VoIPowered By Mediatrix®
A Division of media5 Corporation

Technical Bulletin

Mediatrix SIP v5.0 & Dgw v2.0.2.23 Delta Document

December 8, 2008

Table of Contents

Introduction

Mediatrix is pleased to introduce the latest version of its Dgw software. This new software version, labelled v2.0, can be integrated on the **Mediatrix 3xxx Series, Mediatrix 44xx Series and Mediatrix 41xx Series**.

This document explains the difference between SIP v5.0.24.161 and the first GA release for Dgw v2.0.2.23. Please refer to the Release Notes documents for the evolution of the firmware versions.

The Dgw v2.0 software is backwards compatible with previous SIP v5.0 for all basic call scenarios.

The following sections subject will be covered within this document:

- Firmware Upgrade
- New Features
- Modified Behaviours
- Removed Features

Firmware Upgrade

The firmware upgrade of a **Mediatrix 41xx Series** from SIP v5.0 to Dgw v2.0 can be performed. Please contact your sales representative in order to obtain more details on how to proceed with this upgrade.

Please note that on 2 ports FXS gateways, Dgw v2.0 is supported on the 4102S only.

The Technical Bulletins are available on the Mediatrix Support Portal at (http://www.mediatrix.com/).

New Features

This section covers the main features introduced in the Dgw v2.0 release:

SIP Signaling

- SIP over TLS
- Registrar Discovery
- Support for draft-ietf-sipping-cc-transfer-03 with RFC 3515
- Support for RFC 4028 SIP Session Timers
- Support for RFC 3891 SIP Replaces Header
- SIP Authentication based on Username
- Configurable default SIP username value
- Configurable SIP Home Domain
- SIP OPTIONS method
- SIP Keep Alive using SIP OPTIONS method
- Shutdown Interface when SIP OPTIONS not answered
- Support of NAPTR as specified in RFC3263

SDP Signaling

- Support for MIKEY as per RFC 3830 and RFC 4567

Media Transport

- Support for SRTP as per RFC 3711
- Support for SRTCP as per RFC 3711
- Support for Clearmode RTP data Format – RFC 4040

Management and Configuration

- Support for SNMPv2 standard traps
- Web-Based configuration using HTTPS
- Configuration backup/restore
- Command Script file download and execution
- Command Line
- Firmware Rollback when software upgrade fails (except on 4102S).

Networking

- Multiple VLANs per Ethernet port
- Multiple IP addresses per link
- Host Firewall

Miscellaneous

- Map “+” to International type of number
- Music on hold played locally
- Custom Tone Configuration Wizard
- New Recovery bank feature (except on 4102S).

Hardware

- Support of Mediatrix Analog products 41xx Series
- Support of Mediatrix 33xx Series & 37xx Series

New Interoperability Options

- Possibility to ignore “+” sign in Authentication and SIP Request
- Possibility to allow reception of less media in SDP Response.
- Possibility to Ignore SIP username parameter.

Modified Behaviours

SIP Signaling

SIP v5.0 Behaviour	Dgw v2.0 Behaviour
▪ ***Registration state on expire***	
The state becomes unregistered and the device re-tries to register the user.	The state stays at registered and the device re-tries to register the user. The state will become unregistered if the re-try fails.
▪ ***Registration refresh***	
If the registration expire is smaller than the re-registration time, the device refreshes the registration at the reception of the 200 OK of the previous REGISTER.	If the registration expire is smaller than the re-registration time, the device refreshes the registration at the expiration of the registration.
▪ ***Registration retries timeout***	
After a registration fails, the registration re-tries is made periodically at each 2 minutes. The timeout is	After a registration fails, a registration re-tries is made exactly 2 minutes after the fail. The timer is

	SIP v5.0 Behaviour	Dgw v2.0 Behaviour
	the same for all registrations. All retries will be performed at the same time interval and the retries can occur at less than 2 minutes after the fail.	independent for each registration.
▪ ***User-Agent header***		
	The header "User-Agent" is present in the SIP request and the SIP response.	The header "User-Agent" is present in the SIP request and "Server" is present in the SIP response.
▪ ***Penalty box***		
	When all destinations are in the penalty box, the last destination is used.	When all destinations are in the penalty box, the destination with the highest priority is used.
▪ ***Handling of out-of-dialog final response***		
	A new context is created and an ACK is sent.	The response is ignored.
▪ ***Re-registration time modification***		
	It is applied immediately, including the current registration.	It is applied only for a new registration context. It requires a registration refresh for the time modification to be applied to the current registration.
▪ ***Invalid response for Register***		
An invalid response is a 200 OK that does not contain exactly the same contact as the one in the register (other than the port 0=5060). It occurs if the 200 OK of a REGISTER does not contain the contact.		
	The device will process the invalid response as a correct response and will try to refresh the registration.	The registration will fail and the registration state will become "InvalidState".
▪ ***Max-forward***		
	The max-forward SIP header presence can be enabled or disabled. The default value is disabled.	The max-forward SIP header is always present and the default value is 70. See the variable *interopMaxForwardsValue*

Networking

	SIP v5.0 Behaviour	Dgw v2.0 Behaviour
▪ ***The 802.1Q user priority and diffserv modification for SIP***		
	The modification is dynamically applied.	The modification requires a service restart to be applied. The service restart will be indicated with a message on the Web page or with the MIB variable *needRestartInfo.*

Telephony Services - FXS Endpoint

SIP v5.0 Behaviour	Dgw v2.0 Behaviour
▪ ***Hold/Unhold on FXS Endpoint***	
The FXS endpoint always assumes that a hold/unhold command is successful. It has no way to confirm the completions before initiating another action like another hold/unhold. So the high levels hold/unhold state can be desynchronized with the real media state.	The FXS endpoint waits for the hold/unhold completion and checks its result. The FXS endpoint does not try to perform an action (other than terminate) on a call when another hold/unhold is already in progress. The high levels hold/unhold state is always synchronized with the real media state. This also means that the flash is ignored when a hold/unhold action is in progress
▪ ***Conference on FXS Endpoint***	
The FXS endpoint re-INVITEs the two conference parties to activate the media and set the stream in G711. When the conference is stopped, the FXS endpoint will re-INVITE the remaining party with full media capabilities. The high level does not wait the conference start/stop completion before trying to apply another command on the call.	The FXS endpoint re-INVITEs the conference party on hold to activate the media (with full media capabilities). When the conference is stopped, two re-INVITEs are sent to the remaining party. The high level waits for the conference start/stop completion before trying to apply another command on the call. This also means that the flash is ignored when a start/stop conference is in progress.
▪ ***Attended transfer in mode transferor***	
If the REFER request is not supported by the transferee, the target and transferee role is inverted and the REFER is retried.	If the REFER request is not supported by the transferee, the transfer fails.
▪ ***Transfer failure recovery in transferor role***	
The transferor waiting for the transfer result has no limit. Therefore, the transferor can recover a failed transfer regardless of the time taken to fail. This has a draw back that the resource can wait forever if the transferee became unreachable. The failed transfer can be recovered in some conditions if the FXS user receives or initiates a new call.	The transferor waits for the transfer result up to a maximum of 4 minutes. After that, it will bye the target and the transferee. This will not cancel the transfer (if the transferee has reached the target) but will disallow the recovery. The failed transfer cannot be recovered if the FXS user receives or initiates a new call.

FXS Processing Capacity

Numbers in **Bold** indicate the difference between SIP 5.0 and Dgw 2.0.

SIP v5.0 Behaviour				Dgw v2.0 Behaviour			
▪ ***Capacity 4104***							
Port #	3 – Way Conf. Calls Available	Calls Using Compressed Codec (G.729, G726, G723)		Port #	3 – Way Conf. Calls Available	Calls Using Compressed Codec (G.729, G726, G723)	
		Without Conf. call	With Conf. calls			Without Conf. call	With Conf. calls
1 - 4	**4**	4	4	1 - 4	**2**	4	4
▪ ***Capacity 4108***							
Port #	3 – Way Conf. Calls Available	Calls Using Compressed Codec (G.729, G726, G723)		Port #	3 – Way Conf. Calls Available	Calls Using Compressed Codec (G.729, G726, G723)	
		Without Conf. call	With Conf. calls			Without Conf. call	With Conf. calls
1 - 8	**8**	8	**8**	1 - 8	**2**	8	**6** (2 ports unavailable)
▪ ***Capacity 4116***							
Port #	3 – Way Conf. Calls Available	Calls Using Compressed Codec (G.729, G726, G723)		Port #	3 – Way Conf. Calls Available	Calls Using Compressed Codec (G.729, G726, G723)	
		With no Conf. call	With Conf. calls			With no Conf. call	With Conf. calls
1 - 8	**8**	8	**8**	1 - 8	**2**	8	**6** (2 ports unavailable)
9 - 16	**8**	8	**8**	9 – 16	**2**	8	**6** (2 ports unavailable)
▪ ***Capacity 4124***							
Port #	3 – Way Conf. Calls Available	Calls Using Compressed Codec (G.729, G726, G723)		Port #	3 – Way Conf. Calls Available	Calls Using Compressed Codec (G.729, G726, G723)	
		With no Conf. call	With Conf. calls			With no Conf. call	With Conf. calls
1 - 8	**8**	8	**8**	1 - 8	**2**	8	**6** (2 ports unavailable)*
9 - 16	**8**	8	**8**	9 – 16	**2**	8	**6** (2 ports unavailable)*
17 - 24	**8**	8	**8**	17 - 24	**2**	8	**6** (2 ports unavailable)*

* The unavailable ports will not have any dial tone until an ongoing call or conference is terminated.

Miscellaneous

SIP v5.0 Behaviour	Dgw v2.0 Behaviour
▪ ***Validation between minimum and maximum packetization time***	
The provisioning forbids to configure a minimum Ptime higher than the maximum and a maximum Ptime lower than the minimum.	No validation is done between the Max-Ptime and the Min-Ptime. The maximum Ptime can be lower than the minimum Ptime. In this case, the minimum Ptime is used by the application.
▪ ***Dynamic payload configuration validation***	
The provisioning forbids setting a payload type used by another codec or RFC 2833.	No validation is done to prevent using the same payload type.
▪ ***Codec modification***	
Enabling / disabling codec is a dynamic operation. The service does not need to be restarted	Enabling / disabling codec requires the Mipt service to be restarted for the change to be effective. The service restart will be indicated with a message on the Web page or with the MIB variable *needRestartInfo.*
▪ ***Unit Administration Mode State***	
When the unit administration state is locked, the *Power* and *Ready* LED blink.	When the unit administration state is locked, the *In Use* LED blinks yellow. When the unit administration state is shutting down, the *In Use* LED is steady on yellow color
▪ ***Recovery Mode versus Partial Reset***	
The Partial reset/Recovery mode provides a way to restart the Mediatrix 41xx in a known and static state at the default IP address 192.168.0.1/24.	
A Recovery mode is done by depressing the *RESET/DEFAULT* button between 5 and 10 seconds.	A partial Reset is done by depressing the *RESET/DEFAULT* button between 7 and 11 seconds.
When in recovery mode, some variables (IP addresses and others) are set to known values. These temporary values are not saved in flash.	The partial reset sets some variables (IP addresses and others) to known values. These values are saved in flash.
When in recovery mode, some “services” of the application are completely disabled, like the telephony features.	After a partial reset, all services stay enabled.
When in recovery mode, some variables cannot be configured. Only variables modified by the user are saved in the flash.	After a partial reset, all variables can be configured. All changes are persistent.
A special LED pattern indicates the unit is in recovery mode. The LED pattern is stopped when the unit leaves the recovery mode.	The partial reset enables the “rescue” network interface. When this network interface is enabled, a special LED pattern is displayed. The LED pattern stops when the “rescue” network interface is disabled by the user.

Removed Features

SIP Signaling

Removed Feature	Comments
RFC 2543 SIP Basic Authentication (as a client)	This non secure mechanism was obsoleted by RFC 3261. RFC 3261 uses Digit Authentication Only.
SIP Publication of Presence Info	This feature is currently on the Roadmap.
SIP public address configuration (NAT Traversal)	This behaviour is no longer supported.
Support using no SIP "replaces"	Obsolete method for replaces. Dgw v2.0 supports the mechanism described in RFC 3891.
Support using "replaces" with "requires"	This feature is currently on the Roadmap.
Support for sip-replaces-01	Dgw v2.0 supports the mechanism described in RFC 3891.
Support for sip-replaces-03	Dgw v2.0 supports the mechanism described in RFC 3891.
Support for draft-ietf-sip-cc-transfer-02	Dgw v2.0 supports the mechanism described in draft-ietf-sipping-cc-transfer-03 with RFC 3515.
Support for draft-ietf-sip-cc-transfer-05 with draft-ietf-sip-refer-02 ▪ Usage of the SIP "Referred-By" field during transfer using Transfer 05 only. ▪ Override SIP "Referred-By" field with local URL	Dgw v2.0 supports the mechanism described in draft-ietf-sipping-cc-transfer-03 with RFC 3515.
Support for draft-ietf-sip-session-timer-04	Dgw v2.0 now supports RFC 4028 - SIP session timers.
Support for draft-ietf-sip-session-timer-08	Dgw v2.0 now supports RFC 4028 - SIP session timers.
DNS SRV record locking. ▪ All messages during a call or registration use the same SRV record.	This behaviour is no longer supported.
Allow resetting authentication credential between SIP transactions. ▪ Remove the authentication header in all SIP requests so that the request always get challenged	This behaviour is no longer supported.
Configurable "unknown info request" SIP response. See the variable *sipInteropAckUnsupportedInfoRequest*.	This feature is currently on the Roadmap.

Removed Feature	Comments
Disable the usage of magic cookie for SIP branch matching for incoming transaction to follow the method described in RFC 2543 (section 10.1.2).	It is now not possible to disable the usage of the magic cookie for SIP branch. The branch matching will behave as described in RFC 3261 (section 8.1.1.7).
Ignore the Via Branch ID in CANCEL. Deviance from RFC 3261. ▪ Ignore the Via Header field's branch parameter in CANCEL requests with no TO tag.	It is no longer possible to ignore the Via Branch ID in CANCEL. The unit behaves according to section 17.2.3 of RFC 3261.
Configurable Default SIP registration expiration. This value is used when the contact in a registration response contains no expires and the SIP Server did not use the RFC 3261 recommended value. See the variable *sipInteropDefaultRegistrationExpiration*	The SIP default registration expiration is no longer configurable. If the SIP server does not provide an expires, the default recommended value in RFC 3261, 3600 seconds, is used.
Use authentication without integrity when responding to SIP authentication request.	It is no longer possible to use authentication without integrity. The Mediatrix unit will apply authentication with integrity when responding to SIP authentication request as per RFC 2617.
Can disable Copy URI parameters to the level of proxy authentication. See the variable *sipInteropProxyAuthenticationUriParametersEnable*	This feature is currently on the Roadmap.
Proprietary method for firewall traversal	This feature is no longer supported.

Media Transport

Removed Feature	Comments
It is possible to disable the Configurable Echo Cancellation. See the variable *voiceIfEchoCancellationEnable*	It is no longer possible to disable the echo cancellation. The Mediatrix unit will proceed to cancel signals that are recognized as echo when appropriate.

POTS Telephony

Removed Feature	Comments
FXS Emergency bypass dialing (Bypass 911). See *emergencyCallMIB*	This feature is no longer supported using the *emergencyCallMIB*, However this can be achieved using the Call Router.
FXS Flash-hook and digits service activation. The end user must perform a flash hook and enter a digit to activate the service.	This feature is currently on the Roadmap.
Message waiting indicator with subscription or without subscription.	This feature is currently on the Roadmap.

Removed Feature	Comments
Shutdown of FXS interface when the SIP server is down. This instructs the FXS unit to suppress loop current on its ports when they cannot be used or when the IP connection is lost. See the variable *fxsLoopCurrentDrop*	This feature is no longer supported.

Country Support

Removed Feature	Comments
Country Support: ▪ Australia 1 ▪ Australia 2 ▪ Australia 3 ▪ Austria 2 ▪ Brazil 1 ▪ Chile ▪ China 1 ▪ Denmark ▪ Germany 3 ▪ Hong Kong 1 ▪ Israel ▪ Indonesia ▪ Japan ▪ Malaysia 1 ▪ Netherlands ▪ Mexico 1 ▪ New Zealand 1 ▪ North America 2 ▪ Russia 1 ▪ Sweden 1 ▪ Thailand ▪ UAE 1 ▪ UK 1	These countries selections are no longer supported. However the Tone configuration can be configured via the Custom Tone Customization Web page.

Management and Configuration

Removed Feature	Comments
Image file download via Remote file. See the variable *imageLocationProvisionSource*	This feature is no longer available.
DHCP configuration of SIP Registrar, Server and Outbound proxy	This feature is no longer supported. The SIP Registrar, Server and Outbound proxy must be configured via a Static IP address.

Networking

Removed Feature	Comments
Ethernet Bridging with VLAN substitution.	This behaviour is no longer supported.
Vendor and site specific DHCP Options.	This behaviour is no longer supported.
Transparent IP Address Sharing with a limited DHCP server.	This feature is currently on the Roadmap.
Uplink Egress Bandwidth control.	This feature is currently on the Roadmap.

Removed Feature	Comments
MAC address spoofing.	This feature is currently on the Roadmap.
STUN client.	This feature is currently on the Roadmap.

Miscellaneous

Removed Feature	Comments
DHCP not found LED behaviour.	No more LED behaviour available when the DHCP server is not found.
PPP Connection not established.	No LED behaviour available when the PPP connection is not established.
Delayed Hot Line.	This feature is currently on the Roadmap.
PIN Dialing.	This behaviour is no longer supported.