Release notes MC Firmware

Firmware 2.14s → 2.14t (10.04.2024)

Functional changes:

1. Display of Captive Portal if the DHCP client was supplied with option 114 by the DHCP server.
2. Bridge-Mode NAT: Introduction of a parameter to define the timeout (TIME_WAIT) for the connection tracking of the kernel. (Default: 120s)

Bugfix:

1. Roaming/Score: Bugfix for TPC rating for APs transmitting on 5GHz channels >= 128. Under certain circumstances it could happen that APs with low SNR value were rated higher than APs with a higher SNR.

Firmware 2.14r → 2.14s (19.03.2024)

Security updates:

Update of the Linux kernel version from 5.4.265 → 5.4.271

OpenSSL update to version: 3.2.1 (30 Jan 2024)

Functional changes:

implemented EST as an additional method for certificate distribution and updating

ping test: Adjustable parameter "Short Interval", which defines the shortened ping interval after an AP change.

update for the WPA supplicant: git 6777ff62

4th MQTT client: Server Name Indicator (SNI) added for TLS connections.

Bugfix:

1. deleting all dump and log files could cause the firmware to crash

Firmware 2.14p → 2.14r (10.01.2024)

Security updates:

Update of the Linux kernel version from 5.4.256 → 5.4.265

OpenSSL update to version: 3.1.4

Functional changes:

1. SCEP: Challenge variant now also possible with V_ASN1_UTF8STRING.
2. SCEP: RFC 5652: Cryptographic Message Syntax (CMS) implemented
3. WLAN-Dump: new option for selecting what is to be recorded:
   moni0 → (Wireless Header)
   wlan0 → (Ethernet Header)

4. DNS forwarding: now with active handling instead of simple forwarding.
5. The Network Test website now also supports IPv6
6. Pseudo Level2 Bridge Mode: the client IP is now also "learned" from received ARP packets.
7. Reverse lookup of the host name via WLAN IP is now possible
8. MQTT Client + Serial can communicate via IPv6.

Firmware 2.14o → 2.14p (18.10.2023)

Security updates:

Update Linux kernel version from 5.4.252 → 5.4.256

Functional changes:

1. SNMP: SNMPv3 queries are now possible
2. LAN client cloning mode
   Preconnect: This allows you to activate the WLAN even if no client MAC has been detected on the LAN port.
3. Bridge: LAN link delay for cloning (5s) and L2 pseudo bridge (15s) mode can be activated.
   MC2-MultiIO: Inversion of inputs and outputs of the values adjustable by configuration.
4. API/Status:
   $.Wireless.Connection adapted for LANCloning.
   $.Accesspoints[%d].Encryption added

Firmware 2.14n → 2.14o (25.08.2023)

Security updates:

Change Linux kernel version from 5.4.249 → 5.4.252

Functional changes:

1. SYN flood detection increased to 40 SYN burst. On average 5 SYN / sec. are still ok.
2. SNMP: Addition of status values from the info of /proc/net/dev
3. Improvement for IPv6 bridging
4. SCEP: If the CA Identity parameter for the URL contains illegal characters the value is URL-Encoded
5. Display of additional warnings in MCConfig (from Vers.: 2_0_3_9) in the column "Status":
   - For certificates that are about to expire or have already expired.
   - For incorrectly configured ping test.

Firmware 2.14m → 2.14n (24.07.2023)

Security updates:

Change Linux kernel version from 5.4.246 → 5.4.249

Functional changes:

1. Web server security:
   - Preferences for the TLS session handshake algorithms can now be set.
   - New option Send HSTS header
2. EAP: EAP-TTLS can now also be performed without certificates. (similar to EAP-PEAP)
3. Wireless: wpa_supplicant now with 802.11v support.
4. Wireless: now shows in the AP list whether an access point supports 802.11v.
5. Serial: The serial interface can now also communicate via TLS.
   Certificates for authentication can also be installed for this purpose
6. Bridge/NAT: now with warnings for conflicts of local services of the device with NAT rules defined by setup.
7. MQTT Bridge: Now also with local web socket port (default 8080)

Bugfix:

1. Serial: Approx. 1.5KB of memory were not released on each TCP reconnect.
2. WLAN dump: If a filter was set in LAN client cloning to record only its own traffic, then the correct MAC was not taken to define the filter.

Firmware 2.14k → 2.14m (14.06.2023)

Security updates:

Change Linux kernel version from 5.4.242 → 5.4.246

Functional changes:

1. wpa_supplicant updated to 2.11-dev (Git Rev. 95C3f0d1)

2. Improvement in relay control via the
   Faulty sequences and relay commands are now rejected with HTTP Error 400.
3. Output of a warning in the debug log if all matching SSID's are evaluated with 0 during the score calculation. This indicates that one of the crypto settings does not match.
4. Warning in debug log after startup if certificates (client and CA certificates) are loaded that are about to expire or have already expired.

Firmware 2.14i → 2.14k (05/16/2023)

Security updates:

Change of Linux kernel version from 5.4.240 → 5.4.242

Functional changes:

1. relay is now controllable via REST API and using statement sequences.
   authentication of individual API/URLs:
2. This makes it possible to secure access to specific API functions with a separate user/password without having to use the user/password for device configuration.
3. remote capture deamon:
   This allows e.g. via Wireshark recordings on the (W)LAN interface of a MCx to be remotely retrieved and displayed live.

Bugfix:

Segfault error in the MQTT function fixed (TLS-Write).
Segfault error in the timer module fixed (Blacklist + ConfigChange)

Firmware 2.14h → 2.14i (12.03.2023)

Security updates:

Linux kernel version change from 5.4.233 → 5.4.240

Functional changes:

1) EAP hanging and 4-way Handshake timeout are now also included in the connection statistics of the AP's used.
   EAP authentication: additional option for enabling TLS 1.2.
   TLS 1.2 was not active until now because of problems with older RADIUS servers.
   For compatibility reasons this option is not active by default.
2) ping test: The debug output has been revised. The debug level for this function is now dependent on the "Wireless Debug Level".

Firmware 2.14g1 → 2.14h (02.03.2023)

Security updates:

Change of Linux kernel version from 5.4.231 → 5.4.233

Functional changes:

1) MQTT client: MQTT client can now send status values, which can also be read via the REST API (Status).
2) MQTT client: QoS adjustable for all publishes.
3) MQTT client: connection timeout adjustable (Previously fixed to 60 seconds).
4) MQTT client: the LWT is now also triggered when the MC is specifically restarted.
5) Logging: WLAN dumps with filter option. So you can e.g. log only your own WLAN traffic. This significantly extends the monitored period in many systems.

Bugfix:

Network dumps: If a lot of data was sent or received via (W)LAN when the memory for the dump files was full, the system could crash (reset).
This bug has been fixed.

Firmware 2.14f → 2.14g1 (10.02.2023)

Security updates:

Linux kernel version change from 5.4.228 → 5.4.231 BuildRoot 2022.08.3.

Functional changes:

The REST API query API/Status/Device now also provides the device name.

Bugfix:

As of version 2.14, an AP Density setting not equal to "autodetect" resulted in poor roaming behavior.

Firmware 2.14e → 2.14f (04.01.2023)

Security updates:

Change Linux kernel version from 5.4.215 → 5.4.228 BuildRoot 2022.08.3

Functional changes:

1. With firmware 2.14, the ARP table of the WLAN interface was deleted after each AP change, so that ARP request - response always had to be exchanged before communication could be continued. With the 2.14f there is the option "Clear ARP" (->Roaming) with which the deletion of the ARP table is prevented by default.
2.
3. (Roaming) The EAP authentication watchdog is now configurable. Previously, this timeout was adjusted based on the measured duration of the last successful EAP handshake. Now a fixed timeout (1,2,3,4 seconds) can also be set.

4. For the transfer of the configuration file a compression of the data takes place now. This leads to a faster transfer of the configuration.

5. (Logging) A separator can now be specified between the various information output. This makes it easier to insert the debug output into a table, if necessary.

6. Detection of replay packets. If these are registered in large numbers within a short time, the WLAN connection is disconnected and re-established.

7. The numbering of the debug files in the USB stick is now done with leading zeros, so that a better sorting of the file names results.

Firmware 2.14d → 2.14e (18.10.2022)

Security updates:

Change Linux kernel version from 5.4.218 → 5.4.219

Fix for:
CVE-2022-42719

Firmware 2.14c → 2.14d (16.10.2022)

Security updates:

Change Linux kernel version from 5.4.215 → 5.4.218

Fix for:
CVE-2022-41674
CVE-2022-42720
CVE-2022-42721
CVE-2022-42722

Firmware 2.14b → 2.14c (10.10.2022)

Security updates:

Change Linux kernel version from 5.4.202 → 5.4.215

Functional changes:

1) new REST API function: LAN port status + OpenVPN server request for CA-Cert and Client-Config
2) MQTT-Client for serial, relay and AUX input

Bug fixes:

1) Relay: The relay timeout that can be started via the input was not reset if the relay was controlled via the network during the expiry time of this timer.
2) Serial: Fixed RTS/CTS handshake error.

Firmware 2.12x → 2.14b (04.07.2022)

Security updates:

Change Linux kernel version from 4.9.290 → 5.4.202

Functional changes:

1. MWLC:
   PAE (Port Access Entity) forwarding implemented in MWLC mode
   MWLC master can now also be defined as host name.

2. Print Server:
   Adaptive detection of whether a connected printer is detected as lp0 or lp1.

3. Web interface:
   Additional page under "Device" → "Network Test"
   Network connections can be tested there starting from the MC.

   Home page: additional information about the connected LAN clients in NAT mode.

4. Default Reset (Clear Dumps and Log):
   now also existing coredump files are deleted.

5. SNMP:
   new info about theIP address of the WLAN interface (1.3.6.1.4.1.29456.3.15.0)

6. AUX-IN:
   Switching the AUX-IN function on and off via Config no longer leads to a reboot of the MC

7. NAT mode: snat option introduced.
   With this the LAN client sees the IP of theLAN interface from the MC as source.

8. ARP probe: during the ARP probe test of the MC, incoming responses are now better evaluated. This avoids that repetitions of ARP probes sent by the AP are recognized as such and are not evaluated as an IP conflict.

9. LTE:
   Added selection of authentication types " PHP+CHAP,PAP,CHAP".
   OpenVPN: Import of client config improved.
   OpenVPN client: TUN mode correction. Masquerading and NAT support.
   OpenVPN server/client: New version: OpenVPN 2.5.6.
   Upgrade LTE firmware only if it is not already the current one
   International Mobile Equipment Identity) in status query
   5G: Kampus network corrections (5G-SA).

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.

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 2.12u → 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 2.12s → 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 2.12r → 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 2.12p → 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 2.12o → 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 2.12m → 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 2.12k → 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 2.12f → 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 2.12a → 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 2.11p1 → 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 MCConfig in the Status column (MCConfig 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 2.11p → 2.11p1 (24. August 2018)

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

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 2.11c → 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 2.11b → 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.