 = 10,10,*,255,255,3,0,5,100,$$,255,$$,$$; [\NumberMapTel2Ip] **Notes:** ▪ RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, and NumberPlan are applied if the called and calling numbers match the DestinationPrefix and SourcePrefix conditions. ▪ The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. ▪ Parameters can be skipped by using two dollar signs ('$$'). ▪ Number Plan and Type can optionally be used in Remote Party ID (RPID) header by using the EnableRPIHeader and AddTON2RPI parameters.
[SourceNumberMapTel2IP]	(**Modification:** New parameters for Source Trunk Group and Source IP Group.) This *ini* file table parameter manipulates the source phone number for Tel-to-IP calls. The format of this parameter is as follows: [SourceNumberMapTel2Ip] FORMAT SourceNumberMapTel2Ip_**Index** = SourceNumberMapTel2Ip_**DestinationPrefix**, SourceNumberMapTel2Ip_**SourcePrefix**, SourceNumberMapTel2Ip_**SourceAddress**, SourceNumberMapTel2Ip_**NumberType**,

Parameter	Description
	SourceNumberMapTel2Ip_**NumberPlan**, SourceNumberMapTel2Ip_**RemoveFromLeft**, SourceNumberMapTel2Ip_**RemoveFromRight**, SourceNumberMapTel2Ip_**LeaveFromRight**, SourceNumberMapTel2Ip_**Prefix2Add**, SourceNumberMapTel2Ip_**Suffix2Add**, SourceNumberMapTel2Ip_**IsPresentationRestricted**, NumberMapTel2Ip_**SrcTrunkGroupID**, NumberMapTel2Ip_**SrcIPGroupID**; [\SourceNumberMapTel2Ip] Where, ▪ DestinationPrefix = Destination number prefix. ▪ SourcePrefix = Source number prefix. ▪ SourceAddress = Source IP address (obtained from the Request-URI in the INVITE message). ▪ NumberType = Number Type used in RPID header. ▪ NumberPlan = Number Plan used in RPID header. ▪ RemoveFromLeft = Number of stripped digits from the left. ▪ RemoveFromRight = Number of stripped digits from the right. ▪ LeaveFromRight = Number of remaining digits from the right. ▪ Prefix2Add = String to add as prefix. ▪ Suffix2Add = String to add as suffix. ▪ IsPresentationRestricted = Calling number presentation (0 to allow presentation; 1 to restrict presentation). ▪ SrcTrunkGroupID = Source Trunk Group ID. ▪ SrcIPGroupID = Source IP Group ID. For example: [SourceNumberMapTel2Ip] SourceNumberMapTel2Ip 0 = 22,03,$$,0,0,$$,2,$$,667,$$,0,$$,$$; SourceNumberMapTel2Ip 0 = 10,10,*,255,255,3,0,5,100,$$,255,$$,$$; [\SourceNumberMapTel2Ip] **Notes:** ▪ RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, NumberPlan, and IsPresentationRestricted are applied if the called and calling numbers match the DestinationPrefix and SourcePrefix conditions. ▪ The manipulation rules are executed in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and Suffix2Add. ▪ Parameters can be skipped by using two dollar signs ('$$'). ▪ IsPresentationRestricted is set to 'Restricted' only if 'Asserted Identity Mode' is set to 'P-Asserted'. ▪ Number Plan and Type can optionally be used in Remote Party ID (RPID) header by using the EnableRPIHeader.

1.8 Obsolete Parameters

The table below lists parameters from the previous release that are now obsolete.

Table 1-3: Release 5.6 Obsolete Web / [ini File] Parameters

Parameter	Description
[SendInviteToProxy]	This parameter is obsolete; instead, use SIPReRoutingMode.
[OfferUnencryptedSRTCP]	This parameter is obsolete; instead, use RTCPEncryptionDisableTx.
[TestMode]	This parameter is now obsolete.
[SASShortNumberLength]	This parameter is obsolete; instead, use SASRegistrationManipulation.

Reader's Notes

2 Supported Features

2.1 SIP Features

2.1.1 Supported SIP Features

The device supports the following main SIP features:

- Reliable User Datagram Protocol (UDP) transport, with retransmissions.
- Transmission Control Protocol (TCP) Transport layer.
- SIPS using TLS.
- T.38 real time Fax (using SIP).
  Note: If the remote side includes the fax maximum rate parameter in the SDP body of the INVITE message, the device returns the same rate in the response SDP.
- Operates with Proxy or without Proxy, using an internal routing table.
- Fallback to internal routing table if Proxy is not responding.
- Supports up to 15 Proxy servers. If the primary Proxy fails, the device automatically switches to a redundant Proxy.
- Supports domain name resolving using DNS NAPTR and SRV records for Proxy, Registrar and domain names that appear in the Contact and Record-Route headers.
- Supports Load Balancing over Proxy servers using Round Robin or Random Weights.
- Proxy or Registrar Registration, such as:

```
REGISTER sip:servername SIP/2.0
VIA: SIP/2.0/UDP 212.179.22.229;branch=z9hG4bRaC7AU234
From: <sip:GWRegistrationName@sipgatewayname>;tag=1c29347
To: <sip:GWRegistrationName@sipgatewayname>
Call-ID: 10453@212.179.22.229
Seq: 1 REGISTER
Expires: 3600
Contact: sip:GWRegistrationName@212.179.22.229
Content-Length: 0
```

  The "servername" string is defined according to the following rules:

  - The "servername" is equal to "RegistrarName" if configured. The "RegistrarName" can be any string.
  - Otherwise, the "servername" is equal to "RegistrarIP" (either FQDN or numerical IP address), if configured.
  - Otherwise the "servername" is equal to "ProxyName" if configured. The "ProxyName" can be any string.
  - Otherwise the "servername" is equal to "ProxyIP" (either FQDN or numerical IP address).

  The parameter GWRegistrationName can be any string. This parameter is used only if registration is Per Gateway. If the parameter is not defined, the parameter UserName is used instead. If the registration is per endpoint, the endpoint phone number is used.

The 'sipgatewayname' parameter (defined in the *ini* file or set from the Web browser), can be any string. Some Proxy servers require that the 'sipgatewayname' (in REGISTER messages) is set equal to the Registrar / Proxy IP address or to the Registrar / Proxy domain name. The 'sipgatewayname' parameter can be overwritten by the TrunkGroupSettings_GatewayName value if the TrunkGroupSettings_RegistrationMode is set to “Per Endpoint”.

REGISTER messages are sent to the Registrar's IP address (if configured) or to the Proxy's IP address. A single message is sent once per device, or messages are sent per channel according to the parameter AuthenticationMode. There is also an option to configure registration mode per Trunk Group using the TrunkGroupSettings table. The registration request is resent according to the parameter RegistrationTimeDivider. For example, if RegistrationTimeDivider = 70 (%) and Registration Expires time = 3600, the device resends its registration request after 3600 x 70% = 2520 sec. The default value of RegistrationTimeDivider is 50%.

If registration per channel is selected, on device startup, the device sends REGISTER requests according to the maximum number of allowed SIP dialogs (configured by the parameter NumberOfActiveDialogs). After each received response, the subsequent REGISTER request is sent.

- Proxy and Registrar Authentication (handling 401 and 407 responses) using Digest method. Accepted challenges are kept for future requests to reduce the network traffic.
- Single device Registration or multiple Registration of all device endpoints.
- Supported methods: INVITE, CANCEL, BYE, ACK, REGISTER, OPTIONS, INFO, REFER, UPDATE, NOTIFY, PRACK, SUBSCRIBE and PUBLISH.
- Modifying connection parameters for an already established call (re-INVITE).
- Working with Redirect server and handling 3xx responses.
- Early media (supporting 183 Session Progress).
- PRACK reliable provisional responses (RFC 3262).
- Call Hold and Transfer Supplementary services using REFER, Refer-To, Referred-By, Replaces and NOTIFY messages.
- Supports RFC 3711, Secured RTP and Key Exchange, according to RFC 4568.
- Supports RFC 3489, Simple Traversal of UDP Through NATs (STUN).
- Supports RFC 3327, Adding 'Path' to Supported header.
- Supports RFC 3581, Symmetric Response Routing.
- Supports RFC 3605, RTCP Attribute in SDP.
- Supports RFC 3326, Reason header.
- Supports RFC 4028, Session Timers in SIP.
- Supports network asserted identity and privacy (RFC 3325 and RFC 3323).
- Support RFC 3903, SIP Extension for Event State Publication.
- Support RFC 3953, The Early Disposition Type for SIP.
- Support for RFC 3966, The tel URI for Telephone Numbers.
- Support RFC 4244, An Extension to SIP for Request History Information.
- Supports Tel URI (Uniform Resource Identifier) according to RFC 2806 bis.

- Supports ITU V.152 - Procedures for supporting Voice-Band Data over IP Networks.
- Remote party ID <draft-ietf-sip-privacy-04.txt>.
- Supports obtaining Proxy Domain Name(s) from DHCP (Dynamic Host Control Protocol) according to RFC 3361.
- Supports handling forking proxy multiple responses.
- RFC 2833 Relay for DTMF Digits, including payload type negotiation.
- DTMF out-of-band transfer using:
  - INFO method <draft-choudhuri-sip-info-digit-00.txt>
  - INFO method, compatible with Cisco gateways
  - NOTIFY method <draft-mahy-sipping-signaled-digits-01.txt>
  - INFO method, compatible with Korea Telecom format
- SIP URL: sip:"phone number"@IP address (such as 1225556@10.1.2.4, where "122556" is the phone number of the source or destination) or sip:"phone_number"@"domain name", such as 122556@myproxy.com. Note that the SIP URI host name can be configured differently per called number.
- Supports RFC 4040, RTP payload format for a 64 kbit/s transparent data.
- Can negotiate coder from a list of given coders.
- Supports negotiation of dynamic payload types.
- Supports multiple ptime values per coder.
- Supports RFC 3389, RTP Payload for Comfort Noise.
- Supports RFC 3824, Using E.164 numbers with SIP (ENUM).
- Supports receipt and DNS resolution of FQDNs received in SDP.
- Supports <draft-ietf-sip-gruu-09>, Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in SIP
- Responds to OPTIONS messages both outside a SIP dialog and in mid-call. Generates SIP OPTIONS messages as Proxy keep-alive mechanism.
- Publishes the total number of free Tel channels in a 200 OK response to an OPTIONS requests.
- Support RFC 3310, HTTP Digest Authentication Using Authentication and Key Agreement (AKA).
- Supports recepit of a REFER method outside of a dialog.
- Support RFC 4458, SIP URIs for Applications such as Voicemail and Interactive Voice Response (IVR).
- Support RFC 3608, SIP Extension Header Field for Service Route Discovery During Registration.
- Support RFC 3911, The SIP Join Header (Partial).
- Support RFC 4730, A SIP Event Package for Key Press Stimulus (KPML) (Partial).
- Support RFC 3455, Private Header (P-Header) Extensions to SIP for the 3rd-Generation Partnership Project (3GPP) [Partial].

- Support RFC 4235, An INVITE-Initiated Dialog Event Package for SIP [Partial].
- Support RFC 3680, A SIP Event Package for Registrations.

2.1.2 Unsupported SIP Features

The following SIP features are not supported:

- MESSAGE method
- Preconditions (RFC 3312)
- SDP - Simple Capability Declaration (RFC 3407)
- S/MIME

2.2 SIP Compliance Tables

The SIP device complies with RFC 3261, as shown in the following subsections.

2.2.1 SIP Functions

The device supports the following SIP Functions:

Table 2-1: Supported SIP Functions

Function	Supported
User Agent Client (UAC)	Yes
User Agent Server (UAS)	Yes
Proxy Server	Third party, only tested with, amongst others, Ubiquity, Delta3, Microsoft, 3Com, BroadSoft, Snom and Cisco Proxies
Redirect Server	Third party
Registrar Server	Third party
Event Publication Agent (EPA)	Yes
Event State Compositor (ESC)	Third party

2.2.2 SIP Methods

The device supports the following SIP Methods:

Table 2-2: Supported SIP Methods

Method	Supported	Comments
INVITE	Yes	
ACK	Yes	
BYE	Yes	

Method	Supported	Comments
CANCEL	Yes	
REGISTER	Yes	Send only
REFER	Yes	Inside and outside of a dialog
NOTIFY	Yes	
INFO	Yes	
OPTIONS	Yes	
PRACK	Yes	
UPDATE	Yes	
PUBLISH	Yes	Send only
SUBSCRIBE	Yes	

2.2.3 SIP Headers

The device supports the following SIP Headers:

Table 2-3: Supported SIP Headers

Header Field	Supported
Accept	Yes
Accept–Encoding	Yes
Alert-Info	Yes
Allow	Yes
Also	Yes
Asserted-Identity	Yes
Authorization	Yes
Call-ID	Yes
Call-Info	Yes
Contact	Yes
Content-Disposition	Yes
Content-Encoding	Yes
Content-Length	Yes
Content-Type	Yes
Cseq	Yes
Date	Yes
Diversion	Yes
Encryption	No

Header Field	Supported
Expires	Yes
Fax	Yes
From	Yes
History-Info	Yes
Join	Yes
Max-Forwards	Yes
Messages-Waiting	Yes
MIN-SE	Yes
Organization	No
P-Associated-URI	Yes (Receive Only)
P-Asserted-Identity	Yes
P-Charging-Vector	Yes
P-Preferred-Identity	Yes
Priority	Yes
Proxy- Authenticate	Yes
Proxy- Authorization	Yes
Proxy- Require	Yes
Prack	Yes
Reason	Yes
Record- Route	Yes
Refer-To	Yes
Referred-By	Yes
Replaces	Yes
Require	Yes
Remote-Party-ID	Yes
Response- Key	Yes
Retry-After	Yes
Route	Yes
Rseq	Yes
Session-Expires	Yes
Server	Yes
Service-Route	Yes
SIP-If-Match	Yes
Subject	Yes
Supported	Yes

Header Field	Supported
Target-Dialog	Yes
Timestamp	Yes
To	Yes
Unsupported	Yes
User- Agent	Yes
Via	Yes
Voicemail	Yes
Warning	Yes
WWW- Authenticate	Yes

2.2.4 SDP Headers

The device supports the following SDP Headers:

Table 2-4: Supported SDP Headers

SDP Header Element	Supported
v - Protocol version	Yes
o - Owner/ creator and session identifier	Yes
a - Attribute information	Yes
c - Connection information	Yes
d - Digit	Yes
m - Media name and transport address	Yes
s - Session information	Yes
t - Time alive header	Yes
b - Bandwidth header	Yes
u - Uri Description Header	Yes
e - Email Address header	Yes
i - Session Info Header	Yes
p - Phone number header	Yes
y - Year	Yes

2.2.5 SIP Responses

The device supports the following SIP responses:

- 1xx Response - Information Responses
- 2xx Response - Successful Responses
- 3xx Response - Redirection Responses
- 4xx Response - Client Failure Responses
- 5xx Response - Server Failure Responses
- 6xx Response - Global Responses

2.2.5.1 1xx Response – Information Responses

Table 2-5: Supported 1xx SIP Responses

1xx Response		Supported	Comments
100	Trying	Yes	The SIP device generates this response upon receiving a Proceeding message from ISDN or immediately after placing a call for CAS signaling.
180	Ringing	Yes	The SIP 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	Yes	The SIP device doesn't generate these responses. However, the device does receive them. The device processes these responses the same way that it processes the 100 Trying response.
182	Queued	Yes	The SIP 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	Yes	The SIP device generates this response if the Early Media feature is enabled and if the device plays a Ringback tone to IP

2.2.5.2 2xx Response – Successful Responses

Table 2-6: Supported 2xx SIP Responses

2xx Response		Supported	Comments
200	OK	Yes	--
202	Accepted	Yes	--

2.2.5.3 3xx Response – Redirection Responses

Table 2-7: Supported 3xx SIP Responses

3xx Response		Supported	Comments
300	Multiple Choice	Yes	The device responds with an ACK, and then resends the request to the first new address in the contact list.
301	Moved Permanently	Yes	The device responds with an ACK, and then resends the request to the new address.
302	Moved Temporarily	Yes	The SIP 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	Yes	The device responds with an ACK, and then resends the request to a new address.
380	Alternate Service	Yes	The device responds with an ACK, and then resends the request to a new address.

2.2.5.4 4xx Response – Client Failure Responses

Table 2-8: Supported 4xx SIP Responses

4xx Response		Supported	Comments
400	Bad Request	Yes	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	Yes	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	Yes	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	Yes	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	Yes	The SIP 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	Yes	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	Yes	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.

4xx Response		Supported	Comments
407	Proxy Authentication Required	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	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	Yes	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.

4xx Response		Supported	Comments
484	Address Incomplete	Yes	The device doesn't generate this response. Upon receipt of this message and before a 200 OK has been received, the device responds with an ACK and disconnects the call.
485	Ambiguous	Yes	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	Yes	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	Yes	This response indicates that the initial request is terminated with a BYE or CANCEL request.
488	Not Acceptable	Yes	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	Yes	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.

2.2.5.5 5xx Response – Server Failure Responses

Table 2-9: Supported 5xx SIP Responses

5xx Response		Comments
500	Internal Server Error	Upon receipt of any of these Responses, the device releases the call, sending an appropriate release cause to the PSTN side. The device generates a 5xx response according to the PSTN release cause coming from the PSTN.
501	Not Implemented	
502	Bad gateway	
503	Service Unavailable	
504	Gateway Timeout	
505	Version Not Supported	

2.2.5.6 6xx Response – Global Responses

Table 2-10: Supported 6xx SIP Responses

6xx Response		Comments
600	Busy Everywhere	Upon receipt of any of these Responses, the device releases the call, sending an appropriate release cause to the PSTN side.
603	Decline	
604	Does Not Exist Anywhere	
606	Not Acceptable	

3 Known Constraints

This section lists known constraints in Release 5.6.

Note: Due to the improved *ini* file format for tables, it's not possible to load an *ini* file that was used by a device running software version 5.2 or later to a device using an earlier version (e.g. 5.0). This can result in an invalid configuration.

3.1 SIP Constraints

This release includes the following known SIP constraints:

1. Channel parameters such as voice/DTMF gain and jitter buffer are collectively configured in the *ini* file per device (not per call). By using Profiles, this limitation can be overcome.
2. The number of RTP payloads packed in a single G.729 packet (M channel parameter) is limited to 5.

3.2 Gateway Constraints

This release includes the following known gateway constraints:

1. In certain cases, when the Spanning-Tree algorithm is enabled on the external Ethernet switch port that is connected to the device, the external switch blocks all traffic from entering and leaving the device for some time after the device is reset. This may result in the loss of important packets such as BootP and TFTP requests, which in turn, may cause a failure in device start-up. A possible workaround is to set the *ini* file parameter BootPRetries to 5, causing the device to issue 20 BootP requests for 60 seconds. Another workaround is to disable the spanning tree on the port of the external switch that is connected to the device.
2. PPPoE is not supported.
3. NTT caller ID Type 2 constraints:
   - The NTT standard describes the CallerID Type 2 generation as a sequence of an incoming call signal, 'C' and 'D' DTMFs, and FSK modulated Data. Generation of the incoming call signal remains the responsibility of the application, but 'C', 'D', and the FSK are generated by the supplied service. The signal can be generated using the UDT signal generation mechanism.
   - Prior to the detection of NTT Caller ID Type 2, two DTMF detections ('C' and 'D') remain unscreened.
4. Setting the V.21 Transport Type to “Bypass” and the Fax Transport Type to “Relay” results in entering the Fax Relay mode at the 2,100 Hz signal. Only at the end of this signal, does the channel enter “Bypass” mode.
5. Transparent With Events Bell modem Transport Type is not supported.
6. The RFC 2198 redundancy mode with RFC 2833 is not supported (i.e., if a complete DTMF digit is lost, it is not reconstructed). The current RFC 2833 implementation supports redundancy for inter-digit information lost.

7. The resolution of the duration of digits On and Off time when dialing to the IP side using RFC 2833 relay is dependent on the basic frame size of the coder being used.
8. Incoming CNG T.38 packets do not switch the channel to T.38 mode.
9. When the fax CNG detector is not Transparent, a fax CNG tone received from the TDM cannot be detected using the Call Progress Tone detector.
10. Debug Recording:
    - Only one IP target is allowed.
    - Maximum of 50 trace rules are allowed simultaneously.
    - Maximum of 5 media stream recordings are allowed simultaneously.
11. Flash-burning control for specific files (BurnCallProgressToneFile) is no longer supported. The new SaveConfiguration parameter must be used instead.
12. VLAN Pass-Through mode is not supported.
13. 10Base-T Half-Duplex is not supported (only 10/100Base-T Full Duplex and 100Base-T Half-Duplex are supported).
14. When using a sample interval of 10 or 5 msec, the channel capacity may be reduced.
15. When using SRTP, channel capacity is reduced. Contact AudioCodes for more details.
16. When using SRTP, the number of basic codec frames per RTP packet cannot be greater than one. In addition, the RTP Redundancy (RFC 2198) feature cannot be activated.
17. The DJBufOptFactor parameter cannot be set to 13 if the channel is configured to operate with Silence Compression enabled.
18. When using m-factor values greater than 8, you must set jitter buffer optimization to 13 to cancel any jitter optimization and avoid under running condition.
19. Date and time should be set after each device reset, unless Network Time Protocol (NTP) is used.
20. The Syslog CDR Date and Time fields are left empty if the device's Date and Time are not set and NTP is not used.
21. Daylight Savings Time is not supported.
22. The following constraints apply when defining coders via the *ini* file:
    - Coder names are case-sensitive.
    - Don't use obsolete coder names (e.g., g729_AnnexB, g7231r53) with the improved coder interface.
    - When an invalid packetization time is used, the coder definition is disregarded.
    - When an invalid rate is used for dynamic-rate coders, the coder definition is disregarded.
23. The device supports only symmetrical coders - the same coder is used for transmit and receive (though different ptime is supported).
24. The 'Transparent' coder doesn't use DSP resources, therefore, the DSP functionality is off (i.e., DTMF detection, silence detection, etc.) and a reset is needed before switching to a different coder.
25. Transcoding is not supported with coder frame sizes other than the default size (refer to SampleBasedCodersRTPPacketInterval).

26. Tables that use the improved *ini* file representation can't be burned to flash memory as 'Client Defaults'.
27. It is highly recommended to use 100Base-T switches. Use of 10Base-T LAN hubs should be avoided.
28. Static NAT is not supported for local IP calls.

3.3 Web Constraints

This release includes the following known Web constraints:

1. For MP-11x, the Home page is not displayed correctly when the number of channels is reduced.
2. The window scrolling for the Home page sometimes does not function correctly when the window is resized.
3. There is no option to load an FXO Coefficient file to the device using the 'Auxiliary Files' page.
4. If the **Home** button is clicked when the device Scenario mode is active, the Web interface does not exit the Scenario mode.
5. On the 'Software Upgrade Wizard' page, the software upgrade process must be completed prior to clicking the **Back** button. Clicking the **Back** button before the wizard completes causes a display distortion.
6. The following pages cannot be added to a Scenario:
   - Web User Accounts
   - Web & Telnet Access List
   - Regional Settings
7. For users who have 'Read Only' access to the Web interface, the 'Read Only Mode' string text does not appear in bold format on the following pages: 'Tel to IP Routing Table', 'SNMP Community String' and 'SNMP Trap Destinations'.
8. The 'IP Routing Table' page can be configured in the Web interface, however, the *ini* file is not updated with the new settings.
9. Not all parameters can be changed on-the-fly in the Web interface. Parameters that can't be changed on-the-fly are depicted with the lightning symbol. To change these parameters, reset the device using the Web interface's **Reset** button.
10. When changing device parameters in the Web interface, the new parameters are permanently stored in flash memory only after the device is reset from the Web or after the **BURN** button is clicked in the 'Maintenance Actions' page.
11. The number of fax calls displayed in the fields 'Attempted Fax Calls Counter' and 'Successful Fax Calls Counter' in the 'Calls Count' pages may not be accurate.
12. In the 'Coders' and 'Coder Group Settings' pages, the voice quality is reduced when G.729 is used with ptime 120, and G.723 is used with ptime 150. Therefore, using these ptimes is not recommended.
13. When loading an *ini* file using the Web interface, the 'swwd' messages appears.

3.4 SNMP Constraints

This release includes the following known Simple Network Management Protocol (SNMP) constraints:

1. SNMP traps are not received when configuring more than one SNMP v3 trap destination.
2. A single GET command to the inetCidrRoute Table may return a “No Such Instance” error, while GET-NEXT (as in WALK) functions correctly.
3. When configuring the acSysInterfaceTable using SNMP or the Web interface, validation is only performed after device reset.
4. When enabling Telnet using SNMP, a fail notification is displayed despite the operation being successful.
5. When defining or deleting SNMPv3 users, the v3 trap user must not be the first or last to be defined. If there are no non-default v2c users, this results in a loss of SNMP contact with the device.
6. In the ipCidrRouteTable, new rows cannot be added and rows that were previously deleted using the Web interface, cannot be deleted.
7. The SNMPv3 users table returns the “line removed“ notice when adding a new row to an active row index.
8. After adding an empty line to the SNMPV3 table, it's impossible to delete it or add new lines.
9. The default values created in an IPSec configuration table are incorrect. The user should override the default values before activating the new row.
10. The acBoardConfigurationError alarm trap, generated as a result of a configuration error, does not clear.
11. The following RTP MIB objects are not supported: rtpRcvrSRCSSRC, rtpRcvrSSRC, rtpSenderSSRC, rtpRcvrLostPackets, rtpRcvrPackets, rtpSenderPackets, rtpRcvrOctets, and rtpSenderOctets.
12. An Ethernet link trap is sent before the link is up - manager does not receive clear. This occurs because a spanning tree algorithm is being calculated in the Ethernet switch.
13. The following encryptions types are currently supported (for SNMP v3 users only):
    - Authentication protocol: MD5 and SHA
    - Privacy protocol: DES and AES128
14. The range of the faxModemRelayVolume MIB object is incorrect. Instead of 0 to 15, it should be -18 to -3, corresponding to an actual volume of -18.5 dBm to -3.5 dBm.
15. Only one SNMP manager can access the device simultaneously.

3.5 CLI Constraints

This release includes the following known command-line interface (CLI) constraint:

1. When connecting to a device using Telnet (CLI), Syslog messages do not appear by default. The **show log** command must be used to enable this feature.

4 Resolved Constraints

4.1 Web Interface

The following Web interface constraints from previous releases have now been resolved in Release 5.6:

1. The 'Web User Accounts' page does not support Scenario mode.

   ✓ **This constraint is now supported!**

2. MP-118 and MP-124: When clicking the Uplink icon on the Home page, the 'Ethernet Port Information' page that opens, sometimes displays incorrect Ethernet port information. To correctly view this information, navigate to Status and Diagnostics > Ethernet Port Information.

   ✓ **This constraint is now fixed!**

3. Screen resolution 1152 x 864 is not supported.

   ✓ **This constraint is now supported!**

4. On the 'IP Settings' page, when selecting a 'multiple' or 'dual' value from the 'IP Networking Mode' field, the 'DHCP' field is incorrectly enabled.

   ✓ **This constraint is now fixed!**

Reader's Notes

5 Earlier Releases

Details of previous releases can be found in the Release Notes of Version 5.4, published by AudioCodes on May 20, 2008.

AudioCodes CPE & Access Analog Gateways

SIP

MediaPack™ MP-124 & MP-11x

Release Notes

Version 5.6

AudioCodes

www.audiocodes.com