M!DGE2 Release Notes
Firmware version 4.2.40.xxx

Release 4.2.40.101
2018-12-10

Note:
The firmware **4.2.40.101** is the first official firmware available on our website and for mass production. If you have any older version provided for testing, upgrade M!DGE2 units at earliest.

New Functionalities

Security Fixes

Fixes

LXC container image not useable
Some LXC container images were installed with insufficient access rights. In such a case, the LXC container would not start up.

Serial Interface configuration
On M!DGE2 with more than one serial interface, only one could be configured for special purpose like device server or protocol server. The first interface could not be changed to anything else but 'login console'. This was fixed and now all serial interfaces can be used for any purpose.

LAN as WAN configuration
The WAN configuration of a LAN interface was not applied correctly. This has been fixed.

IP packets with DSCP tag not processed by M!DGE2
Special IP packets with DSCP tag 0x40 did not pass the internal network switch of M!DGE2 and therefore could not be received, sent or forwarded. This has been fixed.

Known Issues

Protocol server restrictions
The serial Protocol server is bound to the 1st LAN IP address, port 8882. It is not possible to re-configure it. Limitations are:

- Only one Protocol server can be configured even in units with more RS232 interfaces
- If Protocol server's mapping is based on WAN IP addresses, masquerading and Destination NAT are required for correct functionality (i.e. incoming data via WAN on UDP port 8882 must be forwarded to local M!DGE2' 1st LAN IP address). If using VPN tunnels, mapping should be configured to these LAN IP addresses.

Terminal servers are not working
Terminal servers are not yet implemented correctly in M!DGE2 units even though it is possible to configure them in GUI.

Mobile connections with ‘4G-only’ option
It might happen that WWAN/mobile connection does not come up if ‘4G-only’ option is selected for a given mobile interface until M!DGE2 is rebooted. Use ‘automatic’ or ‘4G-first’ options.

Release 4.2.40.100
2018-11-19

New Functionalities

Voice signalling
Voice signalling is now possible without any Voice licence.

SW update package validated before upload
An invalid SW update package is identified in the web interface before the actual transfer to the target was performed skipping the process of slow upload of potential invalid packages via mobile network. The new architecture also allows us to provide better and more detailed feedback on the current update status.

New version of igmpproxy
Igmpproxy was updated to version 0.2.1. This also fixes a bug on interfaces with an alias IP setup.

Several changes to the WLAN settings to comply with RED (2014/53/EU)

WLAN advanced user license
Setting up regulatory domain and antenna gain parameter is required to have a WLAN advanced user licence. The new default parameters are "EU" for the regulatory domain and "3 dBi" for the antenna gain. Please contact our customer support if you need this WLAN advanced user licence.

HTTPS access with client certificates
Functions which communicate with HTTPS-Servers (like SW update from URL or SDK) can now authenticate with client-certificate and key.

MQTT publishing from SDK
Functions for publishing MQTT messages were added to the SDK scripting language.

Password hashes replace encrypted passwords in configuration
We changed our password handling to use cryptographic hashes instead of symmetric encrypted passwords wherever possible. Therefore, you have to provide the administrator password for downgrading to older SW releases as these still rely on the passwords to be stored on the device.
For SNMP access the passwords still need to be available. Therefore. users which shall be able to log in via SNMP need the new setting "Store password in device" to be enabled.

GNSS default antenna type set to "active"
As passive GNSS antennas are very uncommon these, days we changed the default setting to active. This is only valid on factory default configuration. A configuration update will keep the existing settings.

Wait for configuration change task to be finished
Changing a configuration setting via CLI or SDK does not block. A new function was implemented to request if all pending tasks have been finished and it is safe to send new configuration change requests.

WLAN MESH
The support of WLAN Mesh (802.11s) is now available. It is possible to configure a pure mesh point or a mesh access point (mesh point and access point).
Currently the encrypted Mesh with TI based M!DGE2 routers is only compatible among themselves.

Support for new GNSS modules
Added support for new Ublox NEO-M8 modules.

uBlox TOBY-L2 support
The uBlox Toby-L2 LTE modem is now supported.

WLAN Inter Access Point Protocol (IAPP)
It is now possible to enable IAPP within the WLAN configuration. This feature will inform the old access point that a WLAN client has associated with a new access point.

Number of VLANs increased
It is now possible to configure up to 10 VLANs instead of 5.

Update of time zone data
North Korea switched back to +09 on 2018-05-05. Our best wishes to all Korean people.

CLI shows WLAN channel
The cli status command will show the current WLAN channel if access point or dual mode is configured.

LED configuration
All LEDs except for "STAT" can be configured to different function like LAN, WAN, WLAN, WWAN, etc.

Bridges without STP
It is possible now to switch off STP completely on bridge-devices.

GUI improvements
Allowing Upload of keys and certificates in nested p12 files.
IP pass-through setup failed on web interface with recent SW releases.
Obsolete GUI interfaces have been removed.

React faster on GNSS flaps
The maximum GNSS flaps were evaluated only once every 5 minutes. This has been changed. Now the GNSS supervision will take action as soon as the maximum flaps have been detected.

Configuration of NTP server stratum
The stratum of NTP server in case of GNSS sync or time from internal clock can be configured now. As these sources are not very accurate this feature should be used with care. Please contact our customer support for detailed information.

Refactory of config converter
Our config conversion tool `cfconvert` which is responsible for converting older and newer configuration files to the configuration release needed by the current version was refactored speeding up this step of SW update or configuration apply by factor or 3-5 and reducing the required flash space by several hundreds of kB which was required for implementation of other features on older hardware like M!DGE or MG102i with very limited flash space.
As a side effect the conversion to configuration versions other than the one used by the current SW release is not supported any more. In normal operation this is not needed anyway. If you have such a requirement please contact our technical support.

Navigation mode of ublox GNSS modules
The operational mode of ublox GNSS modules is now automatically set up portable or stationary depending on the router settings of `admin.area` (mobile or stationary).

Security Fixes

Update of Lighttpd
Lighttpd was updated to version 1.4.50. On older releases Security relevant issues were back ported.
CVE-2015-3200: Injection of log entries fixed on lighttpd

Log display in web interface vulnerable to Cross-Site-Scripting (XSS) attack
The web interface which displays the system log was vulnerable to JavaScript XSS attacks. An attacker capable of placing malicious content in the system log could execute JavaScript code in the web browser of the user.

Security bug fixes on 3rd party SW packages
CVE-2015-3200: Use-after-free fixed in Linux kernel

Security bug fixes in 3rd party SW packages
CVE-2018-14526 Unauthenticated EAPOL-Key decryption in wpa_supplicant

Fixes

SDK improvements
The SDK function `nb_can_setattr` failed if the optional parameter restart was different from 0.
Fixed typo in modification time of files in `nb_transfer_list`.

Mismatch between VLAN network settings and DHCP settings triggers reboot
In situations where the VLAN network settings (network address/netmask) did not fit with the DHCP range configured for that network, the router would go into reboot. This was fixed. Now the DHCP server on the mis-configured interface will not be started and a warning is given to the user.

Authorities certificates were not used for all HTTPS downloads
Some functions where data are downloaded from a server the "Authorities" certificates were not used. E.g. it was not possible to update WWAN module firmware from HTTPS.

GUI improvements
Changing the priority of WAN interfaces in GUI did change bridged WLAN client interface setup. WAN links are displayed as bridgeable devices. This has been fixed.
WLAN channels did not appear when WLAN band was changed. This has been fixed.
Changing between 4G-Only and automatic increased the amount of transferred data. This was a failure of data display and did not affect the actual data traffic.
The IAPP feature was not displayed if WLAN dual mode was configured. This has been fixed.
The interface numbering was wrong during modem firmware update. This has been fixed.
Display of the configuration web site of the WLAN Administration was fixed.
WAN interfaces could be reconfigured to LAN if port assignment was changed in GUI.
Changes on port setup could switch configured WAN interfaces to act as LAN interfaces.
User data from the web administration interface was not escaped correctly in some cases.
Clicking on 'Cancel' in the certificate settings accidentally applied the changes.

Certification installation over CLI
It was not possible to install WLAN certifications for client mode over the CLI command. That has been fixed.

SNMP walk timeout
In certain cases, an SNMP timeout could occur during an SNMP walk. That has been fixed.

uBlox TOBY-L2 improvements
Clients connected to the LAN side of the router could not communicate to the WAN network, because IP forwarding was disabled. That has been fixed.

SNMP: unknown type in vendor MIB
The MGTrapHistoryEntry SNMP MIB was not standard conform. That has been fixed.

Fixed SDK example script
The SDK example script 'dio-server.are' contained a logical error that could trigger an error on runtime.

WLAN module order
WLAN modules were not swapped according to board descriptor. This has been fixed.

Soft bridges sometimes not in UP state after configuration
Depending on which devices were bridged on one of the soft bridges (BR1, BR2), the soft bridge was not set to state UP if no local IP address was configured. Therefore, packet forwarding between these devices failed.

SW update URL was identified as invalid by mistake
Due to internal escape sequence URLs containing special characters like '&' were identified as invalid.

Usernames starting with 'admin' or 'root' not able to login
Additional users starting with 'admin' or 'root' like 'admin-user' were not able to login after change of administrator password.

Ping supervision failed on IP pass-through
In IP pass-through the ping supervision failed to contact the server and therefore restarted the router even if the WWAN connection was fine.

No DNS on routed network adapter to LXC container
A virtual network adapter which is configured as routed interface for LXC container did not provide DNS to the LXC. DNS for such interfaces can now be configured the same way as it is done for other interfaces.

Setting up bridged network interfaces for LXC guests without network and gateway
The network settings of a bridged virtual network interface should be defined by the bridge and not by the interface as it is common sense for all bridged interfaces.

Certificate key handling
Changing the certificate key of the system could fail and leave the system without usable certificate keys. This was fixed.

Empty user password affected other users
If the setting 'user.0.password' contained an empty string, all other users were not able to log in any more. This is not a valid configuration anyway, but it was not intended behaviour neither and therefore was fixed.

WLAN: disconnected clients displayed.
In certain circumstances, the WLAN status and GUI were still showing some disconnected clients as connected. That has been fixed.

Known Issues