

Release notes MC Firmware

Firmware 2.04b --> 2.04d (11. May 2015)

1. Linux Kernel 4.0.0-rc5+ --> 4.0.0+
2. Change in the roaming strategy. With the firmware 2.04b the roaming has been controlled by the bridge application. With the 2.04e roaming is completely left to the WLAN driver of the Linux kernel.
3. access point parameters that prevent a connection to the client are now show in red in the access point list.

Firmware 2.04d --> 2.04r (28. July 2015)

1. DHCP-Server with clear function for reservations
2. MWLC Bridge-Mode added
3. (Wireless --> Roaming) Lower SNR Threshold Parameter removed.
4. (Wireless --> Roaming) in AP Density Modus : "Auto detect" Mode the roaming decisions are done by the bridge application and not only by the WLAN driver of the operating system. The focus is now more on a good signal strength of the AP's and not so much on the potentially possible transmission speed. It is recommended by us to set the AP Density Mode to "Auto Detect".

Firmware 2.04r --> 2.06d (09. September 2015)

1. new Linux-Kernel 4.1.5+
2. DHCP problem in "Level 2 Pseudo-Bridge" Mode solved
3. DHCP-Server revised. Now the processing of the reservations is better.
4. new parameter "Stay connected" in "LAN Client Cloning" - Mode added
5. Improved processing of certificate files
6. NTP RTC Config --> now a start date can defined by a parameter that is set at start up.
7. at "Admin" the HTTPS - Port can be configured.

Firmware 2.06d --> 2.06f (04. October 2015)

1. No downgrade of the firmware to 2.04x should be done with 2.06d. The device will crash and needs maintenance.
2. Some unnecessary parameter in the config were removed.

Firmware 2.06f --> 2.06k (18. November 2015)

1. SCEP (Simple Certificate Enrollment Protocol) Function added („Wireless --> SCEP“)
2. „MWLC Master“ Mode corrected

Firmware 2.06k --> 2.06p (17. December 2015)

1. Bug-fix: The firmware 2.06k in bridge-mode „Single Client NAT“ generates a reboot of the device. The rebooting can only be stopped by doing a default reset of the device
2. Changes in the firmware to serve the 2 new MC devices (MC2, MC4).
3. Additional function to send the state of the WLAN connection to a node connected to the LAN side of the MC device. This information is send with UDP datagrams.
4. Changes to the definition of NAT rules:
In a simple NAT rule now several ports can be defined for forwarding to an IP address
5. The MC-Config-Program can now communicate with unicast datagrams via the LAN site of the MC devices. This will fasten the firmware upgrade.

Firmware 2.06p --> 2.06q (07. January 2016)

1. Changes to the USB-Printerserver: So far, the manufacturer and the product info has been registered when a printer is connected to the MC. Without this information, the printer server has not been started. Some printers don't provide this information. The Firmware 2.06q starts the printer server even without this information.
2. Small changes to the website.

Firmware 2.06q --> 2.06s (04. February 2016)

1. Bug-fix in the serial interface module: Falsification of the serial received data could happen, when the interface received special character sequences and the mode "no parity" was active.
2. Change in the roaming module: To make a decision for a change to another AP a "Probe response" has to be received from that AP in the last 10 seconds.

Firmware 2.06s --> 2.06u (19. February 2016)

1. Handshake handling in serial COMSERVER mode revised.
2. Error found in the processing of NAT rules.

Firmware 2.06u --> 2.07b (22. March 2016)

1. In the section „Roaming“ the ping function has been revised.
2. Bug found in the timer module. This error could potentially bring the WLAN client to a restart or stop the devices so that a manual reset is needed.
3. Serial interface: XON - XOFF protocol handling improved

Firmware 2.07b --> 2.07c (12. April 2016)

1. The state of the LAN-Ports are now transferred to the MCCConfig-Program.
2. The LAN-Status is now shown correctly by the LAN-Port-LED's (MC2 + MC4)
3. The optional temperature sensor is integrated into the firmware

Firmware 2.07c --> 2.07g (13. May 2016)

1. The state of the serial port (Ser1) and the USB-Memory-Stick is now transferred to the MCCConfig-Program.
2. Now up to 16 DNS-Server-IP's can be registered by the DHCP-Client (WLAN side).
3. Now 2 NTP-Server can be configured.
4. Now DHCP-Server-Rules can be defined as config parameter, to ensure that the LAN clients gets there right IP addresses.
5. A list of BSSID's can be defined that will be preferred or avoided by the roaming algorithm to select the best access point.
6. It is now possible with the MC-Config program (v. 2.2.0.11) to send a preliminary configuration to an MC device. Only when the configuration is confirmed via the MC-Config program within a predetermined time after restart, this configuration is marked as permanent. This can prevent a permanently access via WLAN to the MC device by an erroneous input of a parameter.

Firmware 2.07g --> 2.07k (01. June 2016)

1. If the LAN-Client-Cloning Mode is selected and the LAN Client Type is „Static“ or „Auto detect“ DNS Server IP addresses can now be configured. If the LAN-Client has a static IP address the MC does not have any DNS information. The MC can not resolve given host names for NTP or SCEP. With the configured DNS IP's the MC can do the name resolutions
2. The number of entries for specific tables was designed variable. These tables have “Add” and “Remove” button at the end of the table. This simplifies the configuration pages and can make them clearer.
3. Bug-fix in the serial module. In UDP mode with not defined remote IP the first datagram should be registered by the MC to send the answer back to that IP. There was an error that the information of the first datagram was not registered correctly. The second received datagram solves that problem. With the firmware 2.07i the first datagram will be registered correctly.

Firmware 2.07k --> 2.07v (25. August 2016)

1. Fixed a bug in the „ping-test“ mode (roaming parameter). Incorrectly evaluation of the sequence numbers let the function get inactive after a few days (depending on the interval parameter).
2. Extension of wireless-dump feature
A parameter for handling the „memory full“ event has been implemented. The user can decide if the dump function should be stopped or if the oldest dump file should be deleted.
3. Changes in the DHCP-Client-Module. The IP request from a some DHCP-Server did not work correctly.

Firmware 2.07v --> 2.08a (20. September 2016)

1. Revision of the Dump function (wireless + Ethernet) for better storage of the wireless and Ethernet recordings.
2. The SNMP function has been significantly expanded. The MIB file of the MC device can now be downloaded from the website of MC (-> Admin -> SNMP)
3. Error in the HTTPS function. If the initial generation of the self-signed certificate was for some reason not fully completed, the HTTPS access to the MC website could not be used. The firmware 2.08a will start the generation again when a defective certificate is detected.

Firmware 2.08a --> 2.09d (14. December 2016)

1. new: Multi-SSID. Several (up to 8) WLAN profiles can now be configured.
2. The number of instances for the serial interfaces are now also displayed dynamically in the MC-Config program and on the web page
3. The function to limit the transmission bit rates has been revised. With the firmware 2.09d, however, only the bit rates for the mode 802.11 b / g can be set.
4. In some WLAN systems it happens that the WLAN controller allocates BSSID's, which occur twice, whereby a BSSID exists in 2.4GHz and the same BSSID is also used in the 5GHz band. The firmware 2.09d takes this into account and runs both BSSIDs separately in the access point list.
5. There is now possible to prioritize traffic through the tunnel in MWLC mode.
6. A time zone can now be configured to get the right local time stamp in the debug log files.
-> see "realtime clock"

Firmware 2.09d --> 2.10c (16. March 2017)

1. New Linux kernel version 4.9.13+ integrated
2. Improved response of the MC to malfunctions during the authentication phase
3. Fixed an error while handling multiple active WLAN profiles.
4. The processing of the files for the trace recordings (WLAN + LAN) has been improved so that now individual files can be selected for download via the MC Config program. These files can be downloaded from the internal flash and from a plugged USB stick
5. Additional information's are now displayed on the home page of the MC in the list of APs. As far as the AP supplies this information, the following is displayed in the "Extra Info" column:
 - Amount of logged in clients
 - Workload (%)
 - TPC Specification of APThis information is now also used for roaming in order to determine the most suitable AP.
6. Fixed an error in the NTP client. If the IP of the timer server had to be determined via DNS and the first attempt of this address resolution failed, the attempt was not renewed. Thus, no time was obtained via an NTP server.

Firmware 2.10c --> 2.10i (02. May 2017)

1. New kernel version 4.9.25 integrated
2. Error in the roaming module when compiling the channels to be scanned..
3. Introduction of a new parameter "Hostname" in the DHCP client module. This means that the "Hostname" parameter, which the DHCP client transmits to the DHCP server, can be set independently of the "Device name" parameter.
4. Fixed bug in the checking certificate validity function. A date beyond 2038 was considered invalid.
5. Wireless Status Information Service extended by some status queries (see manual)

Firmware 2.10i --> 2.10k (18. May 2017)

1. Improved scan behavior in the 5 GHz band. Now also "hidden" SSID's are recognized.
2. Improved the transmission of broadcast packets in the pseudo-level 2 bridge mode.
These packets are sometimes sent by the WLAN system as unicast (level 2) packets.

Firmware 2.10k --> 2.10n (12. June 2017)

1. With the 2.10k firmware it came isolated to reboots when roaming, if the signal values (SNR) were only relatively weak. It could be determined that these reboots were triggered by overly intensive debug messages of the Linux kernel. After switching off these messages, this behavior could no longer be observed.
2. The SNMP function has now a "CommunityName" parameter so that a value other than "public" can be set.
3. In bridge mode "Level 2 Pseudo-Bridge" you can now activate a DHCP Relay Agent.

Firmware 2.10n --> 2.10r (04. August 2017)

1. Implementation of a monitoring function which ensures that the bridge process is restarted after an unintended

termination.

2. A "memory leak" caused the free memory to be used up. This was especially the case when the LAN client often opened and disconnected new TCP connections. Depending on the intensity, this could lead to a standstill of the bridge function and require a manual reboot.
3. The Serial Port Config has a new option that determines how to handle data that is received when a wireless connection is not yet available.

Firmware 2.10r --> 2.10s (01. September 2017)

1. Bug found that can terminate the bridge process. This could happen in conditions of a weak signal level with many faulty transmission attempts.
2. Linux kernel version 4.9.46+ integrated

Firmware 2.10s --> 2.11a (10. October 2017)

1. In the debug log messages, the date is now also given in the time stamp.
2. Correction in the SNMP module. Some counters defined as 64-bit values were previously supplied as 32-bit values only.
3. Additional option in NAT & Single Client NAT Mode:
With the "Forward DNS requests" option active, the DNS queries that arrive via the LAN side on the local LAN IP are routed to the DNS server defined on the WLAN side.
4. During repeated failed attempts to authenticate, the WPA Supplicant has blocked the affected SSID for 10 seconds. However, the resulting interruption is very troublesome in some applications. Therefore, an algorithm has been installed, which cancels this lock very soon after activation. The interruption is thus limited to approx. 3 seconds.
5. Linux kernel version 4.9.53+ integrated

Firmware 2.11a --> 2.11b (17. October 2017)

1. Update of the WPA supplicant due to the vulnerability issue known under the name KRACK ("Key Reinstallation Attack") in the security standard WPA2.

Firmware 2.11b → 2.11c (01. February 2018)

1. Linux kernel version 4.9.61+ integrated
2. Zero pointer error in DHCP client fixed.
3. Bug in the log server function fixed.
4. Implemented a NTP server on the LAN side. This NTP server is only active in NAT or Single-Client-NAT mode and transmits the data received by the NTP client on the WLAN side.

Firmware 2.11c → 2.11m (14. June 2018)

1. Linux kernel version 4.9.105+ integrated.
2. Memory error in "Level2 Bridge Mode" fixed. If the LAN client often went offline, memory was reserved that was not freed. This could lead to the MC being unable to communicate after a longer time.
3. Additional parameter "AP Scoring" in the "Roaming" section:
This parameter can be used to determine whether all information such as transmission power, channel load, bandwidth (20 or 40 Mhz) and signal strength (SNR) is used for the rating of an AP or whether the stronger signal alone is rated.
4. Additional "Connection Watchdog" function introduced in the "Roaming" section:
This function enables a monitor that registers the incoming WLAN data from the currently connected AP. If any data is not received for the given time, a new scan is performed. The current AP is rated lower in the following "scoring", so that the AP is likely to change.
5. New parameter in "LAN Client Cloning Mode":
"MAC to Clone" can be used to define a MAC address that is to communicate via WLAN.

Firmware 2.11m → 2.11p (13. August 2018)

1. "Logging" → WLAN Dump Event function deactivated. It turned out that this function has no practical benefit.

2. At „Roaming“ → "Preferred / avoided access points" there is now the option "strictly avoid" with which an access point can be blocked.
3. fixed an error in the relay function in UDP mode.

Firmware 2.11p → 2.11p1 (24. August 2018)

1. fixed an error in the ranking of the AP's in the 2.4GHz band.

Firmware 2.11p1 → 2.12a (28. November 2018)

1. Linux kernel version 4.9.140 integrated
2. The interfaces via which the MC-Config program can access the MC can now be restricted:
 - LAN + WLAN (default)
 - LAN
 - Zugriff gesperrt
3. integrated support for AC radio cards
4. The switching status of the relay can now also be queried via the WLAN info from the LAN client.
5. If WLAN or LAN recordings are active on an MC (→ Logging), this status is displayed in the MCCConfig in the Status column (MCCConfig from version 2.0.2.42).
6. Experimental power save function implemented. This allows the MC to be put into sleep mode for a certain time. In this state, the energy requirement is reduced to ~30% of normal consumption.
7. Port MAC authentication for LAN clients implemented in NAT mode
8. Faster start-up of the MC at the same location (first test last WLAN frequency)
9. If a default reset is done via the reset button, the MC checks whether a USB stick with the file "Default.cfg" is plugged into the device. If yes, this Config is stored internally and activated.
10. LAN cloning: Improved and corrected procedure for handling ARP packets

Firmware 2.12a → 2.12f (25. March 2019)

1. Linux kernel version 4.9.164 integrated
2. Pseudo Level 2 Bridge Mode:
Support for passive clients implemented.
When this function is activated, LAN clients that do not send any data on their own are made "known" in the WLAN by the MC sending pings with the IP of the passive LAN client to a specific IP via WLAN.
3. Home Webside:
In addition to the SNR, the signal strength and the noise level of the received signal are now also displayed.
4. Relay Function:
You can now append a sequence to the command to switch off the relay, which specifies a delay time with which the relay is to be switched off. The delay time is defined as follows <xx> (xx = time in seconds)
5. Bugfix: Special certificate format can now be imported again.
6. Feature: Bridge-Mode
If the bridge function is deactivated, it is now possible to define the IP settings on the LAN side (incl. DHCP client function).

7. Antenna gain can now be specified as a parameter. This allows the radio transmitter to adjust the transmit power so that the legal requirements are met.

Firmware 2.12f → 2.12k (19. September 2019)

1. Linux kernel version 4.9.193 integrated
2. Possible use of TLS to encrypt communication with MCConfig during firmware upgrades or log file downloads
3. Bugfix for crashes when using SNMP with SNMPWalk. Corrections when querying unsigned values.
4. Relay function: Error with missing zero termination eliminated. Now it is also possible to switch on the relay with a delay.
5. Serial function with RS485: Correction for the control of the driver IC
6. WPA3 modes extended. The WPA/WPA2/WPA3 mode can now also be selected.
7. Wireless: DHCP-Renew now also configurable when changing the access point.
8. Website now also works with TLS 1.2
9. Wireless-Info now provides information not only about the configured interval. Now status information can also be queried by request. (only via the LAN side)
10. An attached USB stick with FAT file system can be formatted with EXT4 via the website. This makes the USB stick better suited for recording debug data (logs or dumps).

Firmware 2.12k → 2.12m (17. October 2019)

1. New Kernel 4.9.196 and Openssl 1.0.2t integrated
2. Monitoring the use of the internal flash memory:
In the meantime, there have been cases where the (W)LANDump function (see Logging) has been permanently switched on by the user.
Due to this intensive use over months, the flash memory's function as a file system is severely restricted after some time due to the high "consumption" of reserve sectors.
With firmware version 2.12m, the (W)LANDump function is automatically switched off with regard to the amount of data written, the time that the dump function is active, and the amount of spare sectors that are still available.
3. Also in the 5GHz range you can now set the minimum bitrate.
4. Consideration of special characters in certificate password

Firmware 2.12m → 2.12o (16. January 2020)

New/Changed Features:

1. Upgrade to kernel version 4.9.209

2. In „relay ON“-mode it is now possible to set a timeout for relay functionality.
3. When LAN client cloning is activated, redundant network information is no longer shown on more than one place on the homepage.
4. Wireless configuration can now be changed on the fly, without a need to reboot!
5. Now also pkcs8 keys without passphrase encryption are accepted.

Bugfixes:

1. A bitrate option for 11gb and 11a was wrong (11MBit instead of 12MBit).
2. Serial RS422 implementation was broken due to an previous patch.
3. WEP-LEAP was not functional so far.
4. DHCP client now changes gateway correctly based on changing of gateway availability or prioritizing.
5. In LAN client cloning mode, ARP requests were sent with the IP of cloned client to the LAN interface. This could lead to ip conflicts on client side.
6. Reloading Website content to fast in conjunction with updating configuration could lead to crashes.
7. The DHCP client is now deactivated if the chosen options prevent needing it.
8. Already closed internal processes were continuing to occupy system resources.
9. When using the relay port, the connection wasn't closed properly, which lead to malfunction of the device.

Security updates:

1. Webserver was hardened against CSS attacks (OWASP-Header & Cookies)
2. DoS attacks and other suspicious connections are now recognized, prevented and logged.
3. Accessing over HTTPS is now only possible with acknowledged secure ciphers.
4. HTTPS und HTTP connections are distinctly separated.
5. Too long configuration variables are now discarded directly after input.

Firmware 2.12o → 2.12p (24. January 2020)

Bugfixes:

1. In some circumstances, it could happen that the gateway IP and the DNS server were not set correctly with static IP settings.

Firmware 2.12p → 2.12r (26. May 2020)

New/Changed Features:

1. New kernel 4.9.223 integrated
2. WPA3 now also works with FT (802.11r)
3. An optional custom certificate for the MC internal web server can now be uploaded.
4. Rest-API now provides more information about the serial interface and the relay under /API/Status. Under /API/Status/Device the kernel version is now also specified.
5. BridgeMode NAT:
If the WLAN interface does not do DHCP and no gateway is defined, a gateway can now be defined on the LAN side.
6. Optimization of the LTE variant for LTE campus networks.
7. Roaming optimization based on IEEE 802.11k with configuration options under "Roaming"

Security updates:

1. jQuery library updated to version 3.5.1
2. Measures against SYN and PING Floods.

Firmware 2.12r → 2.12s (29. October 2020)

New/Changed Features:

- 1) New Kernel 4.9.240 integrated
- 2) Improvement in certificate import
- 3) Wireless: Bugfix for the adhoc mode
- 4) Serial: Instead of an IP address you can now also specify a hostname
- 5) Rest API: Import of certificates and status query of loaded certificates is now possible
- 6) Long-term recording of WLAN signal values and roaming processes is now possible
- 7) Relay: Status information of the current state on the website corrected

Firmware 2.12s → 2.12u (08. January 2021)

New/Changed Features:

- 1) New kernel 4.9.253 integrated.
- 2) Possible deadlock on startup fixed.
- 3) The AP list on the "Home" page now also shows the minimum bitrate of the AP.
This allows to make settings regarding the minimum bitrate on the "Wireless -> Main Parameter" page if necessary.
- 4) The function for monitoring the WLAN connection could generate a reset of the WLAN connection too early during the first authentication (EAP). This has been corrected.
- 5) The status query via API now provides information about the WLAN and (or) the LTE radio card.
- 6) 802.11ac option only visible if an AC wireless card is present.
- 7) Maximum switch-off delay for relay function increased from 100 to 3600 seconds.

Firmware 2.12u → 2.12v (15. January 2021)

New/Changed Features:

- 1) Shortens the time it takes to establish a WLAN connection after a restart, only in the case when EAP authentication is active.

Firmware 2.12v → 2.12w1 (29 July 2021)

Security updates:

- 1 New kernel 4.9.277:
This kernel closes the vulnerability that became public under the keyword "FragAttacks".

Functional changes:

- 1 Admin:
Under "Admin" → "Securing Passwords" you can now set that the encrypted parameters (passwords, PSK, certificate keys etc) are not exported when downloading the config.
- 2 NAT bridge mode:
NAT mode now supports the operation of an FTP server on the LAN port. Due to the dynamic ports used for FTP file transfers, it was not possible to define NAT rules for them before. It is now possible to mark a port forwarding rule with the ":ftp" property, so that with the support of the Linux kernel the used ports are automatically forwarded correctly.
In NAT mode, it is now possible to specify a DMZ IP. This allows you to define an IP to which all data packets for which there is no matching forwarding rule are forwarded.
- 3 SCEP:
Expiration improvements. (Improvements for Nexus SCEP service)
Certificate is only replaced after successful expiration (initial generic certificate for SCEP possible). A challenge password is now also transferred during a renewal. Renewal/enrollment can be triggered by configuration value. If possible, an HTTP session is used for the entire renewal/enrollment process (necessary for load balancing of the SCEP service).
- 4 Statistics→Network:
Bit rates and transmitted bytes/frames are displayed more legibly.
- 5 LANCloning:
Parsing the host name from the DHCP request and displaying it on the status page.
- 6 Serial → Special Options → Resend unacknowledged :
Data received via the serial interface and forwarded via TCP are not considered confirmed until they are

confirmed as correctly received by the other side via TCP.

If a TCP connection is interrupted and reestablished, the data saved as unacknowledged is sent again via the new connection.

This can lead to repetitions at the receiver of this data.

7 Network → IP Address:

You can now additionally define special routes if certain IP address ranges are to be reached via special gateways

Bug fixes:

1 Serial → Comserver Mode

In Comserver Mode the handshake mode (RTS/CTS or DTR/DSR) did not work properly

2 Kernel

Fixed problem with transmit bitrate selection in 802.11b/g networks. This problem occurred as of firmware 2.12u.

Firmware 2.12w1 → 2.12x (29. Nov 2021)

Security updates:

New kernel 4.9.290 integrated

Functional changes:

1. Start date:
The MC now no longer starts from the year 2000, but starts with the year in which the firmware was compiled.
2. Json:
UTF-8 and ISO8859-1 escaping corrected
3. LTE:
Delta upgrade function for firmware of EC25 and RM500Q
4. TLS1.2:
NULL ciphers disabled
5. Wireless:
When connecting to access points, a warning will be issued if the channel usage is particularly high. The channel usage for 2.4GHz and 5GHz is better displayed on the web page.
6. SNMP:
The status of the individual LAN ports can now be queried.
7. NAT: Added configuration for +hairpinning (NAT loopback).
8. SCEP:
Longer CA/SCEP server URL possible
Option for HTTP redirect ("Location: ...") added
Option HTTP proxy added.

Bug fixes:

1. Wireless:
802.11k – the Number of neighbor APs limited. If the AP provided a list with more than 31 neighbor AP's, a crash could occur.
2. Wireless:
If the MC was switched on with WLAN switched off and DHCP active, the DHCP client was not started correctly when the WLAN was subsequently switched on via API.