

MC

802.11 a/b/g/n

WLAN-Bridge
&
Serial Client Adapter

Handbuch



MC1



MC4



MC2



MC6C

Inhaltsverzeichnis

1 Technische Beschreibung	5
1.1 Anschlüsse am MC1	6
1.2 Anschlüsse am MC2	7
1.3 Anschlüsse am MC4	8
1.4 Anschlüsse am MC6C	8
1.5 Bedeutung der LED-Anzeigen	8
1.6 Technische Eigenschaften	10
1.7 WLAN - Schnittstelle	10
1.8 Sicherheits- und Installationshinweise	10
2 Inbetriebnahme	11
2.1 <i>Inbetriebnahme des MC</i>	11
2.1.1 Inbetriebnahme mit dem MC-Config-Programm	11
2.1.2 Inbetriebnahme über das MC WEB-Interface	13
2.2 Zurücksetzen der Einstellungen auf Defaultwerte	13
3 Webinterface Informationsseite	13
3.1 System Information	14
3.2 Wireless Status Information	14
3.3 Wired LAN Status Information	16
3.4 Relay Status Information	16
3.5 Input Status Information	17
3.6 Serial 1	17
3.7 Traffic Usage Information	18
3.8 Network Information	18
3.9 Access Point Information	19
3.10 HTTPS Webinterface	20
3.11 Storage Status Information	20
3.12 WLAN und LAN-Dump-Dateien	21
4 Firmware- und Konfigurationsmanagement: Device Menü	21
4.1 Firmware	21
4.2 Configuration Management	23
4.3 Network Test	24
5 Einstellung der Betriebsparameter: Configuration Menü	25
5.1 Admin	25
5.1.1 Device Name	25
5.1.2 Security	25
5.1.3 SNMP	26
5.1.4 Webserver	26
5.1.5 URL Authentication	27
5.1.6 Configuration tool accessibility	27
5.1.7 Auto Firmware Upgrade	28
5.1.7.1 Funktion	28
5.1.7.2 Voraussetzungen	28
5.1.7.3 Aufbau der Antwortdatei	28
5.1.7.4 Bereitstellung der Firmwaredatei	29
5.1.7.5 Sicherheitshinweise	29
5.1.7.6 Parameter	29
5.1.8 Other Options	29
5.1.8.1 Serial port instances	29
5.1.8.2 Power Save	29
5.1.8.3 Securing Passwords	29
5.1.8.4 Webserver certificate	29
5.2 Security	30
5.3 Certificate	31
5.3.1 Main Certificate	31
5.3.2 SCEP	32
5.3.3 EST	32
5.4 Network	34
5.4.1 IP Address	34
5.4.2 Bridge	35
5.4.2.1 Bridge-Mode OFF	36
5.4.2.2 LAN-Client-Cloning	36

5.4.2.3 NAT und Single Client NAT.....	39
5.4.2.3.1 Forwarding rules for NAT.....	41
5.4.2.3.2 DHCP-Server.....	42
5.4.2.3.3 Static DHCP Server entries:.....	43
5.4.2.4 Level 2 Pseudo-Bridge Modus.....	44
5.4.2.5 MWLC Mode.....	46
5.4.2.5.1 MWLC-Master.....	47
5.4.2.5.2 MWLC-Slave.....	47
5.4.3 Bridge not active Mode.....	48
5.4.4 MQTT Client.....	49
5.5 Wireless.....	51
5.5.1 Main Parameter.....	52
5.5.1.1 Wireless Mode.....	52
5.5.1.2 SSID-Profiles.....	52
5.5.1.3 Phy Mode.....	52
5.5.1.4 Country selection.....	52
5.5.1.5 Enable sleep mode.....	52
5.5.1.6 802.11bg bitrate setting.....	52
5.5.1.7 802.11a bitrate setting.....	52
5.5.1.8 Power selection.....	52
5.5.1.9 Antenna gain.....	52
5.5.1.10 Antenna selection.....	52
5.5.1.11 Filter SSID.....	52
5.5.1.12 Wireless Status Information Service.....	53
5.5.2 SSID Profile.....	53
5.5.2.1 SSID Profile.....	53
5.5.2.2 Profile change action.....	53
5.5.2.3 Connect Action.....	54
5.5.2.4 Security Parameter.....	54
5.5.2.5 EAP.....	56
5.5.2.6 Certificates.....	56
5.5.3 Roaming.....	56
5.5.3.1 Roaming Parameter.....	57
5.5.3.1.1 AP Density.....	57
5.5.3.1.2 Channels for Roaming.....	57
5.5.3.1.3 Min scan interval.....	57
5.5.3.1.4 Max scan interval.....	57
5.5.3.1.5 Blacklist Timer.....	57
5.5.3.1.6 802.11r(FT) Mode.....	58
5.5.3.1.7 Accesspoint Score Calculation.....	58
5.5.3.2 Background Scanning.....	58
5.5.3.3 Connection Watchdog.....	58
5.5.3.4 Ping-Test.....	58
5.5.3.5 Connection test (ARP).....	59
5.5.3.6 Preferred / avoided access points.....	60
5.5.3.7 Clear ARP.....	60
5.6 Funktion der seriellen Schnittstelle.....	60
5.6.1 Parameter der seriellen Schnittstelle.....	60
5.6.2 Network-Configuration Parameter.....	61
5.6.2.1 TCP/IP-Server-Mode:.....	61
5.6.2.2 TCP/IP-Client-Mode:.....	61
5.6.2.3 UDP/IP-Mode:.....	61
5.6.2.4 Printerserver-Mode:.....	61
5.6.2.5 COMSERVER-Mode:.....	62
5.6.2.6 MQTT Mode:.....	62
5.6.2.7 REST-API.....	62
5.6.2.7.1 Daten an die serielle Schnittstelle senden.....	62
5.6.2.7.2 Daten von der seriellen Schnittstelle empfangen.....	62
5.6.3 „Keep alive“-Parameter.....	63
5.6.4 „Handshake-Mode“ Parameter.....	63
5.6.5 Enable dump.....	64
5.7 Printer server configuration.....	64
5.8 Relay Configuration.....	64
5.8.1 Parameter zur Steuerung des Relais.....	64

5.8.2 Verzögertes Ein- und Ausschalten des Relais.....	66
5.9 Realtime Clock Configuration.....	67
5.10 Input Configuration.....	67
5.10.1 Input-Abfrage im UDP-Mode.....	68
5.11 Logging Configuration.....	68
5.11.1 Systemmeldungen aufzeichnen.....	68
5.11.1.1 Debug Log.....	68
5.11.1.2 Debug Information.....	69
5.11.1.3 Syslog Server.....	69
5.11.1.4 Traffic Dump Configuration.....	70
5.11.1.4.1 Debug-Dateien mit dem MC-Config Programm vom MC herunterladen.....	73
5.11.1.5 Debug Configurations.....	74
6 Systemmeldungen: Statistics Menü.....	75
6.1 Statistics - System Log.....	75
6.2 Statistics - Network.....	76
7 Konfiguration der MC-Geräte mit einem USB-Speicherstick.....	77
7.1 Übertragung einer Konfigurationsdatei bei einem „Default-Reset“.....	77
7.2 Anwendung für den Config-USB-Stick.....	77
7.2.1 Initialisierung eines USB-Speichersticks.....	77
8 REST-API.....	78
9 Open Source Compliance Information.....	81

Abbildungsverzeichnis

Abbildung 1.1: Gesamtsystem (Beispiel).....	5
Abbildung 1.2: Anschlüsse und LED's am MC1-SL-M12.....	6
Abbildung 1.3: WK8 Spannungsanschluss.....	7
Abbildung 1.4: M8 Spannungsanschluss.....	7
Abbildung 1.5: Steckeranordnung auf der Rückseite des MC2-SL-M12.....	7
Abbildung 1.6: Steckeranordnung auf der Rückseite des MC4-SL-M12.....	8
Abbildung 1.7: MC6C im Gehäuse.....	8
Abbildung 2.1: Aufbau zur Inbetriebnahme des MC.....	11
Abbildung 2.2: Erstinbetriebnahme mit dem MConfig-Programm.....	12
Abbildung 2.3: Screenshot vom MC-Config-Programm.....	12
Abbildung 3.1: Access Point Liste.....	19
Abbildung 3.2: USB-Speicherstatus.....	21
Abbildung 3.3: WLAN- und LAN-Dump-Dateien.....	21
Abbildung 4.1: Firmware Upgrade Dialog.....	22
Abbildung 4.2: Configuration Management.....	23
Abbildung 4.3: Network Test.....	24
Abbildung 5.1: Certificate Upload.....	32
Abbildung 5.2: LAN Client Cloning Mode.....	38
Abbildung 5.3: NAT-Modus (Beispielkonfiguration).....	39
Abbildung 5.4: Level 2 Bridge (Beispielkonfiguration).....	44
Abbildung 5.5: MWLC-Mode Beispielkonfiguration.....	46
Abbildung 5.6: Parameter für die Pingtest-Funktion.....	59
Abbildung 5.7: Preferred or avoided AP list.....	60
Abbildung 5.8: Serial MQTT Parameter.....	62
Abbildung 5.9: Relais Parameter.....	64
Abbildung 5.10: Debug Log Parameter.....	70
Abbildung 5.11: Traffic Dump Configuration.....	71
Abbildung 5.12: Wireless und Ethernet Dump Dateien.....	72
Abbildung 5.13: Download Dumps and Logs mit dem MC-Config-Programm.....	73
Abbildung 5.14: Dateiauswahl zum Herunterladen oder zum Löschen.....	73
Abbildung 5.15: Debug Configurations.....	75
Abbildung 6.1: Beispiel einer System Log Ausgabe.....	76
Abbildung 6.2: Beispiel einer Statistics Network Ausgabe.....	76
Abbildung 7.1: Init USB Config Stick.....	77

1 Technische Beschreibung

Der MC ist ein WLAN-Adapter zum Anschluss von Geräten mit Ethernet-, USB- oder serieller Schnittstelle an drahtlose Netzwerke nach dem 802.11 a/b/g/n Standard. Der MC verbindet über die Ethernet-Schnittstelle alle Geräte des LAN-Segments an das er angeschlossen ist mit einem über WLAN erreichbaren Netzwerk.

Über die serielle Schnittstelle kann der MC Daten empfangen und senden, die von einem über das Netzwerk (WLAN oder LAN) angeschlossenen Kommunikationspartner gesendet bzw. empfangen werden. Dieser Kommunikationspartner kann wiederum ein MC sein oder aber ein Rechner, der über eine passende Applikation diese Daten empfängt bzw. sendet. Über die USB-Schnittstelle können u.a. Drucker angeschlossen werden. Der MC kann damit als Printerserver arbeiten. Über den USB-Port sind aber auch Erweiterungen möglich, die z.B. zusätzliche serielle oder I/O - Schnittstellen bieten.

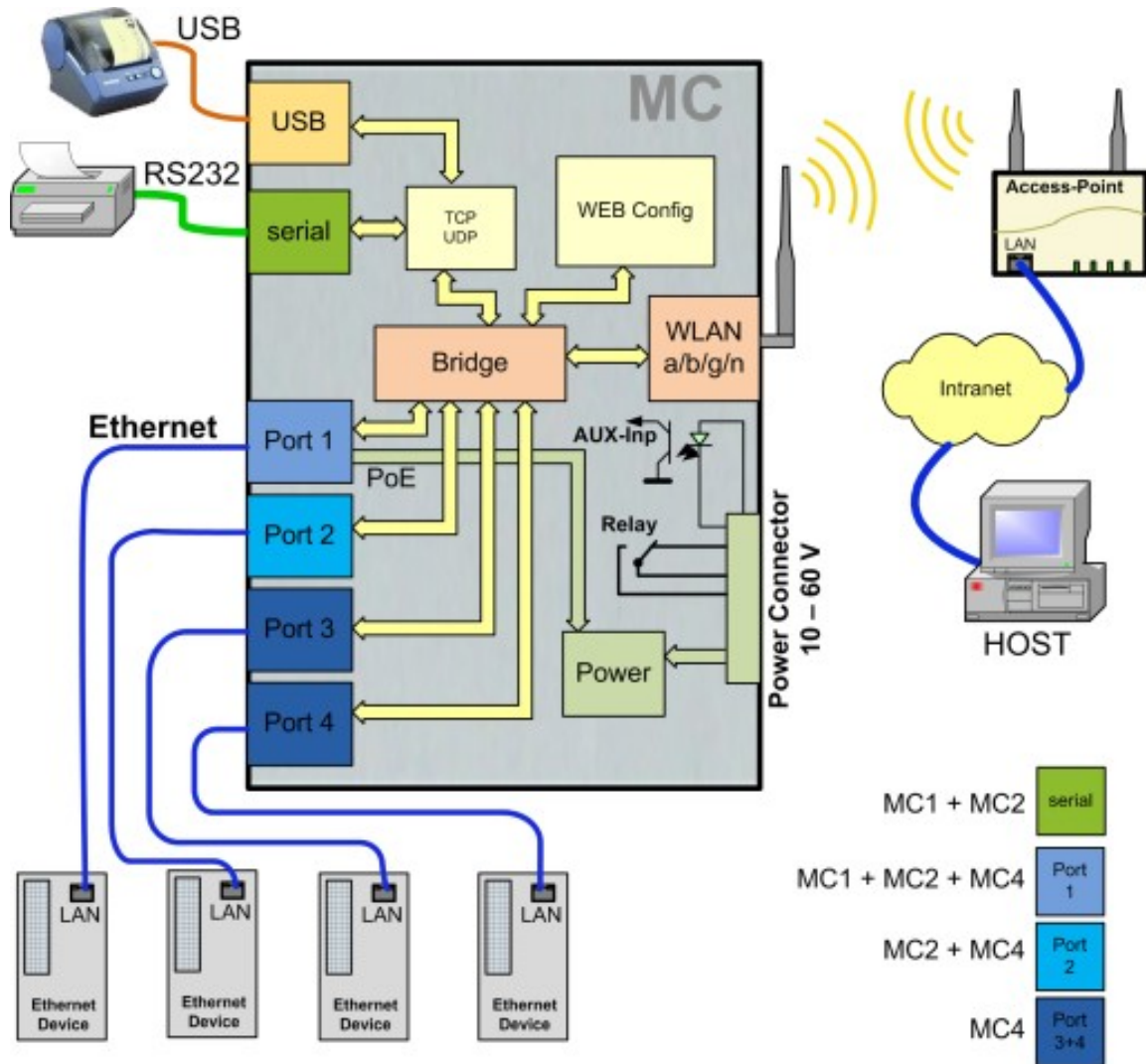


Abbildung 1.1: Gesamtsystem (Beispiel)

Die verschiedenen Gerätevarianten MC1, MC2 und MC4 unterscheiden sich im Wesentlichen in der Anzahl der LAN-Ports. Der MC4 hat keinen RS232 Anschluss.

Alle Varianten funktionieren mit der gleichen Firmware.

Das zentrale Bauteil des MC ist ein ARM® Cortex®-A9 Prozessor, der alle Funktionen steuert. Die Schnittstellen sind:

- 1) Mini-PCI-Express Socket
- 2) Ethernet-Interface mit einem bis 4 Ports 10/100/1000 MBit/s +Auto-MDIX (auto crossover Funktion)
Port 1 hat die PoE (Power over Ethernet) Funktion.
- 3) 1 x serielle Schnittstelle mit 6 Steuerleitungen (nicht beim MC4)
- 4) 1 x USB2 – Anschluss z.B. für Etiketten-Drucker oder Schnittstellenerweiterungen

5) optional: Relais-Schaltkontakt + Schalteingang mit Optokoppler

Der Ethernet-Anschluss ist als RJ45 Stecker ausgeführt. Der LAN-Port 1 hat eine PoE Funktion (IEEE 802.3af), sodass der MC über diesen Port mit Spannung versorgt werden kann.

Die serielle Schnittstelle wird über eine 9pol. D-SUB Buchse angeschlossen. Die Belegung ist so gewählt, dass der Anschluss über ein 1 zu 1 seriell Kabel mit dem COM-Port eines PC's verbunden werden kann. Die genaue Belegung können Sie der Abbildung 1.2 entnehmen.

Zur Stromversorgung benötigt der MC eine Spannungsquelle im Bereich zwischen 10-60V. Der typische Energiebedarf liegt bei ca. 3,0 Watt (WLAN + LAN-Port aktiv)

1.1 Anschlüsse am MC1

Die folgenden Bilder zeigen, wie die Anzeige-LED's und Anschlüsse am MC1 angeordnet sind.

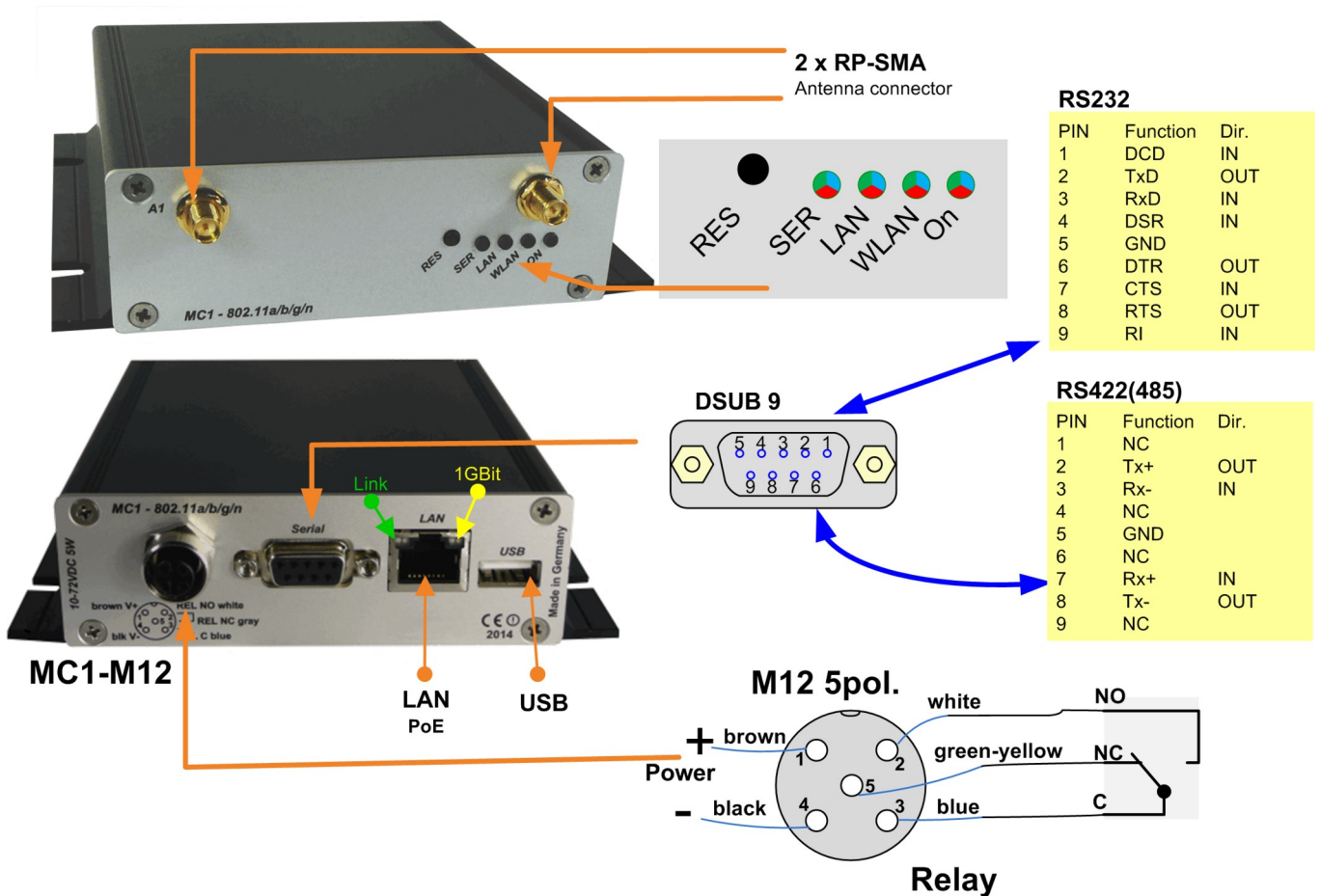
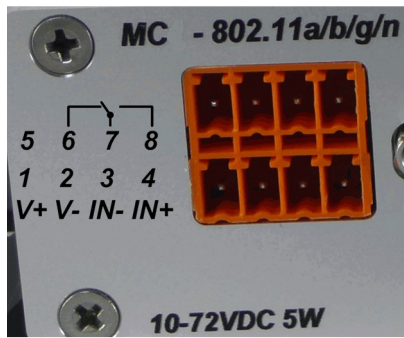


Abbildung 1.2: Anschlüsse und LED's am MC1-SL-M12

Die Abbildung zeigt den MC1 in der Standard-Ausstattung mit einer seriellen Schnittstelle und einem 5 poligen M12-Steckerverbinder zum Anschluss der Spannung und des Relais-Schaltkontakts.

Den Spannungsanschluss gibt es für alle MC-Geräte in weiteren Varianten:



MC -WK8

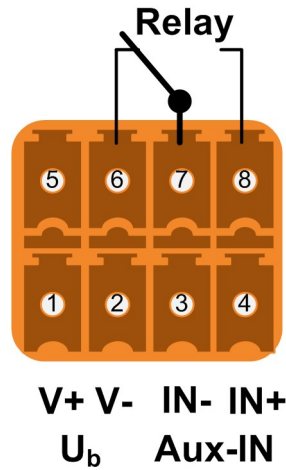
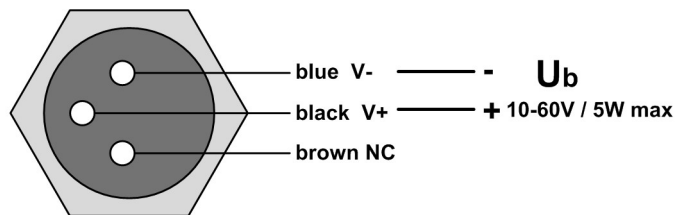


Abbildung 1.3: WK8 Spannungsanschluss



MC1-M8

Abbildung 1.4: M8 Spannungsanschluss

1.2 Anschlüsse am MC2

Der MC2 hat auf der Frontblende die gleichen LED's incl. Resettaster wie der MC1. Die Rückseite hat folgende Steckeranordnung:

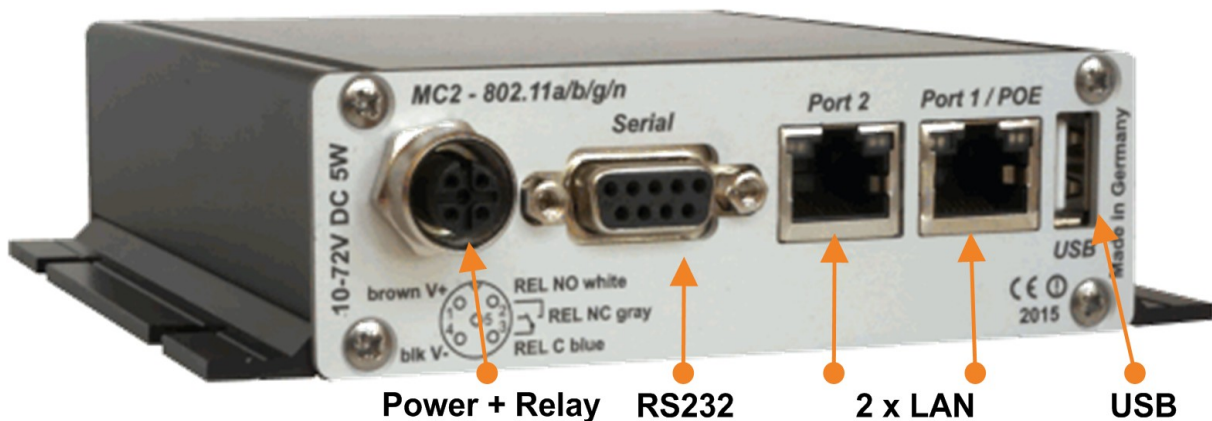


Abbildung 1.5: Steckeranordnung auf der Rückseite des MC2-SL-M12

Den MC2 gibt es auch in den Varianten MC2-Sx-WK8 und MC2-Sx-M8.

1.3 Anschlüsse am MC4

Der MC4 hat auf der Frontblende die gleichen LED's incl. Resettaster wie der MC1. Die Rückseite hat folgende Steckeranordnung:

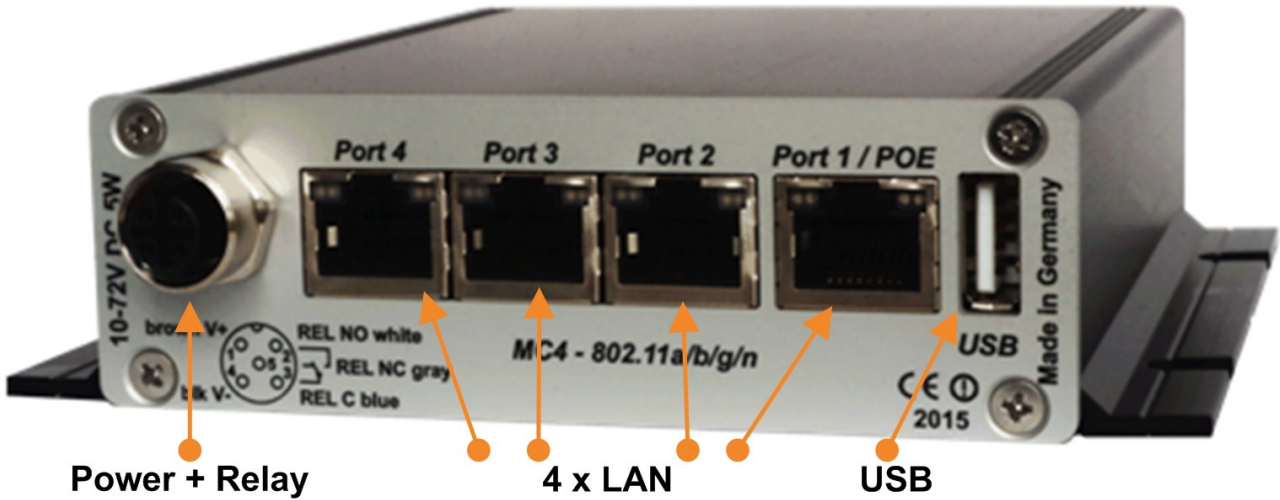


Abbildung 1.6: Steckeranordnung auf der Rückseite des MC4-SL-M12

Den MC4 gibt es auch in den Varianten MC4-Sx-WK8 und MC4-Sx-M8 (ohne Relais)

1.4 Anschlüsse am MC6C

Der MC6C-G1 hat auf der Oberseite die gleichen LED's wie der MC1. Die Resettaste kann mithilfe einer Nadel bzw. einer Büroklammer über eine Bohrung im Gehäuse betätigt werden.

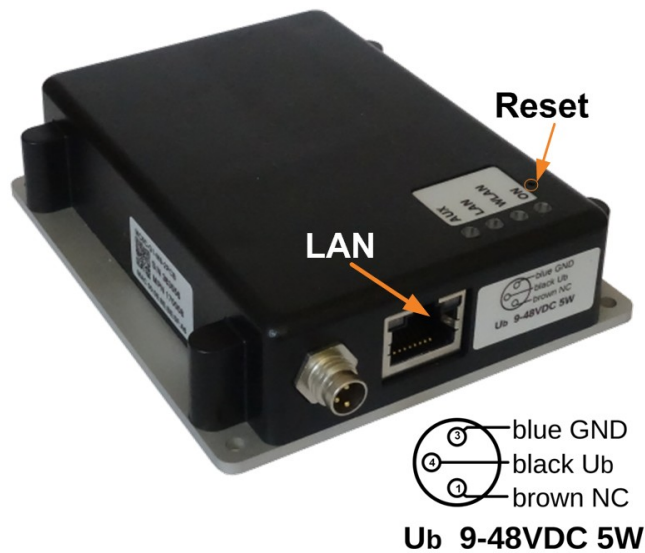


Abbildung 1.7: MC6C im Gehäuse

1.5 Bedeutung der LED-Anzeigen

Die 4 LED's an der Frontseite zeigen den Betriebszustand des MC an. Alle LED's sind 3-farbige rot, grün und blau leuchtende LED's. Wenn alle drei Farben eingeschaltet sind, leuchten die LED's weiß.

Alle 4 LED's leuchten nach dem Einschalten oder nach einem Reset einmal kurz weiß auf. Wenn die LED's WLAN + LAN + SER blau blinken, wird gerade entweder eine neue Firmware geflasht oder eine neue Konfiguration aktiviert.

LED	Zustand	Funktion
On	aus	keine oder nicht ausreichende Versorgungsspannung
	grün	Versorgungsspannung angeschlossen
	grün / orange blinkend	Normalbetrieb Dieses grün <--> orangene Blinken zeigt, dass das MC-Programm arbeitet.
	blau orange blinkend	(ab Firmware 2.15) Zeigt an, dass der MC wegen ungenügend sicherer Einstellungen nicht als Bridge aktiv ist. Die Konfigurationsschnittstellen (WEB + MCConfig) sind aktiv. Beachten Sie dazu die Hinweise im Web-Interface oder im MCConfig-Programm. (Config→Security) Im Auslieferungszustand bzw. nach einem Default-Reset wird dieser Zustand angezeigt, weil kein User/Passwort gesetzt ist.
WLAN	aus	WLAN Schnittstelle abgeschaltet
	rot blinkend	Der MC sucht nach passenden AP's oder ist dabei sich zu authentifizieren
	grün	WLAN-Verbindung OK. Kurzes rotes Aufleuchten signalisiert Aktivität (Senden oder Empfangen) auf der Schnittstelle.
LAN	aus	Kein Gerät an den LAN-Ports angeschlossen
	grün	An einem der LAN-Ports ist ein Gerät angeschlossen und eingeschaltet.
	grün / orange blinkend	Kurzes oranges Aufleuchten bei Aktivität auf der Schnittstelle.
Serial TCP- Mode	aus	Die Schnittstelle ist inaktiv
	grün	Ein Kommunikationspartner hat sich mit der Schnittstelle verbunden. Wenn Daten gesendet oder empfangen werden wird die rote LED für kurze Zeit eingeschaltet.
	grün / orange blinkend	
	grün blinkend	Die Schnittstelle ist im TCP- Server Mode aktiv und wartet auf eine Verbindung.
	rot blinkend	Die Schnittstelle ist im TCP- Client Mode aktiv und wartet auf den Aufbau der Verbindung zum Server.
Serial UDP- Mode	aus	Die Schnittstelle ist inaktiv
	grün	Schnittstelle initialisiert
	grün / weiß blinkend	Daten werden gesendet oder empfangen. Wenn kontinuierlich Daten gesendet oder empfangen werden, leuchtet die LED dauernd weiß.

Tabelle 1: LED Zustandsanzeige

1.6 Technische Eigenschaften

Spezifikationen:	
Ethernet	1, 2 oder 4 x LAN-Port 10/100/1000 MBit/s Auto MDI/MDIX
Seriell	1 x RS232, 300-460,8 KBit/s, RTS, CTS, DSR, DTR, RI, DCD oder (optional) RS485
USB	1 x USB 2.0 zum Anschluss von Druckern oder USB-Adaptern mit verschiedenen anderen Schnittstellen
Relais	1 x Umschalter max 1A@24V, max 125VAC
Schalteingang	1 x galv. getrennt 10 – 60V
Antennenanschluss	2 x RPSMA (optional TNC oder RPTNC)
Spannungsversorgung	10 – 60 VDC oder 802.3af PoE über den LAN Port 1
Energiebedarf	<= 5W (3W typisch)
Temperaturbereich	0-60°
Maße	105x125x35mm
Gewicht	ca. 400g

1.7 WLAN - Schnittstelle

WLAN-Schnittstelle:		
Technologie	802.11 a/b/g/n WLAN (2.4 + 5 GHz Band)	
Antennen:	2 Antennen (2T2R MIMO)	
Verschlüsselung	WEP (64, 128bit) + TKIP/AES	
Sicherheit	802.11i WPA(2)(3) – PSK 802.1x EAP-PEAP, -TLS, -TTLS, -LEAP	
Kanäle	802.11b/g/n ETSI 1-13, USA/Kanada 1-11 802.11a/n ETSI 19 + 5, USA/Kanada 25 (U-NII-1 + UNII-2A + U-NII-2C+U-NII-3)	
Datenraten	Mode	Datenrate
	802.11b:	1, 2, 5.5, 11Mbps
	802.11g / a	6, 9, 12, 18, 24, 36, 48, 54Mbps
	802.11n (20MHz)	1Nss: max. 72.2Mbps 2Nss: max. 144.4Mbps
	802.11n (40MHz)	1Nss: max. 150Mbps 2Nss: max. 300Mbps
Sendeleistung	802.11b/g 17 dBm	802.11a 15 dBm
	802.11gn 16 dBm	802.11an 15 dBm

Tabelle 2: Eigenschaften der WLAN-Schnittstelle

1.8 Sicherheits- und Installationshinweise

VORSICHT: Störanfälligkeit medizinischer Geräte

Dieses Gerät strahlt Hochfrequenzenergie im ISM-Frequenzbereich (Industrial, Scientific, Medical) ab.

- Achten Sie darauf, dass alle medizinischen Geräte in der Nähe dieses Geräts die Vorgaben zur Störanfälligkeit für diese Art der Hochfrequenzenergie erfüllen.

ACHTUNG: Funkstörungen im Wohnbereich

Dieses Gerät ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen.

- In diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

ACHTUNG: Elektrostatische Entladung

Dieses Gerät enthält Bauelemente, die durch elektrostatische Entladung (ESD) beschädigt werden können.

- Treffen Sie entsprechende Schutzvorkehrungen gegen elektrostatische Entladung.

ACHTUNG: Anforderung an die Spannungsversorgung

Das Modul ist ausschließlich für den Betrieb mit Sicherheitskleinspannung (SELV) nach EN/IEC 60950-1 und VDE 0805 ausgelegt.

– Achten Sie auf die korrekte Spannungsversorgung.

ACHTUNG: Anforderung an die Stromquelle

Das vorliegende Gerät darf nur mit Spannungsversorgungen betrieben werden, die die Vorgaben der EN/IEC 60951-1 für Stromquellen begrenzter Leistung erfüllen.

– Betreiben Sie das vorliegende Gerät mit einer Spannungsversorgung, die die Vorgaben der EN/IEC 60951-1 erfüllt.

– Betreiben Sie das vorliegende Gerät alternativ in einem Gehäuse, das den Anforderungen einer Brandschutzumhüllung nach EN/IEC 60951-1 genügt.

ACHTUNG: HF-Abstrahlung

Dieses Gerät strahlt Hochfrequenzenergie im ISM-Frequenzbereich (Industrial, Scientific, Medical) ab.

– Betreiben Sie das Gerät mit einem Mindestabstand von 20 cm zwischen dem Strahler bzw. der Antenne und Ihrem Körper.

2 Inbetriebnahme

Zur Erstinbetriebnahme verbinden Sie bitte zunächst einen Rechner mit Ethernet-Anschluss über ein Patchkabel mit dem LAN-Anschluss des MC.

Nach dem Einschalten der Versorgungsspannung des MC leuchten zunächst alle LED's kurz weiß auf. Danach leuchtet nur die ON-LED grün, die auch bald darauf anfängt orange-grün zu blinken. Nach ca. 15 Sekunden ist die Applikation vollständig betriebsbereit und die LED's leuchten mit der Funktion, wie sie oben beschrieben wurde.

2.1 Inbetriebnahme des MC

2.1.1 Inbetriebnahme mit dem MC-Config-Programm

Zur Inbetriebnahme kann der MC zunächst nur über den LAN-Anschluss kommunizieren, weil in der Regel kein Funknetz mit einer passenden SSID vorhanden ist bzw. die WLAN Funktion abgeschaltet ist.

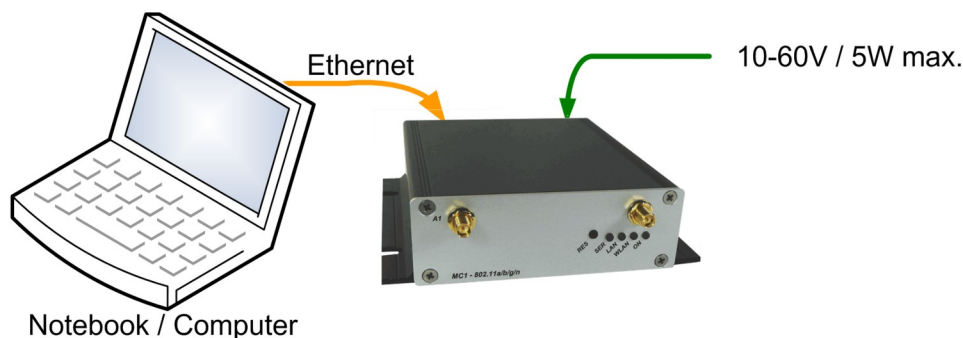


Abbildung 2.1: Aufbau zur Inbetriebnahme des MC

Der MC wird mit einem PC mit Ethernet-Anschluss verbunden. Auf dem PC wird das MC-Config-Programm gestartet.

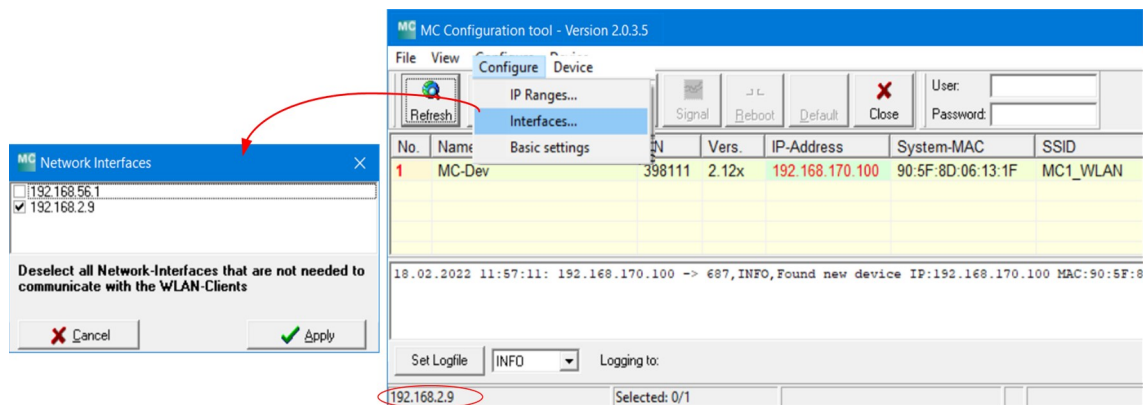


Abbildung 2.2: Erstinbetriebnahme mit dem MCConfig-Programm

Worauf zu achten ist:

- Der angeschlossene PC (Notebook) sollte auf der LAN-Schnittstelle eine **feste** IP-Adresse haben (kein DHCP).
- Diese IP sollte im MC-Config-Programm unten links in dem Statusfeld auftauchen.
- Wenn dort mehrere IP-Adressen aufgeführt werden, können Sie nur die relevante Schnittstelle mit „Configure“ → „Interfaces“ gezielt aktivieren.
- Nach einer Änderung dieser Konstellation betätigen Sie noch mal die „Refresh“-Taste beim MC-Config-Programm.
- Eine aktive Firewall auf dem PC könnte ggf. die Kommunikation zum MC verhindern.

Das MC-Config-Programm ermittelt nach dem Start zunächst alle Netzwerk-Schnittstellen, die aktuell auf dem Rechner aktiv sind. Auf diese Schnittstellen werden Broadcast-UDP-Anfragen geschickt, auf die MC-Geräte antworten. Die antwortenden Geräte werden registriert und in einer Liste angezeigt.

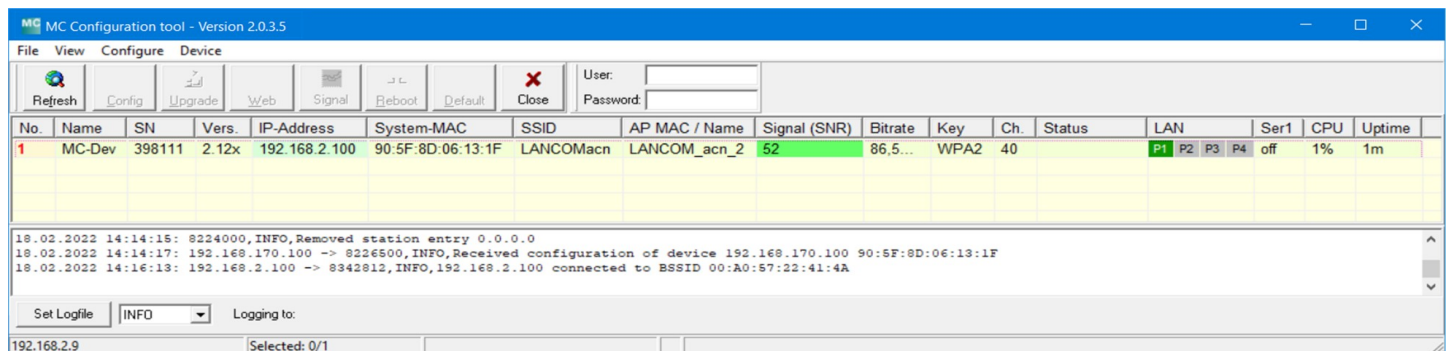


Abbildung 2.3: Screenshot vom MC-Config-Programm

Neben den Gerätedaten wie Name, Seriennummer, Firmwareversion, IP-Adresse und MAC-Adresse werden auch WLAN Verbindungsdaten angezeigt. Zunächst kann man nur die eingestellte SSID sehen. Wenn eine Verbindung zu einem Access Point besteht, wird die MAC-Adresse und bei bestimmten WLAN-Systemen auch der Name dieses AP's angezeigt. Die Signalstärke wird als SNR-Wert in dBm mit einer entsprechenden Hintergrundfarbe dargestellt. Die SNR-Werte kann man wie folgt interpretieren:

- Signal ≥ 40 → sehr gute Verbindung
- Signal ≥ 30 → gute Verbindung
- Signal ≥ 20 → Verbindung noch ausreichend
- Signal < 20 → Verbindung eingeschränkt, die Bitraten werden verringert um Daten zu übertragen.

Eine genauere Beschreibung zur Bedienung des MC-Config-Programms finden Sie in einem separaten Handbuch.

2.1.2 Inbetriebnahme über das MC WEB-Interface

Wenn Sie das MC-Config-Programm nicht nutzen möchten oder können, kann man die MC Geräte auch mit Hilfe eines WEB-Browsers in Betrieb nehmen.

Dazu muss man die LAN-Schnittstelle es Inbetriebnahme-Rechners auf eine feste IP-Adresse einstellen. Passend wäre z.B. die IP 192.168.1.10 mit der Subnetz-Maske 255.255.255.0

Computer LAN Interface Parameter	MC with firmware >= 2.15.1	MC with firmware <= 2.14y
IP	192.168.1.10	192.168.170.10
Gateway	192.168.1.254	192.168.170.254
Subnet mask	255.255.255.0	255.255.255.0

Wenn der MC mit der Defaulteinstellung (siehe -> 2.2) startet, kann man mit dem WEB-Browser mit Angabe der Adresse 192.168.1.1 eine Verbindung zum MC Gerät herstellen und sich die Home-Webseite des MC anzeigen lassen. Von da aus kann man die notwendigen Einstellungen vornehmen.

2.2 Zurücksetzen der Einstellungen auf Defaultwerte

Der MC kann durch Festhalten der Resettaste in den Auslieferungszustand zurückgesetzt werden. Wenn Sie die Resettaste drücken und gedrückt halten, durchläuft der MC Sequenzen, die durch wechselnde auf allen 4 LED's gleiche Farben angezeigt werden.

Startend mit weiß wechselt die Farbe auf blau --> rot --> grün und startet dann wieder von vorn mit weiß. Wenn das 3. mal blau erscheint und Sie weiter die Resettaste gedrückt halten, wird das Zurücksetzen der Einstellungen vorgenommen. Alle LED's werden dabei ausgeschaltet. **Danach** kann die Resettaste gelöst werden. Wenn vor der 3. „Blauphase“ die Resettaste gelöst wird, muss der MC durch eine erneute kurze Betätigung der Resettaste neu gestartet werden.

Der MC hat folgende (wichtige) Werkseinstellungen ab Firmware 2.15:

Device Name: „MC-Dev“
Global Security: **Best**
Wireless **OFF**
IP = **192.168.1.1**
Netmask = **255.255.255.0**

WLAN IP = 192.168.170.100
WLAN Netmask = 255.255.255.0
WLAN Gateway = 192.168.170.1

user = „ (leer)
password = „ (leer)

Seriell 1: inaktiv
Relais: inaktiv
Input: inaktiv

3 Webinterface Informationsseite

Nachdem Sie über den Webbrowser eine Verbindung mit dem http-Server des MC hergestellt haben, wird zunächst eine Seite mit Informationen zum MC und zum aktuellen Status des Geräts angezeigt. Diese Webseite kann angezeigt werden, ohne das die ggf. gesetzten Werte für „User“ + „Password“ abgefragt werden.

Bei allen anderen Seiten werden diese Angaben einmalig abgefragt, falls sie gesetzt wurden.

3.1 System Information

In diesem Abschnitt finden Sie allgemeine Informationen zum Gerät:

Info	Bedeutung	Anmerkung
Device Name	Name des Geräts	Diese Angabe wird unter → Admin konfiguriert und erscheint im MC-Config-Programm als Gerätename.
Uptime	Laufzeit	Dies ist die Zeit, die seit dem letzten Einschalten bzw. dem letzten Reset des MC vergangen ist
Realtime clock (UTC)	Datum- und Zeitangabe (Universal Time Coordinated)	Hier wird die interne Uhrzeit des Gerätes angezeigt. Beim Start setzt der MC die interne Uhr auf das Datum, an dem die Firmware kompiliert wurde mit der Uhrzeit 00:00:00. Wenn ein Zeitserver konfiguriert ist (Configuration -> Realtime Clock), versucht der MC diesen zu erreichen und die UTC-Information zu erhalten. Gelingt dies, stellt der MC die interne Uhr entsprechend. Diese Zeitangabe wird u.a. verwendet, um Debug-Ausgaben zu machen und um Zertifikate zu validieren.
Serial number	Seriennummer	
Firmware Version	Version der Firmware	
Kernel Version	Version des Kernels	Das Betriebssystem des MC basiert auf Linux. Die hier angegebene Versionsnummer gibt die Kernel-Version an, die aktuell in die Firmware eingebunden ist. Beachten Sie dazu bitte diesen Hinweis: --> 9

System Information

Device Name	MC-Dev
Uptime	0 Week(s) 0 Day(s) 00:01:23
Realtime clock (UTC)	17.10.2023 7:02:10
Realtime clock (Local Time)	17.10.2023 8:02:10
Serial number	326550
Firmware Version	2.14p
Kernel Version	Linux version 5.4.256

Tabelle 3: System Informationen

3.2 Wireless Status Information

In diesem Abschnitt finden Sie Informationen zum Status der WLAN Verbindung.

Operation Mode	Betriebsmodus	Der MC kann entweder als Client in einer WLAN Infrastruktur arbeiten (Infrastructure) oder im Adhoc Modus
AP Mac Address (BSSID)	AP MAC Adresse	Dies ist die MAC-Adresse des Access Points (AP) mit dem der MC verbunden ist. Wenn der AP auch einen Gerätenamen mitteilt, wird auch dieser hier angegeben.
SSID	Netzwerkname	Dies ist die Kennung des WLAN Netzwerks mit dem sich der MC verbinden soll bzw. verbunden hat.

Connection state	Verbindungsstatus	Status der Verbindung zum AP. Je nach dem welche Authentifizierung eingestellt ist, können verschiedene Meldungen angezeigt werden:	
		Idle	keine Verbindung vorhanden
		Disconnected	zuvor bestehende Verbindung wurde unterbrochen
		EAP Success	EAP Authentifizierung abgeschlossen
		KeyCompleted	Austausch der Schlüssel abgeschlossen
		Connected	verbunden
		Authenticate	Authentifizierung läuft
		Associate	Assoziierung läuft
		Associated	Assoziierung abgeschlossen
		EAP Started	EAP Authentifizierung läuft
		Timeout	Timeout im Authentifizierung Prozess
		EAP Failed	EAP Authentifizierung fehlgeschlagen
EAP Select Method	EAP Authentifizierung läuft		
Security	aktive Verschlüsselungs- und Authentifizierungsmethode	Verschlüsselung	Anzeige
		WEP	WEP-40 (104)
		WPA(2,3)	WPA(2,3)-PSK
		WPA(2,3)-Enterprise	WPA2(3)/IEEE 802.1X/EAP
Connection time	Verbindungszeit	Dies ist die Dauer der Verbindung zwischen dem MC und dem aktuellen AP	
Bitrate	Sendebitrate	Dies ist die aktuelle Bitrate mit der Daten zum AP gesendet werden.	
Channel / Frequency	Kanal-Nr. und Frequenz	Dies ist die Kanalnummer und die Frequenz auf der die Kommunikation zum aktuellen AP stattfindet.	
SNR	Signal - Geräusch - Verhältnis Dies ist eine Angabe über die Signalqualität und berechnet sich aus der Differenz von Signal- und Rauschpegel (siehe unten) Die Werte können wie folgt bewertet werden:		
	SNR	Zustand	
	>= 40	sehr guter Empfang	
	>= 30	guter Empfang	
	>= 20	Noch guter Empfang, je nach Einstellung (→ Roaming) beginnt der MC „bessere“ AP's durch Scannen der anderen Kanäle zu suchen.	
	>= 10	schwaches Signal: der MC verringert die Sendebaudrate und scannt andere Kanäle um „bessere“ AP's zu finden.	
	< 10	sehr schwaches Signal, der Datendurchsatz kann stark vermindert sein.	
Zusätzlich werden noch statistische SNR Werte angezeigt: Min xx dB Max yy dB, 24h: Min aa dB Max bb dB xx + yy = minimale und maximale SNR Werte bei der Verbindung mit dem aktuellen AP aa + bb = minimale und maximale SNR Werte innerhalb der letzten 24 Stunden			

Signal	Signalpegel	Der Signalwert liegt zwischen -30 bis -90 dBm
Noise	Rauschpegel	Normalerweise sind hier Werte zwischen -90 bis -95 dBm zu erwarten.
Channel Usage	Kanalauslastung	Die Funkkarte liefert einen Wert der die Auslastung des aktuellen Kanals in % angibt. Dieser Wert wird hier farbig angezeigt. Grün → geringe Auslastung Orange → mäßige Auslastung Rot → hohe Auslastung

Wireless Status Information

Operation Mode	Infrastructure
AP Mac Address (BSSID)	00:A0:57:22:41:4A (LANCOM_acn_2)
SSID	LANCOMacn
Connection state	Connected
Security	WPA2-PSK
Connection time	2m 39s
Bitrate	72MBit
Channel/Frequency	HT20 SGI 1 Stream MCS-Index 7
SNR	46dB (Min 40dB Max 48dB, 24h: Min 23dB Max 48dB)
Signal	-49 dBm
Noise	-95 dBm
Channel Usage 5GHz	5%

Tabelle 4: Wireless Status Information

3.3 Wired LAN Status Information

In diesem Abschnitt wird der aktuelle Zustand des bzw. der LAN-Ports angezeigt.

Wired LAN Status Information

LAN link state	Link: Up Speed: 100MBit/s Duplex: Full MDI-X: Cross
----------------	---

LAN link state	Zustand des LAN-Port	Link	down → es ist kein LAN-Kabel angeschlossen up → LAN-Kabel angeschlossen, Client-Gerät erkannt
		Speed	10, 100, 1000 MBit/s → Übertragungsgeschwindigkeit
		Duplex	Half, Full → Gleichzeitiges Senden und Empfangen an oder aus
		MDI-X	Straight, Cross → MDI-X Status

Tabelle 5: LAN Link Status Informationen

3.4 Relay Status Information

Diese Information wird nur angezeigt, wenn die Relais-Funktion aktiviert ist.

Relay Status Information

Relay Mode

TCP-Server listen on port 12345 Timeout: 5 sec

Current State

OFF

Info	Bedeutung	Anmerkung														
Relay mode	Relais-Modus	Informationen zum eingestellten Betriebsmodus des Relais-Schaltkontakts. <table border="1" data-bbox="624 479 1355 1055"> <thead> <tr> <th>Modus</th> <th>Funktion</th> </tr> </thead> <tbody> <tr> <td>Disabled</td> <td>Funktion nicht aktiv</td> </tr> <tr> <td>TCP (UDP)</td> <td>Die Relais-Funktion öffnet einen TCP (UDP) – Socket und wartet auf Daten, die das Relais steuern.</td> </tr> <tr> <td>Internal</td> <td>Das Relais wird über das Eingangssignal gesteuert.</td> </tr> <tr> <td>serial Trigger</td> <td>Das Relais schaltet ein, wenn Daten empfangen werden, die über die serielle Schnittstelle gesendet werden. Damit kann z.B. eine Aufwach-Funktion für das am MC angeschlossene Gerät realisiert werden. Das Relais fällt wieder ab wenn länger als „Timeout“ keine Daten über die serielle Schnittstelle gesendet werden.</td> </tr> <tr> <td>WLAN Status</td> <td>Das Relais schaltet ein, wenn eine WLAN-Verbindung vorhanden ist.</td> </tr> <tr> <td>MQTT Client</td> <td>Das Relais wird über MQTT gesteuert</td> </tr> </tbody> </table>	Modus	Funktion	Disabled	Funktion nicht aktiv	TCP (UDP)	Die Relais-Funktion öffnet einen TCP (UDP) – Socket und wartet auf Daten, die das Relais steuern.	Internal	Das Relais wird über das Eingangssignal gesteuert.	serial Trigger	Das Relais schaltet ein, wenn Daten empfangen werden, die über die serielle Schnittstelle gesendet werden. Damit kann z.B. eine Aufwach-Funktion für das am MC angeschlossene Gerät realisiert werden. Das Relais fällt wieder ab wenn länger als „Timeout“ keine Daten über die serielle Schnittstelle gesendet werden.	WLAN Status	Das Relais schaltet ein, wenn eine WLAN-Verbindung vorhanden ist.	MQTT Client	Das Relais wird über MQTT gesteuert
Modus	Funktion															
Disabled	Funktion nicht aktiv															
TCP (UDP)	Die Relais-Funktion öffnet einen TCP (UDP) – Socket und wartet auf Daten, die das Relais steuern.															
Internal	Das Relais wird über das Eingangssignal gesteuert.															
serial Trigger	Das Relais schaltet ein, wenn Daten empfangen werden, die über die serielle Schnittstelle gesendet werden. Damit kann z.B. eine Aufwach-Funktion für das am MC angeschlossene Gerät realisiert werden. Das Relais fällt wieder ab wenn länger als „Timeout“ keine Daten über die serielle Schnittstelle gesendet werden.															
WLAN Status	Das Relais schaltet ein, wenn eine WLAN-Verbindung vorhanden ist.															
MQTT Client	Das Relais wird über MQTT gesteuert															
Current State	aktueller Zustand des Relais															

Tabelle 6: Relaisstatus

3.5 Input Status Information

Diese Information wird nur angezeigt, wenn die Input-Funktion aktiviert ist.

Input Status Information

Input State

OFF

3.6 Serial 1

In diesem Abschnitt wird der aktuelle Zustand des seriellen Ports angezeigt.

Serial 1

```

State                               Serial Port is active
Device                               /dev/ttyMC0
Network Connection                   Mode: 'TCP-Server' IP: 192.168.170.132:59879 (Established)
Baudrate - Parity - Databits         115200 - None - 8
Serial Tx Frames/Bytes                3122/48642
Serial Rx Frames/Bytes                30412/49441
Network Tx Frames/Bytes               421/49441
Network Rx Frames/Bytes               98/48804
Net->Uart: Bytes in Buffer            162
Uart->Net: Bytes in Buffer             126
    
```

Info	Bedeutung	Anmerkung
State	Status	Hier wird angezeigt, ob der serielle Port aktiviert ist
Device	Devicename	Diese Angabe bezeichnet die Hardwareeinheit mit der die serielle Schnittstelle realisiert ist. Standard ist die Bezeichnung: /dev/ttymx0 Wenn am USB-Port ein passender USB <--> Seriell Adapter angeschlossen ist, sind auch Angaben wie: /dev/ttyUSB0 (1,...) möglich
Network Connection	Modus und Zustand	Hier wird angezeigt, in welchem Modus der serielle Port arbeitet und in welchem Zustand sich die Verbindung aktuell befindet. z.B. Mode: 'TCP-Server' IP: 0.0.0.0 (Listen Port 8888)
Baudrate Parity Databits	Parameter der seriellen Verbindung	Mit diesen Werten wird angezeigt, wie die serielle Schnittstelle aktuell eingestellt ist.
Serial Tx Frames/Bytes Serial Rx Frames/Bytes Network Tx Frames/Bytes Network Rx Frames/Bytes Net->Uart: Bytes in Buffer Uart->Net: Bytes in Buffer	Statistische Werte	Diese hier angezeigten Werte zeigen, wie viele Bytes bzw. Datenpakete über die serielle Schnittstelle gesendet bzw. empfangen wurden.

Tabelle 7: Status der seriellen Schnittstelle

3.7 Traffic Usage Information

In diesem Abschnitt werden statistische Angaben über die Datenmenge gemacht, die in der letzten Minute bzw. in der letzten Stunde über die WLAN- und die LAN-Schnittstelle ausgetauscht wurden.

Traffic Usage Information	
	Time periods for usage are based on runtime:
Traffic usage for LAN	Last Minute: 332 KByte Last Hour: 8 MByte
Traffic usage for Wireless	Last Minute: 94 KByte Last Hour: 7437 KByte

3.8 Network Information

Dieser Abschnitt zeigt abhängig vom konfigurierten Bridge-Modus Informationen zu den aktiven Netzwerk-Schnittstellen an.

Bridge - Type	Angezeigten Informationen (abhängig von der Konfiguration des MC und der angeschlossenen LAN-Clients)																						
LAN Client Cloning	<table border="1"> <thead> <tr> <th>Bridge</th> <th></th> </tr> </thead> <tbody> <tr> <td>Bridge Type</td> <td>LAN Client Cloning</td> </tr> <tr> <td>Client Detection</td> <td>Detected Client information by DHCP</td> </tr> <tr> <td>Client IP</td> <td>192.168.170.63 (Autodetected)</td> </tr> <tr> <td>Client Netmask</td> <td>255.255.255.0 (Autodetected)</td> </tr> <tr> <td>Client Gateway</td> <td>192.168.170.249 (Autodetected)</td> </tr> <tr> <td>Client DNS</td> <td>8.8.8.8 (Autodetected)</td> </tr> <tr> <td>Client Hostname</td> <td>LAPTOP-BLROHENO (From DHCP Request)</td> </tr> <tr> <td>Client MAC</td> <td>54:E1:AD:B4:DB:81 (Autodetected)</td> </tr> <tr> <td>Original WLAN Card MAC</td> <td>00:0E:8E:B4:F5:22</td> </tr> <tr> <td>LAN MAC</td> <td>90:5F:8D:04:FB:96</td> </tr> </tbody> </table>	Bridge		Bridge Type	LAN Client Cloning	Client Detection	Detected Client information by DHCP	Client IP	192.168.170.63 (Autodetected)	Client Netmask	255.255.255.0 (Autodetected)	Client Gateway	192.168.170.249 (Autodetected)	Client DNS	8.8.8.8 (Autodetected)	Client Hostname	LAPTOP-BLROHENO (From DHCP Request)	Client MAC	54:E1:AD:B4:DB:81 (Autodetected)	Original WLAN Card MAC	00:0E:8E:B4:F5:22	LAN MAC	90:5F:8D:04:FB:96
Bridge																							
Bridge Type	LAN Client Cloning																						
Client Detection	Detected Client information by DHCP																						
Client IP	192.168.170.63 (Autodetected)																						
Client Netmask	255.255.255.0 (Autodetected)																						
Client Gateway	192.168.170.249 (Autodetected)																						
Client DNS	8.8.8.8 (Autodetected)																						
Client Hostname	LAPTOP-BLROHENO (From DHCP Request)																						
Client MAC	54:E1:AD:B4:DB:81 (Autodetected)																						
Original WLAN Card MAC	00:0E:8E:B4:F5:22																						
LAN MAC	90:5F:8D:04:FB:96																						

Bridge - Type	Angezeigten Informationen (abhängig von der Konfiguration des MC und der angeschlossenen LAN-Clients)
NAT oder Single Client NAT	<p>Network Information</p> <p>Interface Wireless (IPv4) IP 192.168.170.79 (DHCP successful) Broadcast 192.168.170.255 Netmask 255.255.255.0 MAC 00:0E:8E:B4:F5:22 default gw 192.168.170.249</p> <p>Interface LAN (IPv4) IP 192.168.2.100 (Static IP) Broadcast 192.168.2.255 Netmask 255.255.255.0 MAC 90:5F:8D:04:FB:96</p> <p>Interface lo (IPv4) IP 127.0.0.1 Broadcast 127.0.0.1 Netmask 255.0.0.0</p> <p>Routing Default gateway 192.168.170.249 on Wireless</p> <p>Bridge</p> <p>Bridge Type Nat</p> <p>DHCP Server Status (LAN)</p> <p>Dynamic IP Range 192.168.2.10 - 192.168.2.20</p> <p>Active clients</p> <p>DHCP Client 1 54:E1:AD:B4:DB:81 192.168.2.10 (LAPTOP-BLROHENO)</p>
Level 2 Pseudo-Bridge	<p>Network Information</p> <p>Interface Wireless IP 192.168.170.72 (DHCP successful) Broadcast 192.168.170.255 Netmask 255.255.255.0 MAC 00:0E:8E:BE:5F:A6 default gw 192.168.170.249 Captive portal: http://192.168.170.249/</p> <p>Interface LAN+ IP 1.1.1.1 Broadcast 1.255.255.255 Netmask 255.255.255.255 MAC 90:5F:8D:05:DA:44</p> <p>Interface LAN IP 192.168.170.72 Broadcast 192.168.170.255 Netmask 255.255.255.255 MAC 90:5F:8D:05:DA:44</p> <p>Interface lo IP 127.0.0.1 Broadcast 127.0.0.1 Netmask 255.0.0.0</p> <p>Routing Default gateway 192.168.170.249 on Wireless</p> <p>Bridge</p> <p>Bridge Type Level 2 Bridge</p> <p>Level 2 Bridge Status</p> <p>Bridge Entry 1 LAN1: 54:E1:AD:B4:DB:81 192.168.170.97 (8sec)</p>

Tabelle 8: Network Information

3.9 Access Point Information

In diesem Abschnitt wird eine Liste der vom MC registrierten Access Points (AP) angezeigt. Der Listeneintrag des aktuell verbundenen AP's ist grau hinterlegt und wird immer an erster Stelle angezeigt. Es folgen die AP's mit passender SSID die potentiell auch für eine Verbindung in Frage kommen. Diese AP's werden mit grüner Schrift dargestellt. Danach werden AP's mit anderer oder unbekannter SSID (hidden) aufgelistet. Die Informationen unter „Security“ geben Auskunft über die Authentifizierungsmethoden, die der jeweilige AP erwartet.

Wenn ein AP die zum MC passende SSID anbietet, aber die „Security“-Einstellungen des AP's verhindern, dass sich der MC mit dem AP verbinden kann, wird die „Security“-Information in **roter** Schrift angezeigt.

Das gleiche gibt für die Spalte „Channel/Frequency“, wenn der AP auf einem Kanal arbeitet, der z.B. durch eine Angabe einer Kanalliste unter Configuration->Wireless->Roaming nicht eingeschlossen ist.

In der Spalte „Extra Information“ wird folgendes angegeben:

- Ländereinstellung (DE)
- Anzahl der Clients / Kanalauslastung (5/2%) (Wenn verfügbar)
- Sendeleistungseinschränkung (17dBm) (Wenn verfügbar)
- 802.11k Info mit der Anzahl der angegebenen Nachbar-AP's (802.11k (1)) (Wenn verfügbar)
- Roamingvorgänge (a / b) a= misslungen b= erfolgreich
- Rauschpegel (-95dBm). Dieser Wert + SNR ergibt den gemessenen Signalpegel. (-95 + 48 = -47dBm)

WLAN Access point list								
BSSID	SSID	Security	SNR	AP Name	Channel/Frequency	Min/Max Bitrate	Last Seen	Extra Information
00:A0:57:22:41:4A	LANCOMacn	[WPA2-PSK-CCMP]	52dB	LANCOM_acn_2	40: 5200MHz	6 / 54 + 11n: BW 20MHz	0	DE 3/6% 11v 802.11k (1) Roam 0/2 -95dBm
00:A0:57:22:41:2A	LANCOMacn	[WPA2-PSK-CCMP]	22dB	LANCOM_acn_1	44: 5220MHz	6 / 54 + 11n: BW 40MHz	3	DE 2/17% 11v 802.11k (1) Roam 0/1 -94dBm
0E:A0:57:22:41:4A	LANCOM_WPA3as	[WPA2-PSK-SHA256-CCMP]	54dB	LANCOM_acn_2	40: 5200MHz	6 / 54 + 11n: BW 20MHz	3	DE 0/6% 11v -95dBm
68:86:A7:13:81:1A	RadiusTest_FT	[WPA2-FT-EAP-CCMP]	31dB	CAP-3502E-H	56: 5280MHz	12 / 54 + 11n: BW 40MHz	68	DE 18/6% 17dBm -94dBm

Abbildung 3.1: Access Point Liste

Neighbor (11sec):
Ch44
Last Seen Extra 00:A0:57:22:41:2A
0 DE 4/2% 802.11k (1) Roam 0/2 -95dBm

Zur Spalte "Extra Information" werden noch zusätzlich Informationen einblendet, wenn man den Cursor über die einzelnen Angaben platziert. So kann man sich z.B. zusätzlich die Liste der Nachbar-AP's anzeigen lassen.

3.10 HTTPS Webinterface

Auf die Webseiten der MC-Geräte kann man auch per HTTPS (Hypertext Transfer Protocol Secure) zugreifen. Damit wird ein verschlüsselter Datenaustausch zwischen MC und Webbrowser ermöglicht. Dazu wird unter „Admin“ der HTTPS-Server auf einem konfigurierbaren TCP-Port (default 443) aktiviert. Für diesen Zugriff verwendet der MC ein selbsterzeugtes Serverzertifikat, das bei der ersten Verbindung im Webbrowser bestätigt werden muss. Die Meldung des Browsers zur Bestätigung ist je nach Browsertyp unterschiedlich.

Firefox	Opera	MS Edge
<p>Zurück (empfohlen) Erweitert...</p> <p>192.168.1.1 verwendet ein ungültiges Sicherheitszertifikat. Dem Zertifikat wird nicht vertraut, weil es vom Aussteller selbst signiert wurde. Fehlercode: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT</p> <p>Zertifikat anzeigen</p> <p>Zurück (empfohlen) Risiko akzeptieren und fortfahren</p>	<p>NET-ERR_CERT_AUTHORITY_INVALID</p> <p>Help me understand</p> <p>Dieser Server konnte nicht beweisen, dass er 192.168.1.1 ist. Sein Sicherheitszertifikat wird vom Betriebssystem Ihres Computers als nicht vertrauenswürdig eingestuft. Mögliche Gründe sind eine fehlerhafte Konfiguration oder ein Angreifer, der deine Verbindung abfängt.</p> <p>Weiter zu 192.168.1.1 (unsicher)</p>	<p>NET-ERR_CERT_AUTHORITY_INVALID</p> <p>Erweitert ausblenden Zurück</p> <p>Dieser Server konnte nicht nachweisen, dass es sich bei ihm um 192.168.1.1 handelt. Das Sicherheitszertifikat wird vom Betriebssystem Ihres Computers nicht als vertrauenswürdig eingestuft. Dies kann auf eine Fehikonfiguration zurückzuführen sein oder auf einen Angreifer, der Ihre Verbindung abfängt.</p> <p>Weiter zu 192.168.1.1 (unsicher)</p>

Die Links in den rot markierten Bereichen führen dazu, dass der Browser das Zertifikat akzeptiert und die Verbindung zum HTTPS-Webserver des MC aufbaut.

- Um diesen Ablauf zu vermeiden, kann auch ein eigenes registriertes Serverzertifikat auf den MC geladen werden. Dies geschieht in dem Abschnitt „Admin“ → 5.1.8.4(Webserver certificate)

3.11 Storage Status Information

An den MC kann ein USB-Speicher-Stick angeschlossen werden, der zur Speicherung von Debug-Meldungen oder von Mitschnitten auf der WLAN - oder LAN Schnittstelle genutzt werden kann.

Wenn ein solcher USB-Speicher-Stick aufgesteckt ist, wird der Status dieses Speichers am Ende der Home-Webseite angezeigt.

Storage Status Information	
USB	Mounted on /mnt/usb Unmount
Filesystem	vfat Format as Ext4 Filesystem
Free	29540MiB from 29586MiB

Abbildung 3.2: USB-Speicherstatus

Vor dem Abziehen des Speicher-Sticks sollte der Anwender mit der Funktion „Unmount“ den Speicher vom System trennen, damit der Inhalt konsistent bleibt. Insbesondere wenn der USB-Stick als FAT-Filesystem formatiert ist, kann es dazu kommen, dass beim Ausschalten ohne vorheriges „Unmounten“ Fehler im Filesystem des USB-Stick entstehen.

Wenn der USB-Stick dazu dient Debug-Meldungen und (oder) (W)LAN Mitschnitte aufzuzeichnen (siehe 5.11), sollte der USB-Stick mit dem EXT4-Filesystem formatiert werden. Dieses Filesystem ist robuster in Bezug auf die Konsistenz der Daten bei plötzlichen Ein- und Ausschalten des MC.

Darum wird an dieser Stelle die Funktion „Format as EXT4 Filesystem“ angeboten. Damit wird der aktuell aufgesteckte USB-Stick mit dem EXT4-Format formatiert. **Dabei werden allerdings alle vorhandenen Dateien auf dem USB-Stick gelöscht.**

3.12 WLAN und LAN-Dump-Dateien

Wenn der Mitschnitt der Kommunikation auf der WLAN oder (und) LAN-Schnittstelle aktiviert ist (siehe „Configuration“ → „Logging“ → „(W)LAN Dump“), werden hier die dabei entstandenen Dateien gelistet. Die Dateien enthalten die aufgezeichneten Daten in komprimierter Form vom Typ „.gz“

Lediglich die Dateien, die gerade beschrieben werden, sind vom Type „.pcap“

Weitere Informationen dazu finden Sie hier → 5.11.1.4

Wireless Dump	
Capture byte count	2666376KByte
Recv count	16462248
Drop count	24634/12616 (If 0)
Recent Dumpfiles	391002_WLANDump_0140_20000101_073944_843916.pcap.gz (21687 KByte)
Recent Dumpfiles	391002_WLANDump_0141_20000101_074048_360020.pcap.gz (18244 KByte)
Recent Dumpfiles	391002_WLANDump_0142_20000101_074233_462674.pcap.gz (21912 KByte)
Recent Dumpfiles	391002_WLANDump_0143_20000101_074310_600030.pcap.gz (16050 KByte)
Recent Dumpfiles	391002_WLANDump_0144_20000101_074604_862172.pcap.gz (19922 KByte)
Recent Dumpfiles	391002_WLANDump_0145_20000101_074731_698195.pcap.gz (19984 KByte)
Recent Dumpfiles	391002_WLANDump_0146_20000101_074851_473225.pcap (26937 KByte)
Ethernet Dump	
Capture byte count	89640KByte
Recv count	79175
Drop count	0/0 (If 0)
Recent Dumpfiles	391002_EthernetDump_0000_20000101_074003_654321.pcap.gz (16143 KByte)
Recent Dumpfiles	391002_EthernetDump_0001_20000101_074251_645069.pcap.gz (16549 KByte)
Recent Dumpfiles	391002_EthernetDump_0002_20000101_074643_559405.pcap (23742 KByte)

Abbildung 3.3: WLAN- und LAN-Dump-Dateien

4 Firmware- und Konfigurationsmanagement: Device Menü

Unter diesem Menüpunkt gibt es die Möglichkeit eine Firmware auf den MC zu übertragen und die eingestellten Parameter als Datei zu speichern oder wieder herzustellen.

4.1 Firmware

Hier kann über einen einfachen Dialog eine Datei ausgewählt und mit „Upload“ zum MC übertragen werden.

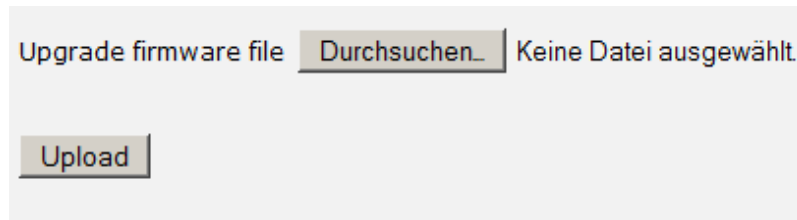


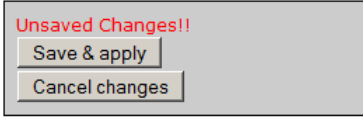
Abbildung 4.1: Firmware Upgrade Dialog



Es ist sehr wichtig, dass in dieser Phase weder die Versorgungsspannung des MC unterbrochen noch die Resettaste betätigt wird.

4.2 Configuration Management

unter diesem Menüpunkt hat man folgende Möglichkeiten:

Reset configuration to defaults	Mit diesem Taster werden alle Parameter auf den Auslieferungszustand zurückgesetzt. Daraufhin wird auf der Webseite oben rechts ein Feld mit 2 Tasten eingeblendet, mit denen der geänderte Zustand gespeichert und aktiviert werden kann („Save & apply“) oder die gemachten Veränderungen wieder auf den Ausgangszustand zurückgesetzt werden („Cancel changes“). 
Download running configuration	Mit dieser Funktion kann der aktive Parametersatz in einer Datei abgespeichert werden.
Download new configuration	Mit dieser Funktion kann der aktive Parametersatz abgespeichert werden. Es werden auch die evt. schon zuvor vorgenommenen Änderungen in die Datei mit übernommen.
Reboot device	Mit dieser Funktion kann der MC neu gestartet werden. Nicht gespeicherte Änderungen gehen verloren.
Upload configuration file	Hiermit kann eine Parameterdatei ausgewählt und mit „Upload“ auf den MC übertragen werden. Wenn sich dadurch Parameter ändern, wird oben rechts wieder der Dialog zur Übernahme und Aktivierung (Save & apply) der Parameter angezeigt. Man kann aber auch das Laden der Datei mit „Cancel changes“ wieder rückgängig machen.

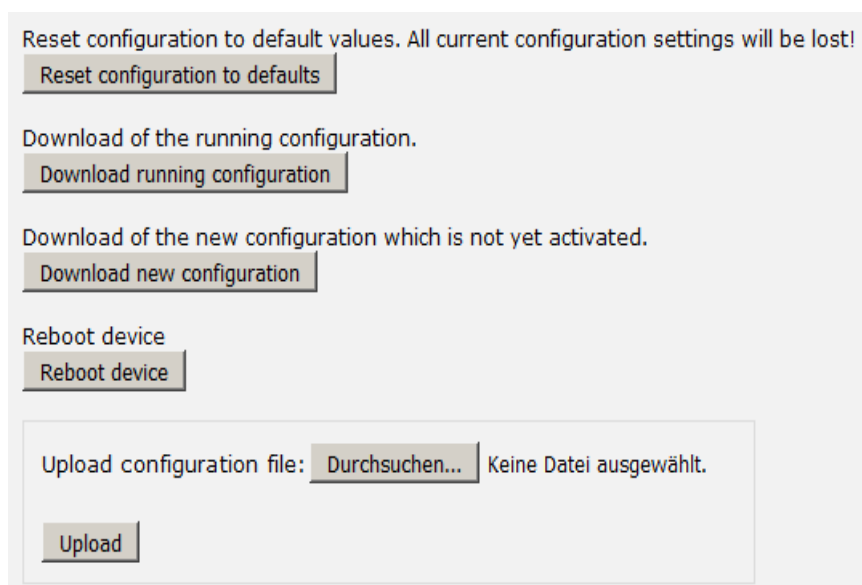


Abbildung 4.2: Configuration Management

4.3 Network Test

(ab Firmware 2.14b)

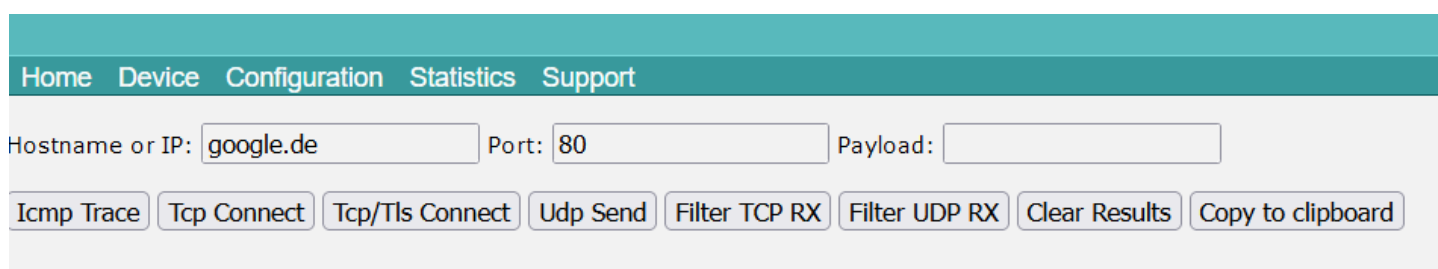
Auf dieser Seite kann man Netzwerkverbindungen zu bestimmten Hosts testen.

Damit lassen z.B. die Parameter für die Einrichtung der Netzwerkschnittstellen testen.

Hier lässt sich auch prüfen, ob bestimmte Ports (TCP oder UDP) auf bestimmten IP-Adressen über das WLAN erreichbar sind.

Folgende Funktionen stehen zur Verfügung:

Funktion	Beschreibung
Icmp Trace	Ping-Test zu einer IP oder einem Hostnamen. Die einzelnen Stationen, die zur Zieladresse führen, werden gelistet.
Tcp Connect	Damit kann eine TCP-Verbindung zu einem Host auf den angegebenen Port aufgebaut werden. Die Verbindung wird im Anschluss gleich wieder geschlossen.
Tcp/Tls Connect	Damit kann eine TCP/TLS-Verbindung zu einem Host auf den angegebenen Port aufgebaut werden. Wenn die Verbindung erfolgreich ist, werden Daten aus dem empfangenen CA-Zertifikat des Servers angezeigt.
Udp Send	Mit dieser Funktion kann ein Datagramm an den angegebenen Host auf den angegebenen Port mit dem Inhalt „Payload“ geschickt werden.
Filter TCP RX	Mit dieser Funktion wird auf dem angegebenen Port überwacht, ob eine TCP-Verbindung über WLAN zu diesem Port aufgebaut wird. Es wird nur der Aufbau der Verbindung gemeldet.
Filter UDP RX	Mit dieser Funktion wird auf dem angegebenen Port überwacht, ob UDP-Daten über WLAN zu diesem Port geschickt werden. Wenn das erste UDP-Paket eintrifft, werden Informationen zum Absender ausgegeben. Es wird nur das erste UDP-Paket von einem Host mit einer bestimmten Quell+Ziel-Port Kombination registriert. Mit „Clear Results“ und anschließendem „Filter UDP RX“ wird der Filter neu gestartet.
Clear Results	Damit werden die Ausgaben gelöscht und die Filter (TCP(UDP) RX zurückgesetzt.



Home Device Configuration Statistics Support

Hostname or IP: Port: Payload:

Abbildung 4.3: Network Test

5 Einstellung der Betriebsparameter: Configuration Menü

Unter diesem Menüpunkt finden sich weitere Untermenüs, über die man Webseiten erreicht, auf denen alle Parameter des MC definiert werden können.

Welche Untermenüpunkte vorhanden sind, ist abhängig von der jeweiligen Variante des MC.

Die folgende Tabelle nennt die zur Zeit vorhandenen Untermenüs.

Menüpunkt	Kapitel	wichtige Parameter	Voraussetzung
Admin	5.1	Gerätename, User, Password	
Security	5.2		
Certificate	5.3		
Network	5.4	IP-Adresse, Bridge-Mode, Filter	
Wireless	5.5	SSID, Security, SCEP, Roaming	
Serial Ports	5.6	Baudrate, Modus usw	Serielle Schnittstelle
Printer Server	5.7	USB-Printer Mode	USB-Port
Relay	5.8	Relay-Mode	Relais Anschluss
Realtime clock	5.9	NTP-Server-IP (Zeitserver)	
Input	5.10	Input-Mode	AUX-In
LAN Port		Auto negotiation (ein / aus)	MC1 oder MC6C
Logging	5.11	Debug-Meldungen ein / aus	

Die einzelnen Webseiten zur Konfiguration werden im folgenden genauer dargestellt und erläutert.

5.1 Admin

Unter Admin werden verschiedene Parameter definiert, die u.a. den Zugriff auf die Webseite und damit auf Statusinformationen und die Konfiguration des MC steuert.

5.1.1 Device Name		
	Device Name	Dieser Name wird mit dem MC-Config-Programm angezeigt und kann auch beim DHCP als Gerätename an den DHCP-Server geschickt werden.
	Lookup Host	Mit dieser Option kann der Hostname vom Nameserver abgefragt werden. Die ggf. empfangene Information wird dann im MConfig in der Spalte „Name“ zusätzlich angezeigt.
5.1.2 Security		
	Administrator Login	Den Zugriff auf die Konfiguration des MC kann man hier durch Eingabe eines Benutzernamens und eines dazu gehörenden Passworts schützen. Das Passwort sollte mindestens 8 Zeichen lang sein, Buchstaben, Zahlen und Sonderzeichen enthalten.
	Monitor Login	Für jemanden, der die Konfiguration nur einsehen, aber nicht ändern soll, kann man als 'Monitor' einen Benutzer festlegen, der die Konfiguration öffnen aber keine Änderungen an den Parametern vornehmen kann.

5.1.3 SNMP

Das Simple Network Management Protocol (SNMP) ist ein Netzwerkprotokoll zur Überwachung und Steuerung von Netzwerkgeräten von einer zentralen Station aus. Die MIB-Datei, die eine Gerätebeschreibung enthält, kann über einen Link vom MC heruntergeladen werden.

SNMP

Enable SNMP

Check this box to enable SNMP server.
Download MIB [here](#)

Ab der Firmware 2.14p werden die SNMP Versionen V1/2/3 unterstützt

Die SNMP-Funktion im MC erlaubt nur Parameter und Werte abzufragen und nicht Parameter zu verändern (read only).

Enable SNMP	SNMP Zugang einschalten
Community name	Der SNMP-Community-Name ist ein einfaches Passwort, das SNMP zur Zugriffskontrolle auf Geräte verwendet wird. Per Default wird dieser Name auf „public“ gesetzt.
Username / Password	Username - Passwort zur Authentifizierung für SNMPv3
Authentication	Angabe des Protokolls zur Authentifizierung
Encryption	Angabe des Encryption Types für die Verschlüsselung der Dateninhalte
SNMP Version	Hier werden die zugelassenen SNMP Versionen definiert
Debug SNMP	Wenn es zu Problemen bei der Nutzung diese Funktion kommt, kann man hier verschiedene Debuglevel angeben, mit dem Ereignisse im SNMP-Modul in die Log-Datei geschrieben werden.

5.1.4 Webserver

Der Webserver des MC kann über HTTP oder HTTPS angesprochen werden. An dieser Stelle kann man die beiden Protokolle (de)aktivieren und jeweils die Portnummern für diese Protokolle festlegen. Die Einstellung der Portnummern kann wichtig sein, wenn man im NAT-Modus arbeitet und LAN-Clients ebenfalls auf diesen Ports erreichbar sein sollen. Für die HTTPS Funktion kann am Ende dieser Seite ein kundenspezifisches Zertifikat für den Webserver hochgeladen werden.

Enable Unencrypted (HTTP)	Die Option erlaubt den Zugriff auf den Webserver per ungesicherten HTTP.
Webserver Port	Hier wird der Port für den Zugriff per HTTP definiert. Der Defaultwert für diesen Port ist 80. Im LAN-Client-Cloning oder im NAT-Modus kann man durch die Änderung dieses Werts erreichen, dass LAN-Client-Geräte über diesen Port erreichbar sind.
Enable Secure (HTTPS)	Die Option erlaubt den Zugriff auf den Webserver per gesicherten HTTPS.
Secure Webserver Port	Hier wird der Port für den Zugriff per HTTPS definiert. Der Defaultwert für diesen Port ist 443. Hier gilt das gleiche wie für den Webserver Port 80.
HTTPS Security	Mit dieser Auswahl kann man bestimmte Anforderungen für den Webserver des MC festlegen.
Security definitions	Wenn die Option „HTTPS Security“ nicht auf „Default“ gestellt wurde, wird hier die Vorgabe definiert. Wie im Helptext angegeben werden die Vorgaben entsprechend den gnuTLS-Strings festgelegt. https://gnutls.org/manual/html_node/Priority-Strings.html
Send HSTS Header	Dadurch wird der Browser angewiesen, Website-Inhalte für einen bestimmten Zeitraum nur über eine sichere Verbindung (HTTPS) zu laden.
Show website state	Normalerweise wird die Homepage mit den Statusinformationen der MC-Geräte ohne die Abfrage von „user“ und „password“ angezeigt. Wenn auch dies eingeschränkt werden soll, kann man mit der Auswahl „need authentication even for status“ die Eingabe notwendig machen. Hier kann man einstellen, dass auch die Status-Webseite des MC nur eingesehen werden kann, wenn man user + password Angaben macht.

API Authentication	Hier kann man die Art der Authentifizierung für die API Schnittstelle es MC festlegen 1) Basic Authentification 2) Gigest Authentification (MD5) 3) Gigest Authentification (SHA 256)
Webserver on Interface	Hier wird festgelegt, auf welchen Schnittstellen, der MC-Webserver arbeitet. 1) All Interfaces 2) Only LAN (Zugriff nur über den LAN-Port)

5.1.5 URL Authentication

<p>Der Zugriff auf die REST-API ist normalerweise entsprechend der Angabe von Admin user/password oder Read-Only user/password geregelt. Wenn Anwendungen über die API auf bestimmte Informationen zugreifen sollen man aber nicht die allgemeinen Zugriffspasswörter dazu herausgeben möchte, kann man hier für bestimmte URL's separate Zugriffsregeln definieren.</p> <p>Wenn man z.B. den Status der WLAN-Verbindung ohne user/password abfragen möchte, dann geht das wie folgt.</p> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>URL Authentication</p> <p>By default, API/URL authentication is performed by the Admin user or Read-only user. The following settings allow configuration for individual URL authentication. URL settings can use the wildcard * like '/API/Status/Wireless/*'.</p> <p>Auth Count <input type="text" value="1"/> Change count of following authentication rules.</p> <p>Authentication Mode <input type="text" value="Allow unauthenticated access"/> Authentication Mode</p> <p>URL <input type="text" value="/API/Status/Wireless/Connection"/></p> </div>

Auth Count	Anzahl der gewünschten Regeln.
Authentication Mode	Folgende Auswahlmöglichkeiten gibt es: <ul style="list-style-type: none"> - Ausgeschaltet - Zugriff ohne user/password - Lesezugriff mit user + password - Schreib+Lesezugriff mit user + password
URL	Hier wird die URL angegeben, auf die zugegriffen werden soll.
Username	Username mit dem ein Zugriff auf diese URL erlaubt ist
Password	Das Passwort zum Zugriff auf diese URL

5.1.6 Configuration tool accessibility

	In diesem Abschnitt wird festgelegt, wie mit dem MConfig-Programm auf das MC-Gerät zugegriffen werden kann.	
MC-Config Interface	Mit dieser Einstellung kann der Zugriff mit dem MConfig-Tool auf den MC eingeschränkt werden. <ul style="list-style-type: none"> - WLAN+LAN - LAN - none 	
Enable TLS	Damit die Daten die mit dem MConfig-Programm vom MC heruntergeladen werden auch verschlüsselt werden, kann diese Option eingeschaltet werden.	
UDP Encryption	Wenn die Kommunikation verschlüsselt werden soll, dann wählen Sie:	
	Use ECDH + AES-256-CBC	Die Verschlüsselung wird aktiviert, wenn das verwendete MConfig-Tool dies unterstützt
	Force ECDH + AES-256-CBC	Die Verschlüsselung wird aktiviert. Das MConfig-Tool muss diese Verschlüsselung unterstützen. Dazu muss eine aktuelle Version des MConfig-Tools (>= 2.0.3.17) verwendet werden.

5.1.7 Auto Firmware Upgrade

Wichtiger Hinweis:

Durch Aktivieren der automatischen Firmware-Update-Funktion kontaktiert das Gerät regelmäßig einen konfigurierten Server und installiert Firmware-Updates ohne weitere Bestätigung durch den Benutzer. Bitte beachten Sie, dass jede über diesen Mechanismus installierte Firmware – unabhängig von ihrer Quelle – zu einem nicht funktionsfähigen System führen kann.

Der Hersteller kann nicht für Fehlfunktionen, Ausfälle oder Schäden haftbar gemacht werden, die durch automatische Updates entstehen. Es liegt in der alleinigen Verantwortung des Benutzers, vor der Bereitstellung zu überprüfen, ob die bereitgestellte Firmware korrekt und kompatibel ist und ordnungsgemäß getestet wurde.

Das Risiko, dass das Gerät funktionsunfähig wird, liegt vollständig beim Anwender.

5.1.7.1 Funktion

Prinzipiell funktioniert die automatisierte Firmwareverteilung mit einem vom Anwender bereitgestellten Webserver. Dieser Webserver empfängt von den MC-Geräten Anfragen, die folgende Informationen enthalten:

FW	aktuelle Firmwareversion des MC
Ser	Seriennummer
Branding	Im Gerät gesetzter Wert
Branch	angefragter Branch (einstellbarer Parameter)

So sieht beispielsweise ein Aufruf eines MC-Geräts beim Webserver aus:

```
https://autoupdate.example.com/check.php?FW=3.14y&Ser=123456&Branding=MyBrand&Branch=Latest
```

Der Server antwortet im INI-Format mit einer Sektion passend zum Branch:

```
[Latest]
SHA512=abcdef1234567890... (64 Bytes als Hex oder Binärwert)
URL=https://firmware-cdn.example.com/firmware/FW_3.15.1.upg.bin
```

Hinweis: Die URL zur Firmwaredatei kann sich auf einem anderen Server befinden als die Steuerungs-URL (also check.php). Das Gerät greift nach Erhalt der Antwort auf die angegebene URL zu.

Falls kein Update erfolgen soll, kann entweder:

```
[Latest]
NoUpdate=1
```

oder einfach eine identische SHA512-Hash + URL Antwort gesendet werden.

5.1.7.2 Voraussetzungen

- In der MC-Gerätekonfiguration müssen die erforderlichen CA-Zertifikate hinterlegt sein, damit TLS-Verbindungen geprüft und akzeptiert werden können.
- Ein Webserver (z. B. Apache, nginx) mit HTTPS-Unterstützung (TLS 1.3)
- Gültiges TLS-Zertifikat (z. B. Let's Encrypt)
- PHP-Unterstützung für einfache Antwortlogik (optional)
- Zugriff auf die aktuelle Firmwaredatei und deren SHA512-Hash

5.1.7.3 Aufbau der Antwortdatei

- Die Antwortdatei vom Webserver hat das INI-Format
- Sektion: muss dem Branch entsprechen (z. B. [Latest], [Stable])
- URL: Direktlink zur Firmwaredatei (HTTPS erforderlich)
- SHA512: Der exakte SHA512-Hashwert der Datei
- Optional: NoUpdate=1 unterdrückt das Update explizit
- Optional: [Control] Sleep=60 setzt ein Pausenintervall (Minuten) bis zum nächsten Versuch

5.1.7.4 **Bereitstellung der Firmwaredatei**

- Die Datei muss über HTTPS erreichbar sein
- Die Domain muss zum Zertifikat passen
- Die Domain kann von der Steuerungs-URL abweichen (z. B. CDN)
- MIME-Type kann application/octet-stream sein

5.1.7.5 **Sicherheitshinweise**

- Der Server muss ein gültiges Zertifikat besitzen, das vom Gerät akzeptiert wird (z. B. Let's Encrypt mit Zwischenzertifikat)
- Nur signierte Firmwaredateien werden vom Gerät akzeptiert
- Bei Fehlern erfolgt Logging am Gerät

5.1.7.6 **Parameter**

Mode	Hier wird festgelegt, mit welchem Intervall der MC beim Upgrade-Server nach einer neuen Firmware fragt. <ul style="list-style-type: none">• Disabled• Check every minute• Check every hour• Check every day
Branch	Der hier eingestellte Wert wird per HTTP – Request an den Webserver mitgeteilt
URL	Adresse des Update-Servers z.B.: https://autoupdate.example.com/check.php

5.1.8 **Other Options**

5.1.8.1 **Serial port instances**

Die Anzahl der seriellen Ports kann durch den Anschluss passender Adapter an den MC-USB-Port erweitert werden. Hier kann man festlegen, wie viele serielle Ports genutzt werden sollen. Diese Einstellung hat lediglich Einfluss auf die Anzahl der seriellen Schnittstellen, die in der Konfiguration angezeigt werden.

5.1.8.2 **Power Save**

Mit dieser Option ist es möglich, den MC für eine bestimmte Zeit in einen Energiesparmodus zu versetzen. Während dieser Zeit verbraucht das Modul nur etwa 1/3 der typischen Leistung. In diesem Zustand kann das Modul jedoch nicht kommunizieren. Nach Ablauf der angegebenen Zeit meldet sich das Modul mit einem Status-Datagramm zurück. Wenn Sie die Funktion nutzen möchten, kontaktieren Sie den Hersteller.

5.1.8.3 **Securing Passwords**

Mit der Aktivierung dieser Option kann man festlegen, dass die in der Config gespeicherten Passwörter und Zertifikatsschlüssel (z.B. PSK) beim Download der Config nicht mitübertragen werden. Damit kann man verhindern, dass aus der gespeicherten Config-Datei eines MC's diese Daten ausgelesen werden könnten. Wenn diese Funktion einmal aktiviert wurde, kann man diese Option nicht mehr ausschalten. Erst über einen Default-Reset kann diese Option abgeschaltet werden. Auch ein Downgrade der Firmware ist mit aktivem „Securing Passwords“ nicht möglich.

5.1.8.4 **Webserver certificate**

Der MC Webserver kann folgende Zertifikate für Zugriffe per HTTP verwenden:

- selbst signiertes Zertifikat
- Ein Zertifikat, das an dieser Stelle auf den MC hochgeladen werden kann
- Das ggf. schon vorhandene Zertifikat, das für die Authentifizierung im Wireless Abschnitt hochgeladen wurde.

Parameter	Select Certificate Hiermit kann man die oben beschriebene Auswahl treffen
------------------	--

	Certificate Password: Hier kann man vor dem Hochladen eines Zertifikats das dazugehörige Passwort angeben
--	--

5.2 Security

Die folgenden Einstellungen dienen der Einhaltung aktueller Sicherheitsstandards, darunter:

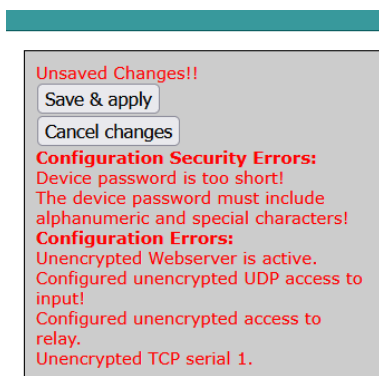
- ISO 27001
- NIS2
- EN 18031
- RED-DA

Die grundlegenden Sicherheitseinstellungen bestimmen die allgemeine Informationssicherheit des Systems.

Mit den hier beschriebenen Einstellungen kann die Verwendung sicherer Verschlüsselungsmethoden deaktiviert werden. Die Aktivierung unverschlüsselter Dienste löst Konfigurationswarnungen aus. Die Nutzer sind allein verantwortlich für die Aufrechterhaltung einer angemessenen Sicherheit und die Minderung damit verbundener Risiken.

Dienste können nach alleinigem Ermessen des Benutzers als gesichert oder ungesichert konfiguriert werden.

Der Parameter „Global Security“ bestimmt das Level mit dem der MC Warnungen bezüglich der Sicherheit der aktuell eingestellten Parameter anzeigt. Bei der Konfiguration über die Webseite werden Warnungen und Fehler unmittelbar bei der Eingabe angezeigt:



Diese Einstellungen sind für „Global Security“ möglich:

Best	Zusätzliche Security Prüfung Admin Login definiert Admin Passwort ausreichend lang (8Zeichen) Admin Passwort mit Sonderzeichen + Zahlen
	Zusätzliche Konfigurationsprüfung: Wenn Schnittstellen aktiviert sind und keine verschlüsselte Kommunikation dafür eingestellt ist, wird das als „Configuration Error“ angezeigt.
Normal	Nur Verschlüsselungsalgorithmen entsprechend der „Openssl Default Provider“ werden angewendet und akzeptiert.
Low	Alle Verschlüsselungsalgorithmen auch die der „Openssl Legacy Provider“ werden angewendet und akzeptiert.

Die weiteren Einstellungen auf dieser Seite, sind sicherheitsrelevante Parameter die auch an anderer Stelle gesetzt werden können, die aber hier thematisch passend angezeigt werden und eingestellt werden können.

Parameter	Gespiegelt von der Seite
Security Administrator Login	Admin
Monitor Login	Admin
URL Authentication	Admin

5.3 Certificate

In diesem Bereich können die im MC-Gerät gespeicherten Zertifikate verwaltet werden.

In den Abschnitten SCEP und EST können zudem Funktionen eingerichtet werden, mit denen Zertifikate automatisch bezogen oder auch erneuert werden können.

5.3.1 Main Certificate

Zur Authentifizierung und zur Prüfung von Serveridentitäten, können verschiedene Zertifikate in den MC-Geräten gespeichert werden.

An dieser Stelle kann das Client-Zertifikat hochgeladen und gespeichert werden, das zur Anmeldung im WLAN per EAP-TLS verwendet wird.

Dazu können hier alle anderen CA-Zertifikate abgelegt werden, die zur Prüfung von Servern-Identitäten benötigt werden. Hier werden zunächst nur 4 Slots angezeigt. Wenn mehr CA-Zertifikate geladen werden, erweitert sich dieser Bereich automatisch.

Certificate Password	Vor dem Upload des Client-Zertifikats muss man hier den Schlüssel eintragen damit der MC Das Zertifikat lesen und speichern kann.
Secure Client Key	Mit der Aktivierung dieser Option wird verhindert, dass beim Abspeichern der Configdatei der im MC gespeicherte Client Key nicht exportiert wird. Das führt aber dazu, dass man bei der Benutzung dieser gespeicherten Configdatei für ein anderes MC Gerät, das Clientzertifikat erneut hochladen muss.

Main Certificate

This is the primary certificate used primarily for wireless authentication and can be automatically updated using SCEP or EST. It can be used for other use like https webserver, too.

Certificate Password:
[Enter certificate password.](#)

Secure client key
Secure the client certificate/key. When enabled, the client key cannot be exported or saved in a configuration file.

Client certificate info
[Information about loaded client certificate](#)

CA certificate info 1
[Information about loaded CA certificate](#)

CA certificate info 2
[Information about loaded CA certificate](#)

CA certificate info 3
[Information about loaded CA certificate](#)

CA certificate info 4
[Information about loaded CA certificate](#)

Upload certificate file: Keine Datei ausgewählt.

Abbildung 5.1: Certificate Upload

5.3.2 SCEP

SCEP steht für **S**imple **C**ertificate **E**nrollment **P**rotocol. Es handelt sich um ein Industriestandard-Protokoll, das die automatisierte Ausstellung und Verwaltung von digitalen Zertifikaten in Public-Key-Infrastrukturen (PKI) ermöglicht. SCEP wurde ursprünglich von Cisco Systems entwickelt und wird heute von verschiedenen Herstellern und PKI-Implementierungen unterstützt.

SCEP vereinfacht den Zertifikatsanforderungsprozess, indem es die Interaktion zwischen Endpunkten (z. B. Geräten oder Benutzern) und der Zertifizierungsstelle (CA) automatisiert. Endpunkte können SCEP verwenden, um Zertifikatsanforderungen (Certificate Signing Requests, CSR) zu generieren und diese an die Zertifizierungsstelle zu senden. Die Zertifizierungsstelle prüft dann die Anforderung und stellt, falls genehmigt, ein digitales Zertifikat aus, das vom Endpunkt zur Authentifizierung und sicheren Kommunikation verwendet werden kann.

Die hier konfigurierbare SCEP Funktion wird in diesem Handbuch nicht näher beschrieben. Wenn Sie diese Funktion benötigen, wenden Sie sich bei Fragen bitte an den Hersteller.

5.3.3 EST

Das Enrollment over Secure Transport (EST)-Protokoll ist ein Standard (RFC 7030), der es Geräten und Anwendungen ermöglicht, sichere digitale Zertifikate von einer Zertifizierungsstelle (CA) über eine HTTPS-Verbindung anzufordern und zu verwalten. Es automatisiert den Prozess der Zertifikatsausstellung und -erneuerung, was besonders wichtig für IoT-Geräte und große Unternehmensnetzwerke ist, die eine automatisierte Zertifikatsverwaltung benötigen.

Hauptfunktionen von EST

- 1) Enrollment (Zertifikatsanforderung)
Beim Enrollment stellt ein Client (z. B. ein Gerät) eine Anfrage an eine CA, um ein neues Zertifikat zu erhalten. Die Anfrage enthält:
 - Ein CSR (Certificate Signing Request), die Informationen wie den öffentlichen Schlüssel und Identitätsdaten des Geräts enthält.
 - Authentifizierungsdaten zur Validierung des Geräts.
- 2) Reenrollment (Zertifikatserneuerung)
Reenrollment ist der Prozess, bei dem ein Gerät ein neues Zertifikat anfordert, um ein bestehendes Zertifikat zu ersetzen, das kurz vor dem Ablauf steht oder bereits abgelaufen ist. Dies stellt sicher, dass das Gerät immer über ein gültiges Zertifikat verfügt und die Kommunikation nicht unterbrochen wird.

- 3) Distribution von CA-Zertifikaten
EST bietet Mechanismen, um CA-Zertifikate sicher an Clients zu verteilen, damit diese die Vertrauenswürdigkeit der CA validieren können.
- 4) TLS-Authentifizierung
 - EST verwendet HTTPS für den sicheren Transport und unterstützt verschiedene Authentifizierungsmechanismen:
 - Username/Passwort (Basic Authentication)
 - Client-Zertifikate (Mutual TLS)

Die hier konfigurierbare EST Funktion wird in diesem Handbuch nicht näher beschrieben. Wenn Sie diese Funktion benötigen, wenden Sie sich bei Fragen bitte an den Hersteller.

5.4 Network

In diesem Abschnitt werden die IP-Adressen des MC und die Eigenschaften der Bridge-Funktion festgelegt.

5.4.1 IP Address

The screenshot shows the 'IP settings' configuration page. At the top, there are tabs for 'Home', 'Device', 'Configuration', 'Statistics', and 'Support'. Below these are sub-tabs for 'Admin' and 'Network', with 'IP address' selected. The main content area includes several settings:

- Enable DHCP Client:** A checked checkbox. Below it is a note: "Check this box to enable the dhcp client for IP configuration. (Disabled for LAN-Client-Cloning)".
- Host Name:** An empty text input field. Below it is a note: "This information is sent to the DHCP server as the parameter 'hostname' during the DHCP process. If this parameter is empty the parameter 'Device Name' (see -> Admin) is used".
- Enable Fallback to Static IP:** A checked checkbox. Below it is a note: "Check this box to enable fallback to static IP if the dhcp client fails".
- Default IPv4 address:** A text input field containing "192.168.170.105". Below it is a note: "Type the IP address of your bridge".
- Default Subnetmask:** A text input field containing "255.255.255.0". Below it is a note: "The subnet mask specifies the network number portion of an IP address. The factory default is 255.255.255.0".
- Gateway Address:** A text input field containing "192.168.170.249". Below it is a note: "This is the IP address of the gateway that connects you to the internet".
- Nameserver Address (DNS):** A text input field containing "0.0.0.0". Below it is a note: "This is the IP address of the nameserver (DNS)".
- Backup DNS 1:** A text input field containing "0.0.0.0". Below it is a note: "This is the IP address of the backup DNS 1".
- Backup DNS 2:** A text input field containing "0.0.0.0". Below it is a note: "This is the IP address of the backup DNS 2".

Enable DHCP:

Mit der Aktivierung dieser Option, bezieht der MC per DHCP die Netzwerkeinstellungen. In der Regel wird dies über eine bestehende WLAN-Verbindung geschehen. Wenn der Parameter „Host Name“ definiert ist, wird diese Angabe in den DHCP-Request übernommen. Ist dieser Parameter leer, wird der „Device Name“ von der Admin-Seite verwendet.

Enable fallback to static IP:

Wenn die Zuweisung der Netzwerkparameter über DHCP fehlschlägt, können die Netzwerkeinstellungen übernommen werden.

IPv4, Subnetmask, Gateway, DNS:

Ohne DHCP werden hier die Netzwerkparameter eingestellt, die der MC über **WLAN** verwendet. Nur im „Pseudo Level 2 Bridge Mode“ ist diese IP-Adresse auch über LAN aktiv.

Format: <SubnetIP>/<MaskBits>,<GatewayIP>

Subnet 1	<input type="text"/>
Subnet 2	<input type="text"/>
Subnet 3	<input type="text"/>
	<input type="button" value="Add"/> <input type="button" value="Remove"/>

Mit diesen Parametern kann man für bestimmte Netzwerke andere GatewayIP's definieren.

IPv6 settings

Enable IPv6 Support (experimental)
Check this box to enable IPv6 support (interface autoconfiguration).

Debug IPv6:
Select log configuration IPv6

Enable Bridge
Check this box to enable IPv6 bridge support. Proxying router advertise with prefix and dhcpv6 relay.

Debug DHCPv6:
Select log configuration DHCPv6

Connection Check
Select connection check method. Test if the gateway replies to neighbor discovery requests.

Reaction
Select action to use when connection is not ready.

IPv6 settings:

Damit wird die IPV6 Funktionalität des MC-Geräts aktiviert.

mDNS settings

Enable mDNS Support
Check this box to enable mDNS (multicast DNS) support.

Debug mDNS:
Select log configuration for mDNS/LLMNR.

Enable LLMNR
Check this box to enable Link Local Multicast Name Resolution (LLMNR) compatibility (Microsoft).

Enable Sernum Host
Check this box to enable mDNS reply to s[Sernum]mcdev.local.

Enable Dev name/Host name
Check this box to enable mDNS reply to [Host/DevName].local.

Reply To Name
On this name the box will reply to an mDNS request in the form [Name].local.

mDNS settings:

mit diesem Verfahren können Namen von Netzwerkgeräten innerhalb eines lokalen Netzwerks in IP Adressen aufgelöst werden, ohne dass ein DNS-Server vorhanden sein muss. Dazu werden alle DNS-Anfragen für die ".local"-Domain per UDP an die mDNS-Multicast-Adresse 224.0.0.251 UDP-Port 5353 gesendet.

Mircosoft Betriebssysteme nutzen zum gleichen Zweck das LLMNR (**Link Local Multicast Name Resolution**) Protokoll. Diese Protokoll kann zusätzlich aktiviert werden und kommuniziert über die Multicast-IP 224.0.0.252 und den UDP-Port 5355

Mit den folgenden 3 Parametern wird festgelegt, auf welche Anfragen das Gerät antworten soll.

5.4.2 Bridge

Der MC unterstützt 5 verschiedene Bridge Modi. Die Modi sind dadurch gekennzeichnet, wie transparent die LAN-Clients am MC an das WLAN angebunden sind, mit welcher MAC-Adresse die LAN-Clients im WLAN arbeiten und ob die LAN-Clients eine eigene IP-Adresse im WLAN haben.

Bridge-Mode	LAN-Clients	IP's im WLAN	Transparenz	Anmerkung
OFF	Beliebig viele	1 (MC IP)	Getrennt	Wenn die Bridge-Funktion deaktiviert wird, können die LAN Clients nicht über die WLAN-Schnittstelle des MC mit anderen Geräten kommunizieren.
LAN Client Cloning	1	1 (LAN Client IP)	alle Ports	Im WLAN ist nur die LAN-Client-IP mit der MAC-Adresse des LAN-Clients registriert.

Single Client NAT	1 + x	1 (MC IP)	alle Ports	Im WLAN ist nur die IP des MC mit der WLAN-MAC-Adresse des MC registriert. Nur ein LAN-Client ist über WLAN adressierbar. Alle anderen LAN-Clients können untereinander und auch ins WLAN kommunizieren.
NAT	beliebig viele	1 (MC IP)	Ports def. per Config	Im WLAN ist nur die IP des MC mit der WLAN-MAC-Adresse des MC registriert. Die LAN-Clients sind nur über bestimmte Ports erreichbar, die in der Portweiterleitungstabelle (NAT rules) festgelegt sind.
Level 2 Bridge	beliebig viele	n x LAN-Clients + 1	alle Ports	Im WLAN sind alle LAN-Client-IP's und die MC-IP mit der WLAN-MAC-Adresse des MC registriert.
MWLC-Mode	beliebig viele	1 (MC IP)	alle Ports	Im WLAN ist nur die MC-IP mit seiner WLAN-MAC-Adresse registriert.

Tabelle 9: Bridge-Modi

5.4.2.1 Bridge-Mode OFF

In diesem Modus ist eine Kommunikation der am MC über den LAN-Port verbundenen Clients über WLAN mit anderen Geräten nicht vorgesehen. Der MC verfügt über 2 IP-Adressen über die auf die MC internen Funktionen zugegriffen werden kann. Das sind z.B. Relais, AUX-IN, serielle Schnittstelle, Webinterface.

Dieser Mode sollte gewählt werden wenn:

- 1) die WLAN Schnittstelle ausgeschaltet ist
- 2) wenn es z.B. bei einer Anwendung darum geht, den MC nur als seriellen Client mit RS232 Schnittstelle zu betreiben. Damit kann man sicherstellen, dass der LAN-Anschluss am MC nicht als Zugang zum WLAN genutzt werden kann.

5.4.2.2 LAN-Client-Cloning

Im „LAN Client Cloning“ Modus geht es darum, ein am LAN-Port des MC angeschlossenes Netzwerkgerät möglichst transparent über WLAN mit einem Netzwerk zu verbinden. Der MC übernimmt für die Kommunikation über WLAN die MAC-Adresse und die IP-Adresse des LAN-Clients.

Wenn der MC mehrere LAN-Ports hat und diese auch angeschlossen sind, wird zur Übernahme der MAC-Adresse nur das Gerät am LAN-Port 1 berücksichtigt. Weitere an den anderen LAN-Ports angeschlossene Geräte können untereinander und auch mit dem „geklonten“ Gerät kommunizieren. Diese anderen Geräte können allerdings nicht über WLAN kommunizieren.

Achtung: Der MC schaltet das WLAN erst an, wenn am LAN-Port Ethernetdaten mit einer MAC-Adresse registriert werden.

Bridge mode configuration

Bridge active

Activate Bridge if you want to exchange data between WLAN and LAN. If the wireless interface is disabled 'Bridge active' has to be switched off

Bridge mode

Select the type of bridging. Single Client NAT and LAN Client Cloning is used when only one client is attached on the LAN port. NAT is used when more than one Client is attached to the LAN Port. Level 2 Pseudo-Bridge is for transparent bridging between LAN and WLAN. Select MWLC-Client or -Server to tunnel the client data between WLAN and the stationary network For further information please refer to the manual

LAN Port Delay

Delay LAN port link up to support clients that transmit important packets after link up.

LAN client Type

Select how LAN-Client detection should work. Static includes DHCP and Autodetect includes DHCP and Static mode.

LAN Client IP

Type the IP address the LAN client to speed up detection. If detection by DHCP is enabled DHCP-Replies will be used for detection.

Subnet mask

Subnet mask of the network the LAN Clients will be connected. This can also be determined by DHCP.

Gateway IP

Gateway IP address of the network the LAN Clients will be connected. This can also be determined by DHCP.

LAN Port Delay:

Wenn der MC zusammen mit dem LAN-Client eingeschaltet wird, kann es sein, dass der LAN-Client schneller bereit ist als der MC. Dann könnte der LAN-Client z.B. zu einem Zeitpunkt schon DHCP Versuche starten, wo er MC noch keine Daten über WLAN weiterleiten kann. Mit aktiviertem „LAN Port Delay“ wird der LAN-Port am MC verzögert eingeschaltet, damit der LAN-Client erst später seine Kommunikation startet.

LAN-Client Type:

Der LAN-Client kann über eine feste IP-Einstellung verfügen, oder per DHCP die IP-Einstellungen über WLAN beziehen.

Abhängig davon kann hier

- DHCP
- Static
- Autodetect

eingestellt werden.

Mit „Static“ und „Autodetect“ können die Parameter IP + Netmask + Gateway vorgegeben werden.

Mit „Autodetect“ kann man sowohl „DHCP-“ als auch „Static“-Clients anschließen. **Dabei muss man aber die Werte für Netzwerkmaske und Gateway IP des Netzwerks angeben, mit dem der LAN-Client arbeitet.** Die IP des Gateways ist wichtig, weil der MC diese IP benutzt um über LAN erreichbar zu sein. Die „LAN client IP“ sollte angegeben werden, wenn der LAN-Client passiv ist, also von sich aus keine Datenpakete mit seiner IP-Adresse sendet. Der MC prüft per ARP-Request, ob die angegebene IP über LAN erreichbar ist. Wenn ja wird diese IP-Adresse dem WLAN-Interface des MC zugeordnet. Damit ist der MC und der LAN-Client mit dieser IP-Adresse über WLAN erreichbar.

DNS1
DNS Server 1 if not determined by DHCP. This DNS server IP can be used by the MC

DNS2
DNS Server 2 if not determined by DHCP. This DNS server IP can be used by the MC

Bridge IP on LAN Port
If no specific bridge IP is defined, the bridge will be visible from the LAN site under the detected or given gateway ip. Normally, this value can be left at 0.0.0.0

IP Timeout
Timeout after detected ip configuration will time out (0 = disable timeout).

Stay connected
If enabled, the wireless connection will not go down even when the LAN link is disconnected

Forward Wake on LAN
If enabled, wake on lan packets are forwarded (UDP port 9) and resent on LAN as broadcast packets.

Forward Other
If enabled, traffic other than ip, ipv6 or arp is directly forwarded in both directions.

MAC to clone
Define here the MAC address that will be cloned. This is useful when more than one MAC can be detected at LAN port 1

Preconnect
If enabled, the wireless connection will come up using the following mac before the client is found. The following mac is learned back to the configuration in this mode.

MAC for Preconnect
Define here the MAC address that will be used for preconnect. If it is empty the mac wireless card is used initially.

DNS1 + 2:
 Wenn der MC einen DNS benötigt um z.B. die IP-Adresse des NTP - Servers aufzulösen, können hier 2 DNS angegeben werden.

Bridge-IP on LAN-Port:
 Wenn man den MC über die LAN-Seite über eine andere IP-Adresse als die Gateway-IP erreichen möchte, kann man diese hier definieren.

IP Timeout:
 Der MC prüft dauernd, ob die „geklonte“ IP noch erreichbar ist. Wenn nach „Ip Timeout“ Sekunden keine Antwort mehr empfangen wurde, wird das WLAN Interface des MC abgeschaltet und erst wieder eingeschaltet bis wieder eine Antwort von der LAN Client IP registriert wurde.

Stay connected:
 Manchmal ist es erforderlich, dass das WLAN Interface des MC trotz ausgeschaltetem LAN Client aktiv bleibt. z.B. in dem Fall, dass das Relais benutzt wird, um den LAN-Client abzuschalten. Dann muss natürlich die WLAN-Verbindung gehalten werden, damit das Relais auch wieder eingeschaltet werden kann.

Forward Wake on LAN:
 Bei aktiver Option werden über WLAN empfangene Wake on LAN Pakete (udp Port 9) als Broadcast über die LAN-Anschlüsse des MC weitergeleitet.

Forward Other
 Wenn diese Option aktiviert ist, wird der gesamte Datenverkehr außer IP, IPv6 oder ARP in beide Richtungen direkt weitergeleitet.

MAC to clone:
 Hier kann man eine bestimmte MAC-Adresse vorgeben, die geklont werden soll. Das wäre z.B. dann nötig, wenn am LAN-Port 1 mehr als eine MAC-Adresse aktiv ist.

Preconnect:
 Normalerweise schaltet der MC im Cloning-Modus das WLAN erst dann an, wenn über den LAN-Port ein Paket vom LAN-Client empfangen wurde. Wenn aber der LAN-Client z.B. erst mit dem Relais des MC unter Spannung gesetzt wird, muss der MC in jedem Fall das WLAN aktivieren.

MAC for Preconnect:
 Der Parameter MAC for Preconnect wird nach einem Start automatisch auf die erkannte Client-MAC gesetzt und bleibt auch dort gespeichert. Für die Ersteinrichtung kann man den Wert leer lassen. In dem Fall wird die MAC der WLAN-Karte für die erste WLAN-Verbindung verwendet.

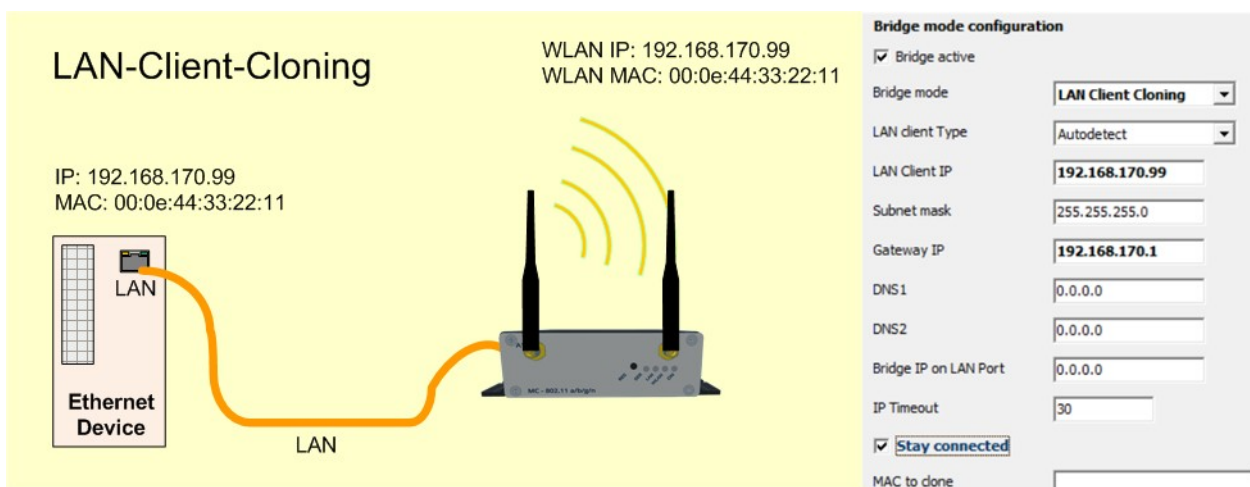


Abbildung 5.2: LAN Client Cloning Mode

Zur Ansteuerung der MC internen Schnittstellen (Webseite, Seriell, Relais, USB) wird die IP-Adresse des LAN-Clients benutzt. Um Kollisionen mit Portnummern, die auf dem LAN-Client benutzt werden, zu verhindern, müssen diese auf dem MC entsprechend angepasst werden. Speziell für die Webseite des MC gibt es unter Configuration->Admin den

Parameter „Webserver Port“ der verändert werden kann, wenn auch der LAN-Client einen Webserver auf Port 80 betreibt.

Vorteile des LAN Client Cloning-Modus:

1. Im WLAN-Netzwerk erscheint der MC zusammen mit dem LAN-Client nur mit einer IP-Adresse

Nachteile des LAN Client Cloning-Modus:

1. An den LAN-Port 1 des MC kann nur ein LAN-Client angeschlossen werden.

5.4.2.3 NAT und Single Client NAT

Im NAT Modus arbeitet der MC mit unterschiedlichen Netzwerken auf der LAN und auf der WLAN-Seite. Im WLAN kommuniziert der MC mit den IP-Einstellungen wie Sie unter 5.4.1 beschrieben sind. Auf der LAN-Seite wird ein davon getrenntes Netzwerk definiert. Wenn Verbindungen über WLAN zu den LAN-Clients hergestellt werden sollen, wird mit einer Tabelle anhand der Portnummer und des IP-Protokolls (UDP/TCP) festgelegt an welche IP-Adresse auf der LAN-Seite die Daten weitergeleitet werden (NAT-Rules).

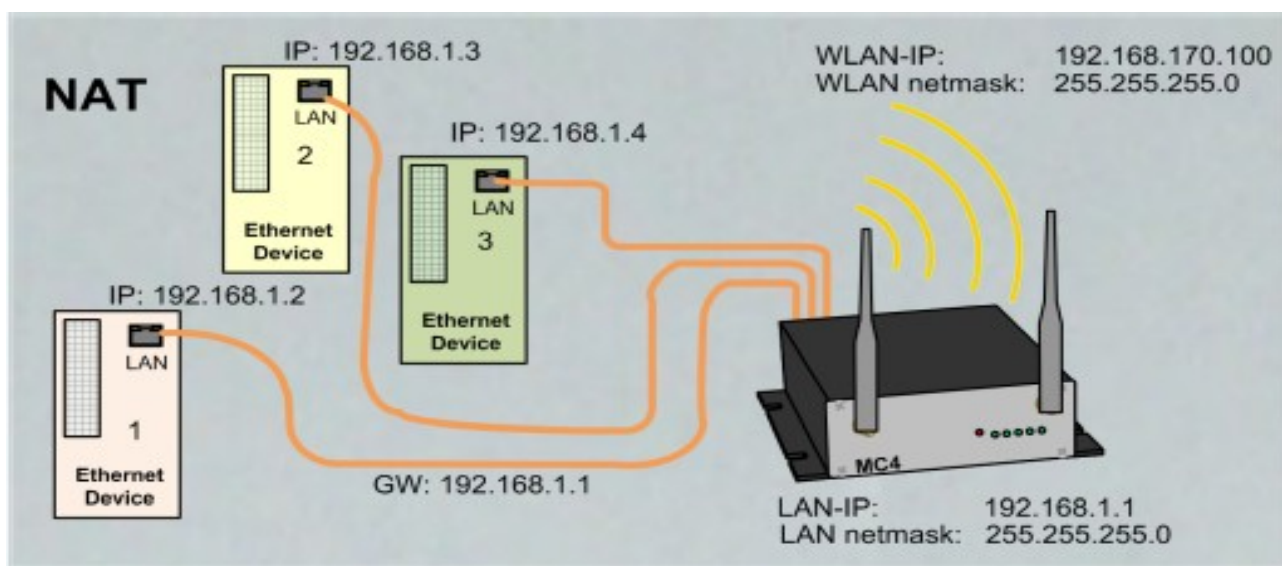


Abbildung 5.3: NAT-Modus (Beispielkonfiguration)

Wenn nur **ein** LAN Client über WLAN erreichbar sein muss, kann die Tabelle entfallen indem man eine IP-Adresse bestimmt, an die alle über WLAN eingehenden Verbindungsanfragen weitergeleitet werden. Für diesen Fall setzt man den Bridge Mode auf „Single Client NAT“.

Bridge mode configuration

Bridge active
Do not disable the bridge except the wireless mode is 'accesspoint'.

Bridge mode:
Select the type of bridging. Single Client NAT and LAN Client Cloning is used when only one client is attached on the LAN port. NAT is used when more than one Client is attached to the LAN Port. Level 2 Pseudo-Bridge is for transparent bridging between LAN and WLAN. Select MWLC-Slave or -Master to tunnel the client data between WLAN and the stationary network

Autodetect LAN client
Check this box to enable auto detection of LAN client IP. The local subnet is arp-pinged and should find the LAN client.

LAN Client IP:
Define the LAN Client IP address or 0.0.0.0 to autodetect the IP

Local IP address:
Type the IP address of your bridge that will be used to the LAN site.

Subnetmask:
The subnet mask specifies the network number portion of an IP address. The default is 255.255.255.0.

Forward DNS requests
Check this box to enable forwarding of DNS requests that are send to our local IP address.

Autodetect LAN client: (Nur Single Client NAT)

Wenn nur ein LAN Client angeschlossen ist, kann man sich bei der Aktivierung dieser Funktion die Definition der LAN-Client-IP-Adresse sparen.

LAN Client IP: (Nur Single Client NAT)

An diese hier angegebene IP werden alle Verbindungsanfragen von der WLAN-Seite weitergeleitet.

Local IP address:

Mit dieser IP Adresse kommuniziert der MC auf der LAN-Seite. Am MC angeschlossene LAN-Clients müssen diese IP als Gateway-IP konfigurieren.

Subnet mask:

Subnetzmaske des lokalen Netzwerks.

Forward DNS requests:

Mit dieser Option wird die Weiterleitung von DNS Anfragen aus dem lokalen Netz an den DNS-Server der der WLAN-Seite freigeschaltet. Damit erübrigt sich die Konfiguration eines speziellen DNS-Server auf den LAN-Clients. Dort muss dann immer nur die lokale IP des MC eingetragen werden.

Enable MAC Authentication
Check this box to enable port authentication via LAN-Client MAC by using configured radius server.

Radius server IPv4 address:
Type the IP address of the radius server.

Radius server port:
Port for radius server.

Radius shared secret:
Shared secret for radius server.

Authentication Timeout:
Timeout for authentication until reauthentication is required.

Radius Debug Level:
Select log configuration for radius.

MAC Authentifizierung (Nur NAT-Mode)

Um zu verhindern, dass sich jedes am LAN-Port des MC eingesteckte Gerät mit dem WLAN verbinden kann, ist es möglich, die MAC-Adresse der zugelassenen Geräte zu registrieren.

Dazu müssen die erlaubten MC-Adressen bei dem Radiusserver des Netzwerks eingetragen werden.

Wenn Sie diese Option aktivieren, werden Parameter angezeigt, die den Zugang zum Radiusserver definieren:

- IP-Adresse
- Portnummer
- Shared secret
- Timeout der Authentifizierung

Zur Fehlersuche kann diese Authentifizierungsfunktion mit dem Parameter „Radius Debug Level“ genauer beobachtet werden. Mit der Einstellung „Detailed“ oder „Maximum“ werden mehr oder weniger detaillierte Meldungen in das Log-File geschrieben, die abgeben welche Schritte der Authentifizierung durchlaufen wurden.

Forwarding rules for NAT

Format: <Protocol: TCP/UDP>:<Port/Range[>Forward Port][,...]>:<IP>[:ftp,snat]

Examples:

TCP:8001>80:192.168.1.2 to redirect TCP connection to port 8001 to 192.168.1.2:80

TCP:987:192.168.1.3 to redirect TCP connection to port 987 to 192.168.1.3

TCP:800-810:192.168.1.4 to redirect TCP connections to the ports between 800 and 810 to 192.168.1.4

TCP:21-23,80,85:192.168.1.4 to redirect TCP connections to the ports 21-23 AND 80 AND 85 to 192.168.1.4

The last optional parameter enables additional options.

'ftp' enables nat helper to access an ftp server behind nat.

'snat' enables SNAT. Outgoing packets on LAN use the source IP of the MC.

NAT Rule 1	<input type="text" value="TCP:8020:192.168.1.10"/>
NAT Rule 2	<input type="text"/>
NAT Rule 3	<input type="text"/>
NAT Rule 4	<input type="text"/>
NAT Rule 5	<input type="text"/>

Mit „Add“ / „Remove“ kann die Anzahl der NAT-Rule-Felder eingestellt werden.

DMZ IP:
Forward all other traffic to this DMZ IP. (Disabled if default 0.0.0.0 is set). All traffic that is not handled local or matching previous NAT rules.

Enable NAT Loopback
Enable NAT-Loopback (also known as Hairpinning).

Special NAT Parameters

Conntracking TIME_WAIT
Change default value of TIME_WAIT state. (Default 120 seconds).

5.4.2.3.1 Forwarding rules for NAT

In diesem Abschnitt werden Regeln definiert, die die Weiterleitung der Verbindungsanfragen von der WLAN Seite zu den LAN-Clients festlegt.

Die Regeln sind wie folgt formatiert:

<Protokoll> : <Portdefinition> : <Client IP>:Option
Protokoll ist entweder **TCP** oder **UDP**

Portdefinition als Weiterleitung

1) Ziel-Portnummer ändert sich nicht:

- Einzelports : 1234 : oder : 123, 1234, 4545 :
- Portbereiche : 8000-8010, 120-130 :

1a) Quell-Portnummer als Weiterleitungskriterium:

Wenn die Quell-Portnummer entscheiden soll, an welche IP die Weiterleitung erfolgen soll, wird dies mit einem führenden '!'-Zeichen vor der Portnummer gekennzeichnet.

- Einzelports : !1234 : oder : !123, !1234, !4545 :

Portdefinition als Umlenkung

2) Ziel-Portnummer ändert sich

- Einzelports : 1234 > 3456 : Client-IP: 192.168.1.10

Es können bis zu 30 dieser Regeln angelegt werden.

DMZ IP: Wenn empfangene Datenpakete über die NAT-Regeln nicht einem Empfänger zugeordnet werden können, werden sie an diese IP geschickt.

Enable NAT Loopback:

Hairpinning, auch bekannt als NAT-Loopback oder NAT-Reflection, ist ein Netzwerkphänomen, bei dem eine Netzwerkverbindung, die eigentlich intern stattfinden sollte, über die externe Adresse einer Firewall geleitet und dann zurück ins interne Netzwerk geschickt wird. Dies kann beispielsweise dann auftreten, wenn ein Gerät im internen Netzwerk versucht, einen Server im gleichen internen Netzwerk über dessen öffentliche IP-Adresse zu erreichen, und die Firewall so konfiguriert ist, dass sie den Datenverkehr umleitet

Special NAT Parameters:

Connection Tracking Timeout:

Wenn eine Verbindung inaktiv wird (für einen bestimmten Zeitraum werden keine Pakete ausgetauscht), entfernt die Firewall des MC nach Ablauf dieser Zeit die Verbindung aus ihrer Verfolgungstabelle und gibt so Ressourcen frei.

Diesen Parameter muss man nur in ganz speziellen Fällen anpassen.

In einer Regeldefinition können sowohl Portbereiche als auch mehrere Portumlenkungen festgelegt werden, indem sie durch Kommata getrennt an werden.

So kann man z.B. mit der Regel:

TCP:3000-3010,4001,4004,5005:192.168.1.2

festlegen, dass alle Daten für die Ports 3000 bis 3010 + 4001 + 4004 + 5005 an die IP-Adresse 192.168.1.2 weitergeleitet werden.

Die Umlenkung von einem Portbereich in einen anderen ist nicht möglich.

Um die Quell-Portnummer als Kriterium für die Zuordnung einer IP-Adresse festzulegen, kann man die Portnummer mit einem führenden Rufzeichen (!) angeben.

FTP-Helper:

Wenn auf einem LAN-Client ein FTF-Server betrieben wird, müssen wegen der dynamischen Portnutzung bestimmte Vorkehrungen getroffen werden, die der Linux-Kernel übernimmt. Dazu muss man in der Definition der NAT-Regel dieses besondere Vorgehensweise mit dem zusätzlichen Parameter „ftp“ aktivieren.

z.B. mit TCP:21:192.168.1.10:ftp

SNAT:

Mit dieser Option wird die Quell-IP der über WLAN ankommenden IP-Pakete durch die IP des MC-LAN-Ports ersetzt.
Beispiel: TCP:12345:192.168.1.10:snat

Weitere Informationen zu dem Thema finden Sie hier: <wikipedia>

5.4.2.3.2 DHCP-Server

Auf der LAN-Seite kann ein DHCP-Server aktiviert werden, der die LAN-Clients mit IP-Adressen versorgt. Die Verteilung der IP-Adressen kann mit einer Reservierungsliste anhand der MAC-Adresse des LAN-Clients oder über den Gerätenamen festgelegt werden.

DHCP Server

DHCP server configuration for LAN clients.
The DHCP server locally manages the LAN client's ip addresses.

Enable DHCP Server

[Check this box to enable the dhcp server configuration.](#)

IP Range start:

[Start of IP range.](#)

IP Range end:

[End of IP range.](#)

Lease Time:

[Lease time in minutes for IPs issued to the clients.](#)

DNS IP:

[Domain Name Server IP. If not needed set to 0.0.0.0. If set to 0.0.0.0 and DHCP-Client on WLAN is active, the DNS data received over WLAN is used](#)

Backup DNS 1:

[Backup 1 Domain Name Server IP. If not needed set to 0.0.0.0. If set to 0.0.0.0 and DHCP-Client on WLAN is active, the DNS data received over WLAN is used.](#)

Backup DNS 2:

[Backup 2 Domain Name Server IP. If not needed set to 0.0.0.0. If set to 0.0.0.0 and DHCP-Client on WLAN is active, the DNS data received over WLAN is used.](#)

Der DHCP-Server bietet nach der Aktivierung folgende Parameter an.

IP Range start (end):

In dem mit diesen 2 IP-Adressen angegebenen Bereich werden die IP-Adressen für LAN-Clients angeboten.

Lease Time:

Die Zeit in Sekunden, nach der eine IP-Adresse neu bestätigt sein muss. Diese Erneuerung wird vom LAN-Client ausgelöst.

DNS IP:

Mit der IP-Adresse liefert der DHCP-Server in der Regel auch die IP-Adresse eines oder mehrerer DNS-Server. Diese DNS-Server können hier definiert werden. Wenn hier keine Angaben gemacht werden, holt sich der DHCP-Server die DNS Informationen von der WLAN-Schnittstelle und übermittelt diese an die LAN-Clients.

Auf der LAN-Seite kann ein DHCP-Server aktiviert werden, der die LAN-Clients mit IP-Adressen versorgt. Die Verteilung der IP-Adressen kann mit einer Reservierungsliste auf Basis der MAC-Adresse des LAN-Clients oder über den Gerätenamen definiert werden.

Static DHCP Server entries

Format: <IP>,<MAC>,<NAME>

Static Entry 1	<input type="text" value="192.168.1.10,,gro-tab"/>
Static Entry 2	<input type="text" value="192.168.1.11,00:08:12:ae:fe:3e,"/>
Static Entry 3	<input type="text"/>
Static Entry 4	<input type="text"/>
Static Entry 5	<input type="text"/>

5.4.2.3.3 Static DHCP Server entries:

Damit LAN-Clients nach dem Einschalten des MC bzw. der ganzen Anlage immer die gleiche IP-Adresse zugewiesen bekommen, kann man in dieser Tabelle über die MAC-Adresse des LAN-Clients oder über den Gerätenamen, der in dem DHCP-Request mitgeschickt wird, bestimmte IP-Adressen aus dem oben definierten IP-Bereich reservieren.

Es können maximal 50 Einträge verwaltet werden.

Vorteile des NAT-Modus:

1. Es können fast beliebig viele LAN-Clients an einen MC angeschlossen werden.
2. Im WLAN-Netzwerk erscheint der MC mit allen LAN-Clients nur mit einer IP-Adresse
3. Wenn in einem Projekt viele Einheiten arbeiten, die aus mehreren LAN-Clients mit einem MC bestehen, ist die Konfiguration für alle Einheiten gleich. Lediglich die IP-Adresse des MC zur WLAN-Seite muss ggf. individuell eingerichtet werden.
4. Die LAN-Clients sind in gewisser Hinsicht besser gegen unerwünschten Zugriff geschützt, weil der MC nur Daten für die konfigurierten Ports durchschaltet.
5. Lokale Broadcast-Datenpakete (auf der LAN-Seite des MC) werden nicht über das WLAN gesendet.

Nachteile des NAT-Modus:

1. Der Zugriff auf die LAN-Clients über WLAN ist nur auf die in den NAT-Regeln definierten Ports möglich.
2. Wenn die LAN-Clients Serverdienste mit gleichen (Standard-)Portnummern (z.B. FTP) anbieten, muss man über WLAN ggf. mit anderen Portnummern arbeiten, um diese Dienste auf den verschiedenen LAN-Clients nutzen zu können.

Wichtig!

Es muss darauf geachtet werden, dass es zu keinen Kollisionen zwischen den Portnummern der LAN-Clients und der internen Schnittstellen des MC kommt. Die internen Schnittstellen des MC sind z.B.

1 serieller Port (default Port 8888)

2 Printer-Server (default Port 9100)

3 MC Webserver (default Port 80 und (oder) 443 (HTTPS), dieser Port kann geändert werden unter Configuration->Admin->Webserver Port)

4 Relais

5 Aux-In

6 MCConfig (UDP+TCP Port 17784 + 17785)

Eine Übersicht der verwendeten Ports kann man unter "Statistics" -> "Network" einsehen -> 6.2

Wenn diese Schnittstellen nicht gebraucht werden, sollte man sie deaktivieren.

5.4.2.4 Level 2 Pseudo-Bridge Modus

Beim Level 2 Pseudo Bridge Mode kommunizieren alle LAN-Clients mit Ihren eigenen IP-Adressen über das WLAN. Dazu wird allerdings bei allen LAN-Clients die MAC-Adresse der WLAN-Karte des MC benutzt. **Voraussetzung für diesen Modus ist es, dass die IP-Adressen aller LAN-Clients und auch die IP des MC im gleichen Netzwerk liegen.**

Dieses Vorgehen kann bei einigen WLAN Infrastrukturen zu Problemen führen, wenn evt. vorhandene WLAN-Controller ARP-Anfragen von der stationären Netzwerkseite anhand einer WLAN-Client Liste beantworten (ARP-Caching). Wenn diese WLAN-Controller nur einen Eintrag MAC <--> IP zulassen, ist der Zugriff auf die LAN-Clients aus dem stationären Netzwerk nicht sicher gegeben, weil ARP-Anfragen evt. nicht beantwortet werden. **Mit dieser Problematik ist in der Regel in controllerbasierten WLAN-Infrastrukturen von CISCO® zu rechnen.**

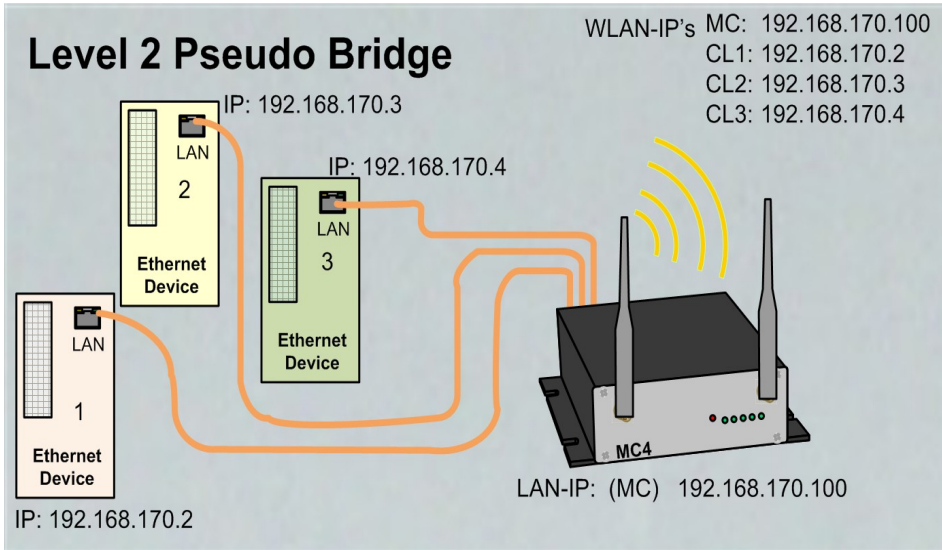


Abbildung 5.4: Level 2 Bridge (Beispielkonfiguration)

In diesem Modus sind nur wenige Einstellungen am MC durchzuführen.

Bridge mode configuration

Bridge active
Activate Bridge if you want to exchange data between WLAN and LAN. If the wireless interface is disabled 'Bridge active' has to be switched off

Bridge mode
Select the type of bridging. Single Client NAT and LAN Client Cloning is used when only one client is attached on the LAN port. NAT is used when more than one Client is attached to the LAN Port. Level 2 Pseudo-Bridge is for transparent bridging between LAN and WLAN. Select MWLC-Slave or -Master to tunnel the client data between WLAN and the stationary network. For further information please refer to the manual

LAN Port Delay
Delay LAN port link up to support clients that transmit important packets after link up.

Scan LAN Clients
Check this box to enable automatic scanning of LAN client IPs.

Forward Multicast/Broadcast
Check this box to enable forwarding of Multicast/Broadcast packets.

Enable DHCP Relay Agent
Check this box to enable relay agent for DHCP requests.

Enable passive client helper
Check this box to enable a helper function for passive clients.

Helper IP
Provide the target IP address for the passive clients helper function that will be pinged in the name of the LAN clients. If no IP is specified the gateway is pinged.

Scan LAN Clients:

Im Fall, dass LAN-Clients am MC passiv sind, also ohne Anfrage selbst keine Daten über Ethernet senden, kann man den MC durch Aktivierung dieser Funktion dazu bringen, das Netzwerk auf der LAN-Seite per ARP-Request regelmäßig zu scannen. Dadurch hat der MC insbesondere nach einem Neustart schnell alle angeschlossenen LAN-Clients registriert.

Forward Multicast / Broadcast

Mit dieser Option kann festgelegt werden, ob Broadcast-Daten die über WLAN beim MC eintreffen auf die LAN-Seite weitergeleitet werden.

Enable DHCP Relay Agent

Wenn die LAN-Clients am MC ihre IP-Adresse per DHCP beziehen, kann diese Option dies unterstützen, indem der MC die DHCP-Requests der LAN-Client so manipuliert, dass die Antworten korrekt bei den LAN-Clients ankommen. Die Notwendigkeit der Unterstützung hängt von der Netzwerkstruktur auf der WLAN-Seite und den Eigenschaften des DHCP-Server ab.

Enable passive client helper

Wenn ein Gerät am LAN-Port angeschlossen wird, das von sich aus keine Kommunikation über den LAN-Port durchführt, sondern vielmehr nur auf Anfragen reagiert, kann mit dieser Funktion der LAN-Client mit seiner IP als Teilnehmer im WLAN besser „bekannt“ gemacht werden. Dazu sendet das MC-Gerät, sobald der Client per ARP-Request erkannt wurde, „im Namen“ des LAN-Clients ein Ping-Request an eine vorgegebene IP-Adresse. Dies geschieht nur ca. 1x pro Minute und auch nur wenn sonst keine Kommunikation stattfindet.

Helper IP

Hier kann eine IP definiert werden, an die der Ping-Request gesendet wird. Wenn die Angabe 0.0.0.0 ist, wird die Gateway-IP als Ziel genommen.

Vorteile:

1. Es können fast beliebig viele LAN-Clients an einen MC angeschlossen werden.
2. Gute Transparenz der LAN-Clients zum WLAN ohne Konfiguration

Nachteile:

1. Der MC und alle LAN-Clients arbeiten mit eigenen IP-Adressen, die aber im gleichen Netzwerk liegen müssen.
2. Schwierigkeiten in einigen WLAN Infrastrukturen mit zentralen Controllern (keine Erreichbarkeit der LAN-Clients aus dem WLAN heraus) .

5.4.2.5 MWLC Mode

Mit dem MWLC-Modus werden alle Einschränkungen bezüglich der Erreichbarkeit, IP-Adressvergabe und der Transparenz insbesondere in Anwendungsfällen mit mehreren LAN-Clients am MC aufgehoben. Dies wird dadurch erreicht, dass der MC in diesem Modus alle am LAN-Port eintreffenden Datenpakete über eine IP/UDP Verbindung (Tunnel) zu einem weiteren MC auf der stationären Netzwerkseite schickt. Dieser MC setzt die empfangenen Datenpakete wieder in den Originalzustand zusammen und sendet sie ins stationäre Netzwerk. Der MC auf der WLAN-Seite arbeitet dabei im MWLC-Slave-Modus und der MC auf der stationären Seite im MWLC-Master-Modus.

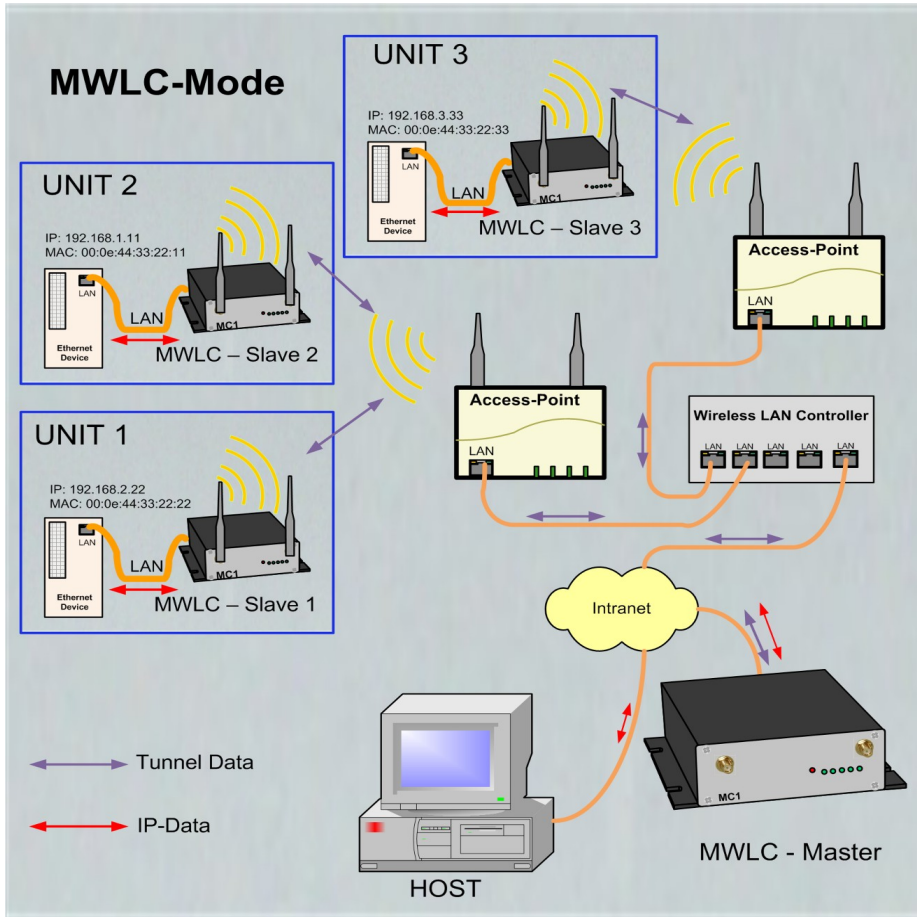


Abbildung 5.5: MWLC-Mode Beispielkonfiguration

In diesem Modus ist es nicht relevant, welche IP-Adressen die Clients im Verhältnis zum MC haben wie z.B. beim Level-2-Pseudo-Bridging. Die Clients werden auch im stationären Netzwerk mit ihren eigenen MAC adressiert. Da der MWLC-Master in dieser Konstellation eine zentrale Rolle spielt und ein Ausfall dieses Geräts die Verbindung aller Clients unterbrechen würde, gibt es die Möglichkeit einen 2. MWLC-Master als Backup zu installieren und die IP-Adresse dieses Backup-Masters in den MWLC-Slaves zu konfigurieren.

Vorteile des MWLC-Modus:

1. Maximale Transparenz der Verbindungen der LAN-Clients über WLAN in das stationäre Netzwerk.
2. Kein besonderer Konfigurationsaufwand auf dem MC egal wie viele LAN-Clients angebunden werden.

Nachteile des MWLC-Modus:

1. Es werden ein oder zwei zusätzliche MC-Adapter auf der stationären Netzwerkseite benötigt.

5.4.2.5.1 MWLC-Master

Home Device Configuration Statistics Support Logout

Bridge mode configuration

Bridge active
Do not disable the bridge except the wireless mode is 'accesspoint'.

Bridge mode
Select the type of bridging. Single Client NAT and LAN Client Cloning is used when only one client is attached on the LAN port. NAT is used when more than one Client is attached to the LAN Port. Level 2 Pseudo-Bridge is for transparent bridging between LAN and WLAN. Select MWLC-Slave or -Master to tunnel the client data between WLAN and the stationary network

High Priority
Enable high priority tunneling data

DHCP Server

DHCP server function is only available when Bridge mode is **NAT** or **Single Client NAT**.

Enable DHCP Server
Check this box to enable the dhcp server configuration.

Der MWLC Master arbeitet mit abgeschalteter WLAN-Schnittstelle.

High Priority:

Damit werden die Daten von und zu den MWLC-Slaves mit einer höheren Priorität verarbeitet als andere Daten.

5.4.2.5.2 MWLC-Slave

Weil das Master-Modul eine zentrale Rolle spielt und somit bei einem Ausfall dieses MC Geräts alle MWLC-Slaves betroffen wären, gibt es die Möglichkeit, einen zweiten Master zu definieren, mit dem sich der MWLC-Slave beim Ausfall des ersten Masters verbindet.

Bridge mode configuration

Bridge active
Do not disable the bridge except the wireless mode is 'accesspoint'.

Bridge mode
Select the type of bridging. Single Client NAT and LAN Client Cloning is used when only one client is attached on the LAN port. NAT is used when more than one Client is attached to the LAN Port. Level 2 Pseudo-Bridge is for transparent bridging between LAN and WLAN. Select MWLC-Slave or -Master to tunnel the client data between WLAN and the stationary network

Master IP
Enter master ip for MWLC-Mode.

Backup Master IP
Enter backup master ip for MWLC-Mode.

High Priority
Enable high priority tunneling data.

Master IP:

IP-Adresse des MWLC-Masters

Backup Master IP:

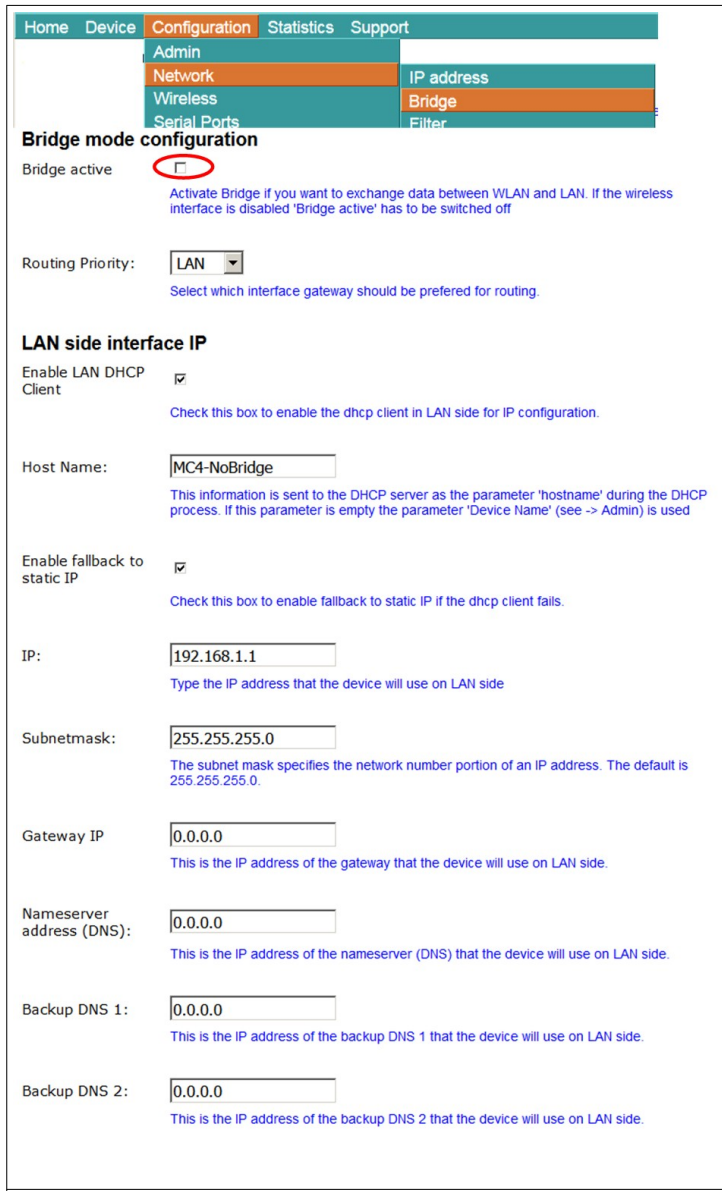
IP-Adresse eines 2. MWLC-Master, der im Fall eines Ausfalls des ersten als Ersatz arbeiten kann.

High Priority:

Damit werden die Daten von und zu den MWLC-Slaves mit einer höheren Priorität verarbeitet als andere Daten.

5.4.3 Bridge not active Mode

Wenn die Bridge Funktion des MC-Geräts abgeschaltet wird, kann man sowohl von der WLAN- als auch über LAN-Schnittstelle auf das MC-Gerät zugreifen, ohne dass zwischen LAN und WLAN Daten ausgetauscht werden. Dieser Modus könnte z.B. dann sinnvoll sein, wenn das MC-Gerät nur als Ethernet zu Seriell Adapter genutzt werden soll. In diesem Modus können 2 verschiedene Zugänge (LAN + WLAN) zum MC-Gerät konfiguriert werden. Die IP-Konfiguration für die WLAN - Schnittstelle wird wie gehabt unter Configuration -> Network -> IP Address eingestellt. Die IP-Konfiguration für die LAN-Seite wird sichtbar, sobald die „Bridge active“ - Option ausgeschaltet wird.

 <p>The screenshot shows the 'Configuration' menu with 'Bridge' selected. Under 'Bridge mode configuration', the 'Bridge active' checkbox is unchecked. Below it, the 'LAN side interface IP' section is visible, including fields for 'Enable LAN DHCP Client', 'Host Name' (MC4-NoBridge), 'Enable fallback to static IP', 'IP' (192.168.1.1), 'Subnetmask' (255.255.255.0), 'Gateway IP' (0.0.0.0), 'Nameserver address (DNS)', 'Backup DNS 1', and 'Backup DNS 2'.</p>	<p>Routing Priority: Wenn WLAN und LAN aktiv ist, ist bei beiden Schnittstellen in der Regel auch ein Gateway definiert. Wenn eine Anwendung auf dem MC-Gerät aktiv eine Verbindung aufbauen will, wird hier festgelegt, welches Gateway dazu verwendet werden soll.</p> <p>Enable LAN DHCP Client: Hiermit kann der DHCP-Client auf der LAN-Seite aktiviert werden, was natürlich nur Sinn macht wenn in dem Netzwerk auch ein DHCP-Server aktiv ist.</p> <p>Host Name: Mit dem hier eingetragenen Namen fordert der DHCP-Client beim Server eine IP-Adresse an.</p> <p>Enable fallback to static IP: Für den Fall, dass der DHCP-Server keine Adresse zuweist, kann man im Folgenden auch IP-Daten angeben, die dann aktiviert werden.</p> <p>In dem folgenden Bereich können alle IP Daten der LAN-Schnittstelle statisch festgelegt werden, wenn kein DHCP aktiv ist.</p>
<p>Format: <SubnetIP>/<MaskBits>,<GatewayIP></p> <p>Subnet 1: <input type="text"/></p> <p>Subnet 2: <input type="text"/></p> <p>Subnet 3: <input type="text"/></p> <p><input type="button" value="Add"/> <input type="button" value="Remove"/></p>	<p>An dieser Stelle können Sie verschiedene Gateways für bestimmte IP-Adressbereiche definieren.</p>

5.4.4 MQTT Client

Mit dieser Funktion ist es möglich, die MC-internen Schnittstellen (Relay, AUX-IN, Seriell) über das MQTT-Protokoll anzusteuern. Zudem kann man auf dieser Seite auch Einstellungen machen, die es möglich machen, MC Statusmeldungen per MQTT zu verschicken.

Manche der folgenden Parameter können mit Variablen versehen werden. Diese Variablen sind aktuell definiert.

Variable	Bedeutung
%dname	Gerätename (siehe Admin)
%wlanmac	MAC-Adresse der WLAN Schnittstelle
%SN	Die Seriennummer des MC
%FW	Firmwareversion des MC

Folgende Parameter sind einzustellen:

Parameter	Funktion	
Broker	Server an den alle Topics und Subscriptions geschickt werden. Hier kann sowohl eine IP-Adresse oder auch ein Hostname angegeben werden.	
Port	Tcp-Port auf dem der Broker Verbindungen erwartet. 1883 ist der Standard-Port für MQTT. Für verschlüsselte Daten der Port 8883.	
TLS Mode	Hier kann eingestellt werden, ob die Daten verschlüsselt werden.	
	1) unencrypted	Ohne Verschlüsselung ggf. mit User + Passwort
	2) TLS Accept All	Verschlüsselt ohne Client-Authentifizierung
	3) Verify by Fingerprint ...	Verschlüsselt: Das Serverzertifikat wird anhand des angegebenen Fingerprints verifiziert.
4) Configured CA Cert	Verschlüsselt: Zur Authentifizierung wird das hochgeladene Client-Zertifikat verwendet.	
Timeout	Timeout in Sekunden für die Verbindung zum MQTT-Server. Wenn der Server über den angegebenen Zeitraum keine Verbindung zum MQTT-Client hat, sendet der Server die unter LWT-Data angegebene Nachricht mit dem Topic LWT-Topic an alle Abonenten.	
Username / Password	Benutzername und Passwort zur Authentifizierung beim MQTT-Server. Diese Angaben sind abhängig von der Konfiguration des MQTT-Servers notwendig oder nicht.	
ClientId	Eindeutige Kennung für die Anmeldung beim MQTT-Server	
Status Topic Type	1) disabled	Keine Statusmeldungen senden
	2) API/Status Parts	Es werden Teile aus dem API/Status im json-Format unter dem Topic „Status Topic“ gesendet. Den Inhalt bestimmen die Pfade die unter „Path x“ definiert sind.
	3) Text	Der unter Status Topic angegebene Text wird als Statusmeldung gesendet.
Status Interval	Zeitabstand zwischen den Statusmeldungen	

Path 1... x	<p>Wenn „Status Topic Type = API/Status Parts“ eingestellt ist, werden hier Teile des API/Status definiert, die gesendet werden sollen</p> <p>Beispiele:</p> <p>\$.Device → sendet alle Elemente der Abfrage API/Status/Device:</p> <pre> { "Device": { "Uptime": "0 Week(s) 0 Day(s) 01:28:54", "UptimeSec": 5334, "SerNum": 300003, "DeviceName": "MC-Dev", "UtcTime": "06.03.2023 16:45:54", "UtcTimeTS": 1678121154, "FirmwareVersion": "2.14h", "KernelVersion": "Linux version 5.4.233", "BuildRoot": { "GitRevision": "1fad7a933d", "Version": "2022.08.3" } }, "Wireless": { "Device": "WLAN Atheros AR9382", "Type": "IEEE802.11an" } } </pre> <p>\$.Device.FirmwareVersion → liefert:</p> <pre> { "Device": { "FirmwareVersion": "2.14h" } } </pre> <p>\$.Wireless.Connection.SNR → liefert die aktuelle Signalstärke der WLAN-Verbindung</p> <pre> { "Wireless": { "Connection": { "SNR": 52 } } } </pre> <p>Die Ausgaben der einzelnen Pfade werden zusammengefasst und dann gesendet.</p>
QoS	Quality of Service (siehe MQTT Protokoll)
LWT Topic	„Last Will and Testament“: Dieses Topic wird beim Broker hinterlegt. Dieser sendet dieses Topic mit dem Inhalt „LWT Data“ wenn der Client innerhalb des Zeitraums „Timeout“ (siehe oben) nicht mehr reagiert.
LWT Data	Last Will Text
Debug	Hier kann ein Debug-Level angegeben werden mit dem Information in die Debug-Log-Datei geschrieben werden.
Client Cert	Hier kann man das Client-Zertifikat hochladen, das im TLS-Mode „Configured CA Cert“ verwendet werden soll.

5.5 Wireless

Unter „Wireless“ werden alle Einstellungen vorgenommen, die definieren, wie sich die WLAN-Schnittstelle des MC-Geräts mit der WLAN-Infrastruktur am Einsatzort verbinden soll.

Es gibt 4 Untermenüs mit folgenden Parametergruppen:

Untermenü	Kapitel	Funktion
Main Parameter	5.5.1	Festlegung der physikalischen Parameter: Frequenzband, Sendeleistung, Ländereinstellung, Antennenkonfiguration
SSID Profile 1	5.5.2	Hier wird der WLAN Netzwerkname festgelegt, mit dem sich der MC verbinden soll. Dazu gehören Einstellungen für die verwendete Verschlüsselung bis zur Möglichkeit Zertifikate auf den MC hochzuladen Wenn gewünscht, kann man mehrere solcher Profile anlegen. Die Anzahl dieser Profile wird unter „Main Parameter“ festgelegt.
Roaming	5.5.3	Spezielle Einstellungen, die den schnellen Wechsel von einem Access Point zum anderen unterstützen können.

5.5.1 Main Parameter

Home	Device	Configuration	Statistics	Support
Wireless Para	Admin	Network		
Enable Wireless Interface	<input checked="" type="checkbox"/>	Wireless	Main Parameter	
Check this box to enable the wireless interface.				
Wireless Mode		Infrastructure		
<small>Select 'Infrastructure' to connect to a wireless (AP) access point, select 'Ad-Hoc' to connect to another bridge or wireless station directly. To use the device as Accesspoint select 'Accesspoint'</small>				
SSID Profiles		1		
<small>Number of SSID Profiles.</small>				
Phy Mode		2.4+5GHz		
<small>Select physical mode - preferred frequencies will be scanned.</small>				
Country selection		Germany		
<small>Select country.</small>				
Enable sleep mode	<input type="checkbox"/>			
<small>Select to enable sleep mode. This is only useful if the device is intended to operate with little power. The reaction time via WLAN will be longer with active sleep mode.</small>				
802.11bg bitrate setting		all bitrates		
<small>If you want to restrict the use of certain bitrates, you can set the bitrates here. Only in special cases this parameter should be set to a value other than 'all bitrates'. This limitation is only applied in the 2.4 GHz band.</small>				
802.11a bitrate setting		all bitrates		
<small>If you want to restrict the use of certain bitrates, you can set the bitrates here. Only in special cases this parameter should be set to a value other than 'all bitrates'. This limitation is only applied in the 5 GHz band.</small>				
Power selection		Auto (MAX)		
<small>Power selection.</small>				
Antenna gain		0		
<small>Antenna gain setting.</small>				
Antenna selection		Ant 1 + Ant 2		
<small>Choose Antenna selection</small>				
Filter SSID	<input type="checkbox"/>			

5.5.1.1 Wireless Mode

zum Aufbau einer WLAN-Verbindung mit Access Points wird hier immer „Infrastructure“ eingestellt.

5.5.1.2 SSID-Profiles

Anzahl der verschiedenen WLAN-Netzwerke die konfigurierbar sein sollen.

5.5.1.3 Phy Mode

Hier wird festgelegt, in welchem Frequenzband (2.4 oder 5 GHz) die Access Points arbeiten, mit denen sich der MC verbinden soll. Man kann auch beide Bänder gleichzeitig verwenden.

5.5.1.4 Country selection

Einstellung des Landes in dem der MC eingesetzt werden soll. Das ist wichtig, damit die länderspezifischen Regeln zur Nutzung der Frequenzbänder eingehalten werden. In der Regel teilen die Access Points diesen Parameter mit. In dem Fall übernimmt der MC diesen Parameter vom AP.

5.5.1.5 Enable sleep mode

Damit kann in beschränktem Umfang der Energiebedarf des MC verringert werden. Die Aktivierung dieser Funktion ist nur bei Anwendungen sinnvoll, die möglichst energieeffizient arbeiten müssen. Wenn diese Funktion aktiv ist, kann der Datenaustausch über WLAN zeitweise etwas verzögert werden.

5.5.1.6 802.11bg bitrate setting

Hiermit kann die Verwendung der möglichen Sendebitraten im **2.4GHz** Band gesteuert werden.

802.11b only -> 1 + 2 + 5.5 + 11 MBit

802.11g only -> 6 + 9 + 12 + 18 + 24 + 36 + 48 + 54 MBit

Die anderen Einstellungen geben die jeweils minimalen Bitraten an.

5.5.1.7 802.11a bitrate setting

Hiermit kann die Verwendung der minimalen Sendebitraten im **5 GHz** Band gesteuert werden.

5.5.1.8 Power selection

Mit diesem Parameter kann die Sendeleistung der Funkkarte im MC ggf. verringert werden. Dies kann sinnvoll sein, wenn nur kurze Entfernungen zu den AP's überbrückt werden müssen und vielen andere Teilnehmer in dem Frequenzband arbeiten.

5.5.1.9 Antenna gain

Mit diesem Parameter muss der Gewinn der angeschlossenen Antenne angegeben werden. Dies gilt insbesondere dann, wenn z.B. gerichtete Antennen angeschlossen werden, deren Gewinn mit mehr als 5 dBi angegeben ist. Entsprechend dieser Angabe, verringert der WLAN-Treiber die Sendeleistung.

5.5.1.10 Antenna selection

Wenn nur ein Antennenanschluss des MC mit einer Antenne bestückt ist, kann man hier einstellen welcher Anschluss das ist. Die Einstellung „Ant 1 + Ant 2“ kann man aber so belassen, auch wenn nur eine Antenne angeschlossen ist.

5.5.1.11 Filter SSID

Diese Einstellung hat Auswirkung auf die AP-Liste, die auf der „Home“ Webseite angezeigt wird. Wenn diese Option aktiv ist, werden nur die AP's angezeigt, die eine „passende“ SSID haben. Damit wird die angezeigte AP-Liste übersichtlicher, insbesondere dann, wenn sehr viele AP's im WLAN-System aktiv sind, die eine andere SSID haben, als in den Profilen definiert sind.

Wireless Status Information Service

This function can be used to send the state of the wireless connection to a network node on the LAN side. The content of this information can be configured and is sent via an UDP datagramm by broadcast or to a given IP address.

Enable wireless info push service

Check this box to enable the service.

Interval:
Interval of the UDP info datagramms in seconds.

Destination IP:
Destination IP address.

Destination port:
Destination UDP-Port.

Format:
Formatstring (possible values: %snr %bssid %apname and more -> see manual.)
snr = Signal Strength, bssid = AP-MAC, apname = AP-Name

Beispiel für Format:
„SNR=%snr;APMAC=%bssid;Link=%wlstat
ergibt zum Beispiel:
SNR=34;APMAC=02:12:34:22:aa:33;Link=1

5.5.1.12 Wireless Status Information Service

Mit dieser Option kann man den MC veranlassen, den Zustand der WLAN-Verbindung an alle oder an einen bestimmten angeschlossenen LAN-Client zu schicken.

Interval

Gibt den Zeitabstand in Sekunden an, in dem die Information gesendet wird.

Destination-IP

Dies ist die Zieladresse für die Statusinformation. Hier kann auch eine Broadcast-Adresse angegeben werden.

Destination port

Dies ist der Ziel UDP-Port für die Statusdaten.

Format

definiert den Inhalt der Information, die gesendet wird. Folgende Werte sind aktuell abfragbar:

%wlstat	1 = verbunden	%wlanip	MC IP über WLAN
%txrate	Sendebitrate	%wlanmac	MC MAC über WLAN
%ch	Funkkanal	%dname	MC Geräte Name
%snr	SNR - Wert	%SN	MC Serien-Nr.
%bssid	AP-MAC	%FW	MC Firmwareversion
%apname	AP-Name	%Relay	aktueller Zustand des Relais

5.5.2 SSID Profile

Ab der Firmware 2.09 ist es möglich, mehrere WLAN SSID Profile zu definieren. Damit kann man den MC so konfigurieren, dass er ohne Eingriff zwischen verschiedenen WLAN Bereichen mit unterschiedlichen SSID's wechseln kann.

Jedes WLAN Profil definiert seine eigenen Parameter für:

- SSID
- Verschlüsselung (WPA/WPA2/WPA3)
- PSK
- 802.1x (EAP-Parameter incl. User + Passwort)

Die 802.1x Zertifikate (Server + User) gelten für alle Profile.

5.5.2.1 SSID Profile

Nr.	Parameter	Wert	Funktion
1	SSID	1-32 Zeichen	Dies ist der Netzwerkname des WLAN's. Dieser wird im 'Infrastructure'-Mode vom AP (WLAN - System) vorgegeben.
2	Priority	1-10	Dieser Wert hat nur eine Bedeutung, wenn mehrere SSID-Profile aktiv sind. Die Priorität bestimmt welches Profil bevorzugt verwendet wird, um sich mit einem WLAN zu verbinden. Der Wert 1 bedeutet die niedrigste Priorität. Wenn nur ein Profil definiert ist, sollte der Wert auf 1 gesetzt sein.

Es sollte vermieden werden, Profile, die nur kurzzeitig verwendet werden (z.B. bei der Inbetriebnahme) auch im „Normalbetrieb“ aktiv zu lassen. Ansonsten können sich Roamingvorgänge unnötig verlängern.

5.5.2.2 Profile change action

Diese Option ist nur relevant, wenn die DHCP-Funktion aktiv ist.

Hier wird festgelegt, was bei einem Wechsel des SSID-Profiles durchgeführt werden muss.

Nr.	Parameter	Wert	Funktion
1	DHCP	Renew Rebind Restart	Diese Einstellung legt fest, wie der MC bei einem Wechsel zu diesem Profil in Bezug auf den ggf. aktiven DHCP-Client verhält. Mit Renew bzw. Rebind wird davon ausgegangen, dass für beide Profile der gleiche DHCP-Server zuständig ist und die schon zugeteilte IP weiterhin benutzt werden kann. Mit „Restart“ wird die DHCP-Prozedur sofort neu gestartet um eine neue IP-Adresse zu erhalten.


5.5.2.3 Connect Action


Diese Option ist nur relevant, wenn die DHCP-Funktion aktiv ist.

Hier kann man angeben, was geschehen soll, nachdem sich der MC mit einen Accesspoint verbunden hat.

Nr.	Parameter	Wert	Funktion
1	DHCP	No action Renew	Diese Einstellung legt fest, was die DHCP-Client-Funktion des MC durchführen soll, wenn eine Verbindung zu einem Accesspoint erfolgreich stattgefunden hat. Diese Aktion wird dann bei jedem Accesspoint-Wechsel durchgeführt. Ein „Renew“ kann bei entsprechend konfigurierten WLAN-Infrastrukturen notwendig sein, die erst dann Daten weiterreichen, wenn eine DHCP-Aktion durchgeführt wurde.

5.5.2.4 Security Parameter

Nr.	Parameter	Wert	Funktion																								
1	Encryption Mode		<p>Hier wird festgelegt welche Verschlüsselungsmethode zur Kommunikation des MC mit dem AP angewendet werden soll. Im Prinzip gibt der AP vor, welche Methode auf dem mit „SSID“ definierten WLAN-Netzwerk zur Anwendung kommt.</p> <table border="1"> <tbody> <tr> <td>1</td> <td>no Encryption</td> <td>keine Verschlüsselung</td> </tr> <tr> <td>2</td> <td>WEP</td> <td>64 oder 128bit Verschlüsselung nach dem RC4-Algorithmus</td> </tr> <tr> <td>3</td> <td>WPA</td> <td>nach 802.11i</td> </tr> <tr> <td>4</td> <td>WPA2</td> <td>nach 802.11i</td> </tr> <tr> <td>5</td> <td>WPA/WPA2</td> <td>automatische Wahl je nachdem was der AP anbietet</td> </tr> <tr> <td>6</td> <td>WPA3</td> <td>Nur WPA3 erlaubt</td> </tr> <tr> <td>7</td> <td>WPA2/WPA3</td> <td>WPA 2 oder 3 erlaubt</td> </tr> <tr> <td>8</td> <td>WPA/WPA2/ WPA3</td> <td>WPA ,WPA2 oder WPA3 Verschlüsselung erlaubt</td> </tr> </tbody> </table> <p> Bei einer WPA-Verschlüsselung empfiehlt sich die Einstellung WPA/WPA2(/WPA3) (automatische Wahl).</p>	1	no Encryption	keine Verschlüsselung	2	WEP	64 oder 128bit Verschlüsselung nach dem RC4-Algorithmus	3	WPA	nach 802.11i	4	WPA2	nach 802.11i	5	WPA/WPA2	automatische Wahl je nachdem was der AP anbietet	6	WPA3	Nur WPA3 erlaubt	7	WPA2/WPA3	WPA 2 oder 3 erlaubt	8	WPA/WPA2/ WPA3	WPA ,WPA2 oder WPA3 Verschlüsselung erlaubt
1	no Encryption	keine Verschlüsselung																									
2	WEP	64 oder 128bit Verschlüsselung nach dem RC4-Algorithmus																									
3	WPA	nach 802.11i																									
4	WPA2	nach 802.11i																									
5	WPA/WPA2	automatische Wahl je nachdem was der AP anbietet																									
6	WPA3	Nur WPA3 erlaubt																									
7	WPA2/WPA3	WPA 2 oder 3 erlaubt																									
8	WPA/WPA2/ WPA3	WPA ,WPA2 oder WPA3 Verschlüsselung erlaubt																									
2	Keying Protocol	nur für WPA(2/3)	<p>Hier kann eingestellt werden, welches Protokoll zur Schlüsselübertragung bei WPA gewählt wird. Nur in Ausnahmefällen sollte hier etwas anderes als „Auto“ gewählt werden</p> <table border="1"> <tbody> <tr> <td>3</td> <td>Auto</td> <td>Der MC bevorzugt CCMP wenn der AP diese Methode anbietet.</td> </tr> <tr> <td>4</td> <td>CCMP</td> <td></td> </tr> <tr> <td>5</td> <td>TKIP</td> <td></td> </tr> <tr> <td>6</td> <td>TKIP + CCMP</td> <td></td> </tr> </tbody> </table>	3	Auto	Der MC bevorzugt CCMP wenn der AP diese Methode anbietet.	4	CCMP		5	TKIP		6	TKIP + CCMP													
3	Auto	Der MC bevorzugt CCMP wenn der AP diese Methode anbietet.																									
4	CCMP																										
5	TKIP																										
6	TKIP + CCMP																										

3	Key	bei WEP	hier wird der WEP-Schlüssel als 10 bzw. 26 stelliger Hexwert angegeben. Ein Beispiel: Wenn der WEP-Schlüssel aus den Zeichen „ABCDE“ besteht, lautet die richtige Eingabe „4142434445“.
		bei WPA	 d die „Passphrase“ angegeben. Diese Zeichenfolge muss tens 8 - und kann maximal 63 Zeichen lang sein. Es gibt Anwendungen, bei denen der Key als 32Byte langer Hexwert angegeben werden muss. Wenn der Zeichenstring, der hier angegeben ist, exakt 64 Zeichen lang ist, wird daraus ein 32Byte langer Hexwert gebildet und dieser als Key abgespeichert.
4	Key Index	nur bei WEP	Auswahl des Schlüssel-Index. In der Regel wird immer „WEP Key 1“ eingestellt.
5	Authentication	nur bei WEP	Auswahl zwischen „Open“ und „Shared Key“ Authentication In der Regel wird immer „Open“ eingestellt
6	Enable 802.11r	nur bei WPA	Das 802.11r Fast Transition (FT) Roaming ist eine Ergänzung zu den 802.11 IEEE-Standards. Mit dieser Option kann eine Methode aktiviert werden, mit der ein schnellerer Wechsel zwischen den AP's des WLAN-Systems ermöglicht wird. Diese Option darf nur aktiviert werden, wenn die APs diese "Fast Roaming"-Funktion nach 802.11r unterstützen und diese Option für die am MC konfigurierte SSID entsprechend auch aktiviert ist. Zu erkennen ist das in der Accesspoint-Liste auf der Home- Webseite des MC. Dort muss in der Spalte „Security“ die Eigenschaft -FT- genannt sein. z.B. [WPA2- FT -EAP-CCMP]
7	Enable SHA256		Aktivieren Sie diese Option nur, wenn Sie sicher sind, dass die WLAN-Infrastruktur SHA256 unterstützt.

5.5.2.5 EAP

1	Enable EAP	Hier wird die Authentifizierung über 802.1x aktiviert. Der Parameter „Key“ unter „Security Parameters“ wird damit deaktiviert.																														
2	EAP-Type	<p>Es gibt verschiedene EAP-Methoden, die hier ausgewählt werden können. Abhängig von der EAP-Methode muss noch ein Passwort angegeben und ggf. müssen auch Zertifikate installiert werden.</p> <table border="1"> <thead> <tr> <th></th> <th></th> <th>User-name</th> <th>Pass word</th> <th>Server-Cert.</th> <th>Client-Cert + Cert. Password</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>TLS</td> <td>✓²</td> <td>x</td> <td>✓¹</td> <td>✓</td> </tr> <tr> <td>2</td> <td>TTLS</td> <td>✓</td> <td>✓</td> <td>✓¹</td> <td>✓</td> </tr> <tr> <td>3</td> <td>PEAP</td> <td>✓</td> <td>✓</td> <td>✓¹</td> <td>x</td> </tr> <tr> <td>4</td> <td>LEAP</td> <td>✓</td> <td>✓</td> <td>x</td> <td>x</td> </tr> </tbody> </table> <p>✓¹ Das Server-Zertifikat muss nicht vorhanden sein. Im Sinne einer sicheren Authentifizierung wird aber empfohlen ein Server-Zertifikat zu laden. ✓² Der Username muss bei TLS in der Regel nicht angegeben werden</p>			User-name	Pass word	Server-Cert.	Client-Cert + Cert. Password	1	TLS	✓ ²	x	✓ ¹	✓	2	TTLS	✓	✓	✓ ¹	✓	3	PEAP	✓	✓	✓ ¹	x	4	LEAP	✓	✓	x	x
		User-name	Pass word	Server-Cert.	Client-Cert + Cert. Password																											
1	TLS	✓ ²	x	✓ ¹	✓																											
2	TTLS	✓	✓	✓ ¹	✓																											
3	PEAP	✓	✓	✓ ¹	x																											
4	LEAP	✓	✓	x	x																											
3	Enable TLS >= 1.2	Diese Option ist per Default aktiv. Wenn der zuständige RADIUSserver neuere TLS Versionen nicht akzeptiert, kann es nötig sein, diese Option abzuschalten.																														
4	Min TLS Version	Hier kann die minimale TLS Version eingestellt werden, die verwendet werden soll.																														
5	No Certificate Verify	Bei EAP-PEAP wird das CA-Zertifikat des RADIUSservers anhand der im MC gespeicherten Zertifikate geprüft. Wenn kein CA-Zertifikat vorhanden ist oder wenn diese Prüfung nicht gemacht werden soll, kann diese Option aktiviert werden.																														
6	Inner auth	nur bei EAP-Type = PEAP oder TTLS Hiermit wird das Protokoll definiert, das für die Kommunikation während der EAP-Authentifizierung verwendet wird. In der Regel ist MSCHAPV2 die richtige Einstellung.																														
7	EAP Username (public)	EAP Benutzername																														
8	EAP Username (private)	EAP Benutzername für die „innere“ Authentifizierung. Nur in Ausnahmefällen unterscheidet sich dieser Benutzername von der ersten Angabe.																														
9	EAP Password	EAP Passwort das im Zusammenhang mit dem EAP Usernamen vergeben wird. Dieses Passwort wird beim EAP-Type TLS nicht benötigt.																														

Die notwendigen Zertifikate können unter Configuration -> Certificate -> Main Certificate verwaltet werden:
> 5.3.1

5.5.3 Roaming

Damit der MC in einer mobilen Anwendung oder einer Umgebung mit sich ändernden Empfangsverhältnissen die Datenverbindung aufrechterhalten kann, wird die Qualität der WLAN-Verbindung laufend überprüft und bei Bedarf eine Verbindung mit anderen besser positionierten Access Points (AP) aufgebaut. Dazu muss der MC in bestimmten Abständen in dem vorgegebenen Frequenzbereich auch auf anderen Kanälen nach alternativen AP's suchen. Dieser kurzfristige Wechsel des Kanals behindert die laufende Datenübertragung. Daher werden Parameter bereitgestellt, die diese Suche und die Kriterien zum Wechsel des AP's einstellbar machen, sodass angepasst an die Einsatzbedingungen die Datenverbindung möglichst stabil gehalten werden kann.


5.5.3.1 Roaming Parameter

Das Roamingverhalten des MC wird durch folgende Parameter bestimmt:

- Das eingestellte Frequenzband (2.4 und (oder) 5 GHz)
- Einen SNR-Schwellwert der bestimmt ob der MC mit kurzen oder langen Zeitabständen nach anderen AP's sucht.
- Angabe eines (langen) Intervalls mit dem der MC die vorgegebenen Kanäle scannt, wenn der SNR Wert **höher** als der angegebene Schwellwert liegt.
- Angabe eines (kurzen) Intervalls mit dem der MC die vorgegebenen Kanäle scannt, wenn der SNR Wert **niedriger** als der angegebene Schwellwert liegt.
- Die explizite Angabe von Kanälen, die der MC scannen soll.

5.5.3.1.1 AP Density

Der SNR-Schwellwert wird durch die Einstellung des Parameters „AP-Density“ vorgegeben. Folgende Werte werden (vor)eingestellt:

Nr.	AP Density	SNR	Anmerkung
1	autodetect (default)	variabel	mit dieser Einstellung wird ein Algorithmus aktiviert, der den SNR-Schwellwert entsprechend der vorgefundenen Gegebenheiten variiert.  Diese Einstellung sollte bevorzugt konfiguriert werden.
2	high	35	Je nachdem wie „dicht“ die AP's in dem Arbeitsbereich des MC montiert sind, kann hiermit ein bestimmter Schwellwert eingestellt werden.
3	medium	30	
4	low	25	
5	static client	20	Wenn der MC an einem festen Standort eingesetzt wird, kann der Schwellenwert relativ niedrig eingestellt werden. Dadurch werden unnötige Scans vermieden.
6	no roaming	0	Wenn Scanvorgänge möglichst minimiert werden sollen, oder es nur einen passenden AP in der Nähe des MC gibt, kann man den SNR Wert mit „no roaming“ auch auf 0 setzen.
7	custom roaming	Para.	Hiermit kann der SNR-Wert individuell vorgegeben werden.

5.5.3.1.2 Channels for Roaming

Insbesondere wenn die WLAN Infrastruktur nur im 2.4 GHz Bereich arbeitet, macht es Sinn, die Kanäle auf denen die APs arbeiten, in dieser Liste zu definieren. Damit kann die Roaming-Funktion des MC das Scannen optimieren.

Für WLAN- Infrastrukturen im 5GHz Bereich macht die Angabe der Kanäle nur Sinn, wenn nur „Nicht DFS Kanäle“ genutzt werden (36,40,44,48) .

5.5.3.1.3 Min scan interval

Mit diesem Parameter wird der Zeitabstand in Sekunden angegeben, mit dem der MC Scans durchführt, wenn der SNR-Wert der bestehenden Verbindung **unterhalb** des SNR-Schwellwerts liegt. 3 Sekunden ist hier der Standardwert.

5.5.3.1.4 Max scan interval

Mit diesem Parameter wird der Zeitabstand in Sekunden angegeben, mit dem der MC Scans durchführt, wenn der SNR-Wert der bestehenden Verbindung **oberhalb** des SNR-Schwellwerts liegt. 60 Sekunden ist hier der Standardwert.

5.5.3.1.5 Blacklist Timer

Wenn bei dem Verbindung-Vorgang mit einem AP ein Fehler auftritt, wird dieser AP zunächst für eine bestimmte Zeit gesperrt. Diese Sperrzeit kann mit dem Parameter „Blacklist Timer“ eingestellt werden. Die Zeit wird in Sekunden angegeben. Ein Wert von 0 bedeutet, dass der Timer **nie** abläuft und somit erst nach einem Reset des MC wieder eine Verbindung mit den AP in der Liste möglich ist.

5.5.3.1.6 802.11r(FT) Mode

Damit ein Client mithilfe der FT-Protokolle von seinem aktuellen AP zu einem Ziel-AP wechseln kann, erfolgt der Nachrichtenaustausch anhand einer der beiden folgenden Methoden:

- Over-the-Air – Der Client kommuniziert direkt mit dem Ziel-AP unter Verwendung der IEEE 802.11-Authentifizierung mit dem FT-Authentifizierungsalgorithmus.
- Over-the-DS – Der Client kommuniziert über den aktuellen AP mit dem Ziel-AP. Die Kommunikation zwischen dem Client und dem Ziel-AP wird in FT-Aktionsframes zwischen dem Client und dem aktuellen AP übertragen und dann über den Controller gesendet.

5.5.3.1.7 Accesspoint Score Calculation

Die Entscheidung mit welchem AP der MC eine Verbindung aufbaut, wird anhand einer Bewertung (Scoring) entschieden, die verschiedene Parameter berücksichtigt. Die Parameter, die zur Verfügung stehen sind auch abhängig von der vorhandenen WLAN-Infrastruktur.

Der wichtigste Wert ist die Signalstärke (SNR).

Von dem SNR Wert ausgehend kann berücksichtigt werden:

- Auslastung des Kanals
- aktuelle Sendeleistung des AP's

Zudem wird eine Statistik über jeden AP geführt, mit dem schon mal eine Verbindung aufgebaut wurde. Dabei werden auch die Fehlversuche registriert, wobei Fehlversuche den Score verringern.

Mit diesem Parameter kann man die Bewertung der zusätzlichen Parameter abschalten und die Bewertung nur auf Basis des SNR durchführen lassen.

5.5.3.2 Background Scanning

Der Standard IEEE 802.11k bietet bei entsprechender Konfiguration des WLAN-Systems den WLAN-Clients an, vom aktuell verbundenen AP eine Liste seiner Nachbar-AP's abzurufen. In der Liste werden die MAC-Adressen und die dazugehörigen Funkkanäle genannt. Damit kann der WLAN-Client gezielter nach alternativen AP's scannen. Der MC unterstützt diese Funktion ab der Firmware 2.12r.

Die Verwendung der Accesspoint-Liste kann wie folgt festgelegt werden:

Nr	Option	Bedeutung
1	Include advanced information	Der MC sucht anhand der intern gespeicherten AP-Liste und der 802.11k - Liste die Kanäle aus, auf denen nach passenden AP's gesucht wird.
2	Only scan channels from neighbor information	Die zu scannenden Kanäle werden ausschließlich anhand der 802.11k - Liste ausgewählt.
3	Ignore neighbor information	Die 802.11k - Liste vom AP wird nicht berücksichtigt.

5.5.3.3 Connection Watchdog

Dies ist eine Option mit der die WLAN-Verbindung überwacht werden kann. Damit soll ein Abbruch der WLAN-Verbindung detektiert werden, indem die empfangenen Datenpakete registriert werden. Wenn innerhalb einer bestimmten Zeit keine eingehenden Datenpakete registriert werden, wird nach einem Scan eine Neubewertung der möglichen Verbindungen durchgeführt. Diese Option sollte nur aktiviert werden, wenn die Anwendung auf den LAN-Clients einen regelmäßigen Datenverkehr über die WLAN-Verbindung erzeugt.

5.5.3.4 Ping-Test

Die Ping-Test-Funktion ist im Wesentlichen eine Fehlersuchfunktion. Wenn es im Betrieb und insbesondere nach einem Wechsel des AP's (Roaming) zu längeren Unterbrechungen der WLAN Verbindung kommen sollte, kann diese Störung mit dieser Funktion im Debug-Log dokumentiert werden. Es ist in dem Fall auch möglich, durch das Rücksetzen und einem Neustart der WLAN-Verbindung zu versuchen, die Unterbrechung zu beheben.

Die Parameter dieser Funktion sind:

Nr.	Parameter	Wert	Default	Funktion
1	Ping IP		192.168.170.1	IP-Adresse, an die Pings geschickt werden.
2	Ping interval	1 - 3600	10	Intervall in Sekunden mit dem die Pings gesendet werden
3	Short interval	0,5 sec 1,0 sec 1,5 sec	0,5sec	Intervall nach einem AP Wechsel
4	Wireless Reconnect		false	Diese Option kann aktiviert werden, um die WLAN-Verbindung nach dem Ausfall einer bestimmten Anzahl von Ping-Antworten neu zu starten.
5	Max. missing replies	1-60	10	Maximale Anzahl der nacheinander ausfallenden Antworten, bevor die WLAN-Verbindung neu gestartet wird.

Ping test

Enable Ping
Check this box to enable pingging.

Ping IP:
IP to use for ping.

Ping interval:
Ping interval in seconds

Short interval: ▼
Select a short ping interval to use after roaming to check the connection.

Wireless Reconnect
Check this box to enable reconnect on ping timeout (Maximum number of missed ping replies reached).

Max. missing replies:
Missing ping replies that are accepted before reconnect.

Abbildung 5.6: Parameter für die Pingtest-Funktion

Da die Unterbrechung der WLAN-Verbindung erfahrungsgemäß häufiger direkt nach einem Wechsel des APs auftritt, wird das Ping-Intervall in dieser Situation kurzzeitig auf „Short interval“ gesetzt. Sobald die erste Antwort korrekt empfangen wurde, wird das Ping-Intervall wieder auf den eingestellten Wert gesetzt. Damit ist sichergestellt, dass ein solcher Verbindungsabbruch schnell erkannt wird und ggf. durch einen „Wireless Reconnect“ zeitnah behoben werden kann.

5.5.3.5 Connection test (ARP)

Diese Option ist eine andere Möglichkeit eine Unterbrechung der Datenverbindung über WLAN zu erkennen.

Wenn der Datenverkehr zu schwach ist oder ungewöhnliche Verzögerungen aufweist, überprüft das System, ob bereits eine ARP-Anfrage gesendet wurde oder ob die Verbindung einen Fehlerstatus aufweist. Sobald ein interner Schwellenwert überschritten wird, wird die konfigurierte Wiederherstellungsmaßnahme automatisch ausgelöst.

Der Parameter „Reaction“ bestimmt die Wiederherstellungsmaßnahme:

Maßnahme	Bedeutung
No action	Der Fehlerstatus wird nur in Debuglog dokumentiert
Re associate	Dabei wird die bestehende Verbindung nicht komplett getrennt, sondern nur der Association-Handshake mit dem Access Point neu initiiert.
Re authenticate	Der 4-Way-Handshake oder EAP/802.1X-Prozess wird erneut durchgeführt. Der Client bleibt mit dem gleichen AP assoziiert, muss aber alle Sicherheitsschlüssel neu verhandeln.

Reconnect	Reconnect startet die Netzwerksuche und Assoziation neu.
Reconfigure	Reconfigure sorgt dafür, dass der wpa_supplicant seine Konfigurationsdatei neu einliest.

5.5.3.6 Preferred / avoided access points

An dieser Stelle können Access Points definiert werden, die bei Roaming-Vorgängen des MC-Geräts entweder präferiert („*Prefer from List*“) oder vermieden („*Avoid from List*“) werden sollen.

Diese Option ist nur aktiv, wenn der Parameter „AP Density“ auf „autodetect“ eingestellt ist.

Die AP's werden mit der MAC-Adresse der BSSID identifiziert.

Diese Funktion macht z.B. dann Sinn, wenn das MC-Gerät sich immer über einen festen Kurs bewegt und in einer Umgebung mit vielen APs nur bestimmte APs verwenden werden sollen, um mit möglichst wenigen Roaming-Vorgängen diesen Kurs fahren zu können. Der „Avoid“-Modus kann sinnvoll sein, wenn bestimmte AP's nur zeitweise gut empfangen werden aber in der Bewegung schnell wieder verdeckt werden. Indem man diese AP's hier einträgt, kann man unnötige Roaming-Vorgänge vermeiden.

Preferred / avoided access points

Enable AP (BSSID) List:

[Enable preferred / avoided AP \(BSSID\) List](#)

The access points (BSSID's) in this list will be preferred / avoided when a roaming decision must be made.

BSSID 1:

BSSID 2:

BSSID 3:

BSSID 4:

BSSID 5:

Abbildung 5.7: Preferred or avoided AP list

Mit der Funktion „Avoid from List“ wird eine Verbindung mit den aufgeführten AP's nicht gänzlich verhindert. Wenn kein anderer passender AP erreichbar ist, wird der WLAN-Treiber des MC trotzdem versuchen, eine Verbindung aufzubauen. Die 3. Option „strictly avoid“ bewirkt, dass sich der MC auf keinen Fall mit den aufgeführten APs verbindet auch wenn keine anderen passenden APs vorhanden sind.

5.5.3.7 Clear ARP

Bei Aktivierung dieser Option wird die interne ARP-Liste des MC nach jedem AP-Wechsel gelöscht. Damit kann erreicht werden, dass die Switches der stationären Netzstruktur durch die dann notwendigen ARP-Requests besser registrieren, dass ein WLAN-Client ggf. den Ethernet-Port gewechselt hat.

5.6 Funktion der seriellen Schnittstelle

Die MC-Geräte verfügen in der Variante MC1, MC2 und optional auch MC6C über eine serielle Schnittstelle, die über (W)LAN angesteuert werden kann.

5.6.1 Parameter der seriellen Schnittstelle

Folgende Parameter können eingestellt werden:

Parameter	Funktion	Default
-----------	----------	---------

Port active	Aktivierung des seriellen Ports	aus		
Device	Port-Adresse	/dev/ttymx0		
Baud rate and format	Einstellung der Baudrate, Datenbits, Stopbits und der Paritybehandlung	9600,8,n,1		
Network configuration	Hier wird eingestellt, in welchem Modus die serielle Schnittstelle über das Netzwerk angesteuert werden kann. Erläuterungen dazu finden Sie im nächsten Abschnitt	TCP-Server, 8888		
Keep alive parameter	Parameter für den TCP-Server oder -Client Modus zur Überwachung der TCP-Verbindung. Lesen Sie dazu die Erläuterung weiter unten.			
Send trigger configuration	Damit nicht jedes einzelne seriell empfangene Zeichen in einem eigenen Netzwerkpaket versendet wird, werden hier 3 Kriterien für das Sammeln und Versenden der Zeichen über das Netzwerk definiert.			
	1	Byte trigger	maximale Anzahl der Zeichen die gesammelt werden.	Default ein : 16
	2	Character timeout	Definition einer maximalen Pause zwischen 2 Zeichen in Millisekunden. Wird diese Zeit überschritten, werden alle bis dahin gesammelten Zeichen gesendet.	Default ein : 100
	3	Frame end trigger	Definition eines Zeichens (als HEX-Wert) das, wenn es empfangen wird, zum Absenden der bis dahin gesammelten Zeichen führt.	Default aus : 0D
Handshake mode	Auswahl für die Steuerung der Handshake - Leitungen der seriellen Schnittstelle. Lesen Sie dazu die Erläuterung weiter unten. 5.6.4			

5.6.2 Network-Configuration Parameter

Für die Nutzung der seriellen Schnittstellen stehen verschiedene Modi zur Verfügung:

5.6.2.1 TCP/IP-Server-Mode:

Mit dieser Einstellung öffnet der MC einen Socket im sog. "Listen"-Modus. D.h. es wird auf einem bestimmten Port (Local port) auf einen Verbindungsaufbau gewartet. Der MC hält immer nur eine Verbindung gleichzeitig. In diesem Modus wird lediglich die Port-Nummer als Parameter angegeben.

5.6.2.2 TCP/IP-Client-Mode:

Hierbei öffnet der MC aktiv eine TCP-Verbindung auf dem angegebenen Port eines anderen Netzknotens. Dieser Netzknoten kann ein anderer MC oder ein Rechner sein, der auf eine Verbindung auf dem angegebenen Port wartet. Neben der Portnummer (Remote port) muss in diesem Modus auch die IP-Adresse des Kommunikationspartners angegeben werden (Server IP).

5.6.2.3 UDP/IP-Mode:

Im UDP-Mode wartet der MC auf dem „Local-Port“ auf Daten, die per UDP/IP an ihn geschickt werden. Die seriell empfangenen Daten werden per UDP/IP an den „Remote-Port“ der Remote-IP-Adresse verschickt. Wenn der Kommunikationspartner nicht bekannt ist, kann die Remote-IP-Adresse incl. Remote-Port auf „0.0.0.0“ bzw. 0 gesetzt werden. In dem Fall übernimmt der MC die Absender IP+Port Information aus dem zuerst auf dem „Local-Port“ eintreffenden Datenpaket.

Der UDP-Mode sollte in solchen Fällen benutzt werden, in denen z.B. eine Trennung der Kommunikationspartner häufiger auftritt. Es muss allerdings beachtet werden, dass das UDP-Protokoll die vollständige Zustellung der Daten nicht sicherstellt.

5.6.2.4 Printerserver-Mode:

Im Printerserver-Mode startet der MC einen TCP/IP-Socket im Server-Modus, der auf dem Port 9100 auf Verbindungen wartet. Dieser Modus ist dafür gedacht, Drucker mit serieller Schnittstelle anzubinden.

5.6.2.5 COMSERVER-Mode:

In diesem Modus kann der MC virtuelle COM-Ports unter Windows® bereitstellen. Auf dem PC wird dazu ein Software-Produkt der Firma Wiesemann & Theis (www.wut.de) eingesetzt. Das Software-Tool wird unter der Bezeichnung COM-Umlenkung geführt. Die W&T COM-Umlenkung bietet in Verbindung mit dem MC die Möglichkeit, serielle Endgeräte über das Netzwerk anzusprechen.

Bitte beachten Sie die Lizenzbedingungen für die Nutzung der COM-Umlenkung.

5.6.2.6 MQTT Mode:

In diesem Modus wird die Kommunikation über MQTT Nachrichten durchgeführt.

Dazu muss natürlich unter „Network → MQTT Client“ ein entsprechender Zugang zu einem MQTT Broker eingerichtet werden.

Network configuration

Port mode ▼
Select the port mode.

MQTT TX Topic:
MQTT TX. Receive on this topic and send to serial.

MQTT RX Topic:
MQTT RX. Publish received serial data to this Topic.

Abbildung 5.8: Serial MQTT Parameter

MQTT TX Topic: Unter diesem Topic empfängt der MC Nachrichten, die über die serielle Schnittstelle gesendet werden.
MQTT RX Topic: Mit diesem Topic werden die über seriell empfangenen Daten an den Broker geschickt.

5.6.2.7 REST-API

In diesem Modus werden Daten der seriellen Schnittstelle über die REST-API ausgetauscht.

5.6.2.7.1 Daten an die serielle Schnittstelle senden

Daten können mit dem Aufruf folgender URL gesendet werden:

```
http(s)://<DevIP>/API/Serial/1/?SendDataStr=Testdata%0d%0a
```

Mit diesem Aufruf wird der String „TestData\r\n“ über die serielle Schnittstelle gesendet.

5.6.2.7.2 Daten von der seriellen Schnittstelle empfangen

Der Zugriff auf die von der seriellen Schnittstelle empfangenen Datenaustausch erfolgt über den Aufruf der URL

```
http(s)://<DevIP>/API/Serial/1/RecvData/0/
```

<DevIP> ist die IP des MC.

Die „/1/“ ist die Nummer der seriellen Schnittstelle. Damit kann man auch weitere serielle Schnittstellen, die z.B. über den USB-Port am MC angeschlossen sind, steuern.

„RecvData/0/“ adressiert den zuletzt empfangenen Datenblock. „RecvData/1/“ den vorletzten usw.

Der MC speichert bis zu 30 Blöcke.

Die Einstellungen unter „Send Trigger Configuration“ bestimmen, wie diese Datenblöcke gebildet werden.

Die seriell empfangenen Daten werden im JSON Format bereitgestellt.

Hier ein Beispiel mit der Ausgabe für die Abfrage „http(s)://<DevIP>/API/Serial/1/RecvData/0/“:

```
{
```

```

"Data": {
  "Length": 10,
  "Str": "Testdata\r\n",
  "B64": "VGVzdGRhdGENCg==",
  "Hex": "54657374646174610D0A"
},
"TS": {
  "Abs": 13260364,
  "Rel": 17509
}
}

```

5.6.3 „Keep alive“-Parameter

Eine TCP/IP-Verbindung bleibt, nachdem Sie einmal aufgebaut wurde, so lange bestehen, bis einer der Kommunikationspartner die Verbindung schließt. Sollte die Verbindung zwischen dem MC und dem Netzwerkkommunikationspartner unterbrochen werden, ohne dass die TCP/IP-Verbindung zuvor geschlossen wurde, kann es passieren, dass sich der MC nicht neu verbindet. Die „Keep alive“ Funktion sendet in dem Zeitabstand von „keep alive period“ Sekunden ein „leeres“ Datenpaket zum Gegenüber. Wenn „keep alive probes“ mal keine Antwort empfangen wurde, setzt der MC den TCP-Socket zurück und startet die Verbindung neu. Insbesondere wenn der MC im TCP-Client-Modus arbeitet, sollte man die „Keep alive“- Funktion aktivieren indem man die Werte für „keep alive period“ und „keep alive probes“ auf Werte > 0 setzt.

5.6.4 „Handshake-Mode“ Parameter

In diesem Abschnitt wird festgelegt, wie die Sende- bzw. Empfangsbereitschaft der seriellen Kommunikationspartner signalisiert wird. Mit den Steuerleitungen RTS, DTR signalisiert der MC Empfangsbereitschaft. Die Signale CTS, DSR sind Eingangssignale über die das angeschlossene serielle Gerät ggf. seine Empfangsbereitschaft mitteilt.

Der MC kann den Datenfluss ferngesteuert (remote) oder auch selbstständig (lokal) bedienen. Der Anwender hat folgende Modi zur Auswahl:

- 1) **no Handshake**: die Signale CTS/DSR werden nicht ausgewertet. Es werden lediglich RTS und DTR aktiv gesetzt, wenn die serielle Schnittstelle über das Netzwerk verbunden ist.
- 2) **XON / XOFF** : Der MC sendet und empfängt die Flusssteuerungszeichen XON = 0x11 und XOFF = 0x13. Der MC sendet ein XOFF Zeichen an den seriellen Partner, wenn der Zwischenspeicher im MC fast gefüllt ist. Wenn der Zwischenspeicher fast leer ist sendet der MC ein XON-Zeichen.
- 3) **RTS/CTS**: Der MC signalisiert über die Signalleitung RTS Empfangsbereitschaft und wertet das Signal CTS aus, um die Empfangsbereitschaft des seriellen Partners zu ermitteln.
- 4) **DTR/DSR**: Der MC signalisiert über die Signalleitung DTR Empfangsbereitschaft und wertet das Signal DSR aus, um die Empfangsbereitschaft des seriellen Partners zu ermitteln.
- 5) **Remote**: In diesem Modus überträgt der MC den Zustand der Eingangs-Signalleitungen CTS, DSR, DCD und RI an den Netzwerkkommunikationspartner. Dies geschieht über einen separaten Socket (Port). Darum muss der Anwender bei dieser Einstellung weitere Angaben abhängig vom eingestellten Netzwerk-Modus machen. Die Zustände der Signalleitungen werden als Zeichenstring beschrieben. Bestimmte Buchstaben beschreiben den Zustand einer bestimmten Signalleitung. Wird der Buchstabe groß geschrieben, bedeutet dies, dass das Signal aktiv ist. Ein Kleinbuchstabe bedeutet ein inaktives Signal. Die Zuordnung ist wie folgt:
 'D' = DSR aktiv ,d' = DSR inaktiv
 'R' = CTS aktiv ,r' = CTS inaktiv
 'C' = DCD aktiv ,c' = DCD inaktiv
 'I' = RI aktiv ,i' = RI inaktiv

Um die Ausgangssignalleitungen RTS und DTR zu steuern, werden folgende Zeichen über das Netzwerk an den MC gesendet:

'D' -> DTR aktiv setzen ,d' = DTR inaktiv setzen
 'R' -> RTS aktiv setzen ,r' = RTS inaktiv setzen

- 6) **RS422 + RS485**: Dieses sind spezielle Modi, die gesetzt werden **müssen**, wenn die serielle Schnittstelle mit einem **RS422 / RS485 Schnittstellen-IC bestückt ist**. Bei RS485 wird die RTS-Leitung genutzt um die Umschaltung zwischen Senden und Empfangen vorzunehmen. Darum gibt es die Möglichkeit, die Aktivierung des Sendetreibers vor und nach dem Senden von Daten festzulegen.

5.6.5 Enable dump

Mit der Aktivierung dieser Option werden alle empfangenen und gesendeten Daten in einer Datei im internen Flash-Speicher des MC aufgezeichnet. Wenn es Probleme bei Datenaustausch auf der seriellen Schnittstelle kommt, kann damit im Zusammenarbeit mit dem Hersteller eine genaue Fehleranalyse vorgenommen werden. Bei Bedarf fragen Sie den Hersteller nach der genauen Vorgehensweise.

5.7 Printer server configuration

Der Printerserver bietet die Möglichkeit, einen Drucker über die USB-Schnittstelle des MC anzubinden. Wenn ein Drucker angeschlossen ist und vom Betriebssystem des MC erkannt wurde, wird auf der Home-Webseite der Status wie folgt angezeigt (Beispiel).

USB Printer Server

State	USB-Printer is connected
Manufacturer	DYMO
Model	DYMO LabelWriter 400
Printed jobs	0
Printed bytes	0

Der einzige Parameter dieser Funktion ist der TCP-Port auf dem der MC die Verbindungen erwartet. (TCP-Server-Mode) Der Standard-Port hat die Nummer 9100 (RAW-Port).

5.8 Relay Configuration

Der MC verfügt abhängig von den Spannungsanschluss am Gerät über ein Relais. Üblicherweise wird es genutzt um z.B. auf Fahrzeugen mit Batteriebetrieb eine Schlummerfunktion zu realisieren.

5.8.1 Parameter zur Steuerung des Relais

Abhängig von eingestellten Modus werden verschiedene Parameter angezeigt.

Relay - OUTPUT configuration

Enable relay control
Check this box to enable relay control.

Mode
Select 'UDP' or 'TCP' to control the relay output via LAN or WLAN. Select 'internal' to control the output via the internal AUX-Input. Select 'Serial Trigger' to switch the relay on when incoming data for the serial port 1 is detected. Select 'WLAN Status' to switch the Relay on when a WLAN connection is established.

Relay restore
Check this box to restore the Relay-Status after a reboot.

Advanced Sequence
Check this box to use advanced relay sequence instead of simple ON or OFF Phrase.

Relay ON
Check this box to define that the relay is on after power up or hardware reset.

Local Port
Portnumber for the IP-Connection (UDP or TCP).

ON Phrase
The data that is received on the defined port is checked for this phrase to switch the relay-output ON. When the phrase is empty any data to that port switches the output to ON.

OFF Phrase
The data that is received on the defined Port is checked for this phrase to switch the relay-output OFF. When the phrase is empty the relay-output is switched off only by the timer.

Timeout (sec)
Define the time in seconds when the relay-output returns automatically from the ON-state to OFF.

Abbildung 5.9: Relais Parameter

Die folgenden Parameter legen die Funktionsweise des Relais fest.

Parameter	Funktion																				
Enable	Hiermit wird die Relais-Funktion ein- oder ausgeschaltet																				
Mode	<p>Art der Relais-Ansteuerung:</p> <table border="1"> <tr> <td>UDP</td> <td>Steuerung über Daten, die über einen UDP/IP Socket auf „Local Port“ empfangen werden.</td> </tr> <tr> <td>TCP</td> <td>Steuerung über Daten, die über einen TCP/IP Server-Socket empfangen werden.</td> </tr> <tr> <td>internal</td> <td>Steuerung über das Eingangssignal (AUX-Input) Wenn der AUX-Input auf „Relay ON / OFF oder toggle eingestellt ist, kann das Relais auch über AUX-Input geschaltet werden, wenn hier ein anderer Mode als „Internal“ eingestellt ist.</td> </tr> <tr> <td>SER trigger</td> <td>Relais einschalten, wenn Zeichen für die serielle Schnittstelle über (W)LAN empfangen wurden.</td> </tr> <tr> <td>WLAN Status</td> <td>Relais einschalten wenn eine WLAN-Verbindung besteht. Ansonsten ist das Relais ausgeschaltet.</td> </tr> <tr> <td rowspan="4">MQTT</td> <td>Steuerung des Relais per MQTT. Parameter für diesen Modus:</td> </tr> <tr> <td>MQTT Ctrl Topic:</td> <td>Der MQTT-Client abonniert dieses Topic um Daten zur Relaissteuerung zu empfangen</td> </tr> <tr> <td>MQTT Ctrl Path:</td> <td>Für den Fall, dass die Daten im JSON Format empfangen werden, kann man hier das Kennwort für das Relais-Kommando nennen. z.B. ein JSON-String mit den Daten: { „Command“ = „ON“ } Wenn man <i>Command</i> hier einträgt, sucht der MC im String nach „Command“ und extrahiert den Wert „ON“ als Kommando zur Relaisansteuerung.</td> </tr> <tr> <td>MQTT Status Topic:</td> <td>Mit diesem Topic wird der Zustand des Relais gesendet. Bei jedem Zustandswechsel des Relais wird dieses Topic gesendet.</td> </tr> <tr> <td>REST API</td> <td>In diesem Mode kann das Relais über die API gesteuert werden. Die URL lautet: http(s)://<DevIP>/API/Relay/Ctrl?Cmd=<Kommando> Das Kommando kann die ON- oder OFF-Phrase sein oder bei aktiver Option „Advanced Sequence“ auch eine Schaltsequenz.</td> </tr> </table>	UDP	Steuerung über Daten, die über einen UDP/IP Socket auf „Local Port“ empfangen werden.	TCP	Steuerung über Daten, die über einen TCP/IP Server-Socket empfangen werden.	internal	Steuerung über das Eingangssignal (AUX-Input) Wenn der AUX-Input auf „Relay ON / OFF oder toggle eingestellt ist, kann das Relais auch über AUX-Input geschaltet werden, wenn hier ein anderer Mode als „Internal“ eingestellt ist.	SER trigger	Relais einschalten, wenn Zeichen für die serielle Schnittstelle über (W)LAN empfangen wurden.	WLAN Status	Relais einschalten wenn eine WLAN-Verbindung besteht. Ansonsten ist das Relais ausgeschaltet.	MQTT	Steuerung des Relais per MQTT. Parameter für diesen Modus:	MQTT Ctrl Topic:	Der MQTT-Client abonniert dieses Topic um Daten zur Relaissteuerung zu empfangen	MQTT Ctrl Path:	Für den Fall, dass die Daten im JSON Format empfangen werden, kann man hier das Kennwort für das Relais-Kommando nennen. z.B. ein JSON-String mit den Daten: { „Command“ = „ON“ } Wenn man <i>Command</i> hier einträgt, sucht der MC im String nach „Command“ und extrahiert den Wert „ON“ als Kommando zur Relaisansteuerung.	MQTT Status Topic:	Mit diesem Topic wird der Zustand des Relais gesendet. Bei jedem Zustandswechsel des Relais wird dieses Topic gesendet.	REST API	In diesem Mode kann das Relais über die API gesteuert werden. Die URL lautet: http(s)://<DevIP>/API/Relay/Ctrl?Cmd=<Kommando> Das Kommando kann die ON- oder OFF-Phrase sein oder bei aktiver Option „Advanced Sequence“ auch eine Schaltsequenz.
UDP	Steuerung über Daten, die über einen UDP/IP Socket auf „Local Port“ empfangen werden.																				
TCP	Steuerung über Daten, die über einen TCP/IP Server-Socket empfangen werden.																				
internal	Steuerung über das Eingangssignal (AUX-Input) Wenn der AUX-Input auf „Relay ON / OFF oder toggle eingestellt ist, kann das Relais auch über AUX-Input geschaltet werden, wenn hier ein anderer Mode als „Internal“ eingestellt ist.																				
SER trigger	Relais einschalten, wenn Zeichen für die serielle Schnittstelle über (W)LAN empfangen wurden.																				
WLAN Status	Relais einschalten wenn eine WLAN-Verbindung besteht. Ansonsten ist das Relais ausgeschaltet.																				
MQTT	Steuerung des Relais per MQTT. Parameter für diesen Modus:																				
	MQTT Ctrl Topic:	Der MQTT-Client abonniert dieses Topic um Daten zur Relaissteuerung zu empfangen																			
	MQTT Ctrl Path:	Für den Fall, dass die Daten im JSON Format empfangen werden, kann man hier das Kennwort für das Relais-Kommando nennen. z.B. ein JSON-String mit den Daten: { „Command“ = „ON“ } Wenn man <i>Command</i> hier einträgt, sucht der MC im String nach „Command“ und extrahiert den Wert „ON“ als Kommando zur Relaisansteuerung.																			
	MQTT Status Topic:	Mit diesem Topic wird der Zustand des Relais gesendet. Bei jedem Zustandswechsel des Relais wird dieses Topic gesendet.																			
REST API	In diesem Mode kann das Relais über die API gesteuert werden. Die URL lautet: http(s)://<DevIP>/API/Relay/Ctrl?Cmd=<Kommando> Das Kommando kann die ON- oder OFF-Phrase sein oder bei aktiver Option „Advanced Sequence“ auch eine Schaltsequenz.																				
Relay restore	Wenn die Schaltstellung des Relais nach einem Neustart (Reboot durch Software) erhalten bleiben soll, markieren Sie diese Option.																				

Parameter	Funktion															
Advanced Sequence	<p>Mit dieser Option kann das Relais mit einem Zeichenstring gesteuert werden, der Schaltsequenzen mit Ein- und Ausschaltphasen und dazwischen Wartezeiten definieren kann. Folgende Kommandos werden erarbeitet:</p> <table border="1"> <thead> <tr> <th>Kommando</th> <th>Parameter</th> <th>Beschreibung</th> </tr> </thead> <tbody> <tr> <td>ON</td> <td></td> <td>Relais schaltet ein</td> </tr> <tr> <td>OFF</td> <td></td> <td>Relais schaltet aus</td> </tr> <tr> <td>S</td> <td>12345</td> <td>Wartezeit in Millisekunden</td> </tr> <tr> <td>ABORT</td> <td></td> <td>Abbruch einer laufenden Sequenz</td> </tr> </tbody> </table> <p>Kommandos werden mit einem ; getrennt</p> <p>Beispiel: „ON;S1500;OFF“ schaltet das Relais für 1,5 Sekunden ein und dann wieder aus.</p>	Kommando	Parameter	Beschreibung	ON		Relais schaltet ein	OFF		Relais schaltet aus	S	12345	Wartezeit in Millisekunden	ABORT		Abbruch einer laufenden Sequenz
Kommando	Parameter	Beschreibung														
ON		Relais schaltet ein														
OFF		Relais schaltet aus														
S	12345	Wartezeit in Millisekunden														
ABORT		Abbruch einer laufenden Sequenz														
Relay ON	Wenn das Relais nach dem Einschalten der Betriebsspannung eingeschaltet sein soll, markieren Sie diese Option. Nach den Ablauf der Zeit „Timeout“ schaltet das Relais wieder in den Ruhezustand.															
Local Port	Portnummer für den Mode UDP oder TCP															
ON Phrase	Zeichenkette zum Einschalten des Relais im Mode „UDP“ oder „TCP“. Wenn hier nichts angegeben ist, schaltet jedes auf dem Port eintreffende Zeichen das Relais an. Der „ON Phrase“ kann eine Zeichenfolge <xx> angehängt werden, die das ON-Kommando um xx Sekunden verzögert. Jedes neue ON-Kommando mit „<xx>“ - Anhang startet den Einschalttimer neu. → 5.8.2															
OFF Phrase	Zeichenkette zum Ausschalten des Relais im Mode „UDP“ oder „TCP“. Der „OFF Phrase“ kann eine Zeichenfolge <xx> angehängt werden, die das OFF-Kommando um xx Sekunden verzögert. Jedes neue OFF-Kommando mit „<xx>“ - Anhang startet den Ausschalttimer neu. → 5.8.2															
Timeout	Zeit in Sekunden, bis das Relais nach dem Einschalten wieder ausgeschaltet wird. Die Angabe 0 bedeutet unendlich lang.															
Power Up Sequence	Dieser Parameter erscheint nur wenn die Option „Advanced Sequence“ aktiv ist. Hier kann man eine Schaltsequenz definieren, die einmalig nach dem Start des Geräts ausgeführt wird. z.B. „ON;S1000;OFF“ Damit wird das Relais nach dem Start für eine Sekunde ein und dann wieder ausgeschaltet.															

Der MC schaltet beim Empfang der korrekten ON- bzw OFF Phrase das Relais in den entsprechenden Zustand und antwortet mit einem Zeichenstring, der dem dann aktuellen Zustand des Relais entspricht.
Die Antwort ist immer 12 Zeichen lang (ON oder OFF Phrase mit angehängten '\0' Zeichen)

In den Modi „UDP“ + „TCP“ kann man irgendeine Zeichenfolge zum MC schicken um den aktuellen Status des Relais als Antwort zu empfangen.

5.8.2 Verzögertes Ein- und Ausschalten des Relais

Ab der Firmwareversion 2.12k besteht die Möglichkeit, die Kommandos zum Ein- oder Ausschalten des Relais zeitverzögert ausführen zu lassen.

Dazu wird direkt nach der „ON -“ bzw. der „OFF Phrase“ eine in Spitzklammern gesetzte Zeitangabe auf den entsprechenden TCP oder UDP Port des MC gesendet.

z.B.: Die ON-Phrase ist auf „ON“ gesetzt. Dann kann man die Zeichenkette „ON<15>“ an den MC schicken, damit das Relais um 15 Sekunden verzögert einschaltet.

Wenn eine Zeitverzögerung aktiv ist, antwortet der MC mit einem Zeichenstring der das letzte Kommando (ON oder OFF) wiedergibt gefolgt von der **verbleibenden** Verzögerung in Spitzklammern.

z.B: „ON<xx>“ wobei „xx“ die aktuelle Anzahl der Sekunden bis zum Einschalten angibt.

5.9 Realtime Clock Configuration

Die MC Geräte verfügen über eine RTC (Real Time Clock), die allerdings nicht mit einer Batterie gepuffert ist. Daher geht eine einmal eingestellte Uhrzeit nach dem Ausschalten der Versorgungsspannung verloren. Der MC startet nach dem Einschalten der Spannung die RTC mit dem Datum 01.01.2000 und der Zeit 00:00:00 Uhr

Unter „Realtime Clock“ kann ein Zeitserver konfiguriert werden, der aktuelle Datum- und Zeitangaben über das Netzwerk (WLAN oder LAN) per NTP einholt.

Die Einstellung eines Zeitservers ist zwingend notwendig, wenn die SCEP Funktionalität genutzt wird. Allerdings hat es auch große Vorteile, wenn Systemmeldungen des MC's mit einem richtigen Zeitstempel versehen werden können.

Parameter	Funktion
Enable NTP Client	Hiermit wird der NTP-Client eingeschaltet
Enable NTS ab FW 2.15	Network Time Security (NTS) ist ein Protokoll, das entwickelt wurde, um die Kommunikation zwischen den Clients und den Zeitservern des NTP-Protokolls (Network Time Protocol) gegen Manipulation zu schützen.
NTP-Server	Hier kann eine IP-Adresse oder ein Hostname (z.B. ptbtime1.ptb.de) für den Zeitserver angegeben werden. Der Defaultwert ist die IP-Adresse 192.53.103.108 Wenn ein Hostname angegeben wird, muss für die Netzwerkverbindung (WLAN) eine DNS IP festgelegt sein (statisch oder über DHCP)
Backup NTP Server	Hier kann ein 2. NTP-Server definiert werden
Timezone	Der Zeitserver liefert eine UTC (<i>Coordinated Universal Time</i>)-Zeit. Um daraus die gültige Ortszeit zu ermitteln, muss man hier die Zeitzone angeben, in der der MC betrieben wird.
Enable DST/ Summertime	In Regionen mit Sommerzeit muss diese Option aktiviert werden.

5.10 Input Configuration

Der MC ist optional mit einem digitalen Eingang ausgestattet. Es ist möglich, den Zustand des Eingangssignals über das Netzwerk anderen Netzwerkteilnehmern zu übermitteln oder über den Eingang das Onboard-Relais zu schalten. Zur Konfiguration stehen folgende Parameter zur Verfügung:

Parameter	Funktion																					
Enable	Hiermit wird die Funktion des digitalen Eingangs eingeschaltet																					
Mode	<table border="1"> <tbody> <tr> <td>1</td> <td>UDP</td> <td>senden des Zustands über einen UDP-Socket (Remote IP : Remote Port)</td> </tr> <tr> <td>2</td> <td>TCP-Client</td> <td>Senden des Signalzustands an einen TCP-Serversocket (TCP-Server-IP : TCP-Server Port)</td> </tr> <tr> <td>3</td> <td>Relay ON</td> <td>Einschalten des Relais bei aktivem Eingangssignal</td> </tr> <tr> <td>4</td> <td>Relay OFF</td> <td>Ausschalten des Relais bei aktivem Eingangssignal</td> </tr> <tr> <td>5</td> <td>Relay toggle</td> <td>Wechsel des Relais-Schaltzustandes beim Aktivieren des Eingangssignals.</td> </tr> <tr> <td>6</td> <td>Intern</td> <td>Geräte interne Verwendung</td> </tr> <tr> <td>7</td> <td>MQTT</td> <td>Senden des Eingangszustands per MQTT.</td> </tr> </tbody> </table>	1	UDP	senden des Zustands über einen UDP-Socket (Remote IP : Remote Port)	2	TCP-Client	Senden des Signalzustands an einen TCP-Serversocket (TCP-Server-IP : TCP-Server Port)	3	Relay ON	Einschalten des Relais bei aktivem Eingangssignal	4	Relay OFF	Ausschalten des Relais bei aktivem Eingangssignal	5	Relay toggle	Wechsel des Relais-Schaltzustandes beim Aktivieren des Eingangssignals.	6	Intern	Geräte interne Verwendung	7	MQTT	Senden des Eingangszustands per MQTT.
1	UDP	senden des Zustands über einen UDP-Socket (Remote IP : Remote Port)																				
2	TCP-Client	Senden des Signalzustands an einen TCP-Serversocket (TCP-Server-IP : TCP-Server Port)																				
3	Relay ON	Einschalten des Relais bei aktivem Eingangssignal																				
4	Relay OFF	Ausschalten des Relais bei aktivem Eingangssignal																				
5	Relay toggle	Wechsel des Relais-Schaltzustandes beim Aktivieren des Eingangssignals.																				
6	Intern	Geräte interne Verwendung																				
7	MQTT	Senden des Eingangszustands per MQTT.																				
Remote Port Remote IP	IP-Adresse und Port des Kommunikationspartners an den die Signalzustände per UDP/IP gesendet werden.																					
TCP-Server Port TCP-Server IP	IP-Adresse und Port des Kommunikationspartners an den die Signalzustände per TCP/IP gesendet werden.																					

Relay Timeout (nur im Mode „Relay ON“)	Wenn über das Eingangssignal das interne Relais geschaltet wird, kann man hier eine Zeit einstellen, die das Relais eingeschaltet bleiben soll. Wenn diese Zeit auf 0 eingestellt wird, gilt die Zeit, die in der Relais-Konfiguration angegeben ist.
ON Text	Zeichenstring der gesendet wird, wenn das Signal aktiv ist.
OFF text	Zeichenstring der gesendet wird, wenn das Signal inaktiv ist.
Sample Rate	Bei aktivierter Option „Report“ werden die jeweiligen Zeichenstrings gesendet, wenn das Eingangssignal wechselt. Mit „Sample Rate“ kann ein Zeitabstand angegeben werden, mit dem der aktuelle Zustand auch ohne Signalwechsel regelmäßig gesendet wird.
Report	Mit dieser Option wird ein Wechsel des Eingangssignals an die aktuell aktive Gegenstation übertragen. Dazu muss entweder eine bestehende TCP-Verbindung vorhanden sein bzw. im UDP-Mode Remote-IP + Port gesetzt sein oder zuvor schon einmal eine Abfrage stattgefunden haben.
MQTT Status Topic:	Mit diesem Topic wird der Zustand des Eingangs gesendet. Bei jedem Zustandswechsel des Eingangs wird dieses Topic gesendet.

5.10.1 Input-Abfrage im UDP-Mode

Im UDP-Mode gibt es die Möglichkeit den Signalzustand von mehreren Stationen im Netzwerk abrufbar zu machen. Wenn die Remote-IP auf „0.0.0.0“ gesetzt ist, wird die Angabe Remote-Port als lokaler Port genommen, auf dem Nachrichten von einer Station im Netzwerk erwartet werden.

Empfängt der MC Daten auf diesem Port, antwortet dieser mit einer „ON“ oder „OFF“ Meldung zur anfragenden Station. Wenn die Option „Report“ gesetzt ist, werden auch Signalwechsel des Input-Signals an diese zuletzt anfragende Station geschickt. Wenn eine andere Station anfragt, werden die Adressdaten dieser Station <IP:Port> als neues Ziel für Statusmeldungen gesetzt.

5.11 Logging Configuration

Der MC bietet folgende Möglichkeiten Daten und Ereignisse aufzuzeichnen:

- 1) Systemmeldungen im RAM, FLASH oder USB Speicher ablegen und diese unter „*Statistics -> SystemLog*“ anzeigen und zum Download bereitstellen. Der Download kann auch mit dem MC-Config-Programm durchgeführt werden.
- 2) Systemmeldungen an einen Syslog-Server senden.
- 3) Den Datenverkehr auf der WLAN- und (oder) der LAN-Schnittstelle mitschneiden.
Die dabei aufgezeichneten Trace-Dateien können über die Home-Webseite (ganz unten) oder über das MC-Config-Program auf einen Rechner übertragen werden.

5.11.1 Systemmeldungen aufzeichnen

Diese hier beschriebenen Möglichkeiten Systemmeldungen oder Mitschnitte des Datenverkehrs aufzuzeichnen, sollen immer nur dazu dienen, auftretende Probleme zu untersuchen und ggf. Maßnahmen aufzuzeigen, wie diese Probleme abgestellt werden können. **Im Normalbetrieb sollten alle hier beschriebenen Einstellungen wieder auf die Defaultwerte zurückgesetzt werden.** Ebenso sollten die evt. noch vorhandenen Log-Dateien über die Funktion: „*Statistics -> SystemLog -> Reset System Log*“ gelöscht werden.

Es gibt die Möglichkeit, die einzelnen Module des MC Betriebssystems unterschiedlich „intensiv“ Systemmeldungen in Form von formatierten Textzeilen erzeugen zu lassen und in einer Datei zu speichern. Wenn es z.B. bei der Nutzung der seriellen Schnittstelle Probleme gibt, kann gezielt dieses Programmteil dazu gebracht werden, sehr genau die auftretenden Ereignisse aufzuzeichnen.

Es empfiehlt sich zur Fehlersuche einen Zeitserver (NTP) zu konfigurieren, damit die Debugmeldungen und auch die (W)LAN-Trace-Mitschnitte zeitlich besser den aufgetretenen Störungen zuzuordnen sind.

Generell sind die Systemmeldungen nicht dazu gedacht, dass der Anwender anhand einer definierten Fehlerliste selbst die Ursache der Störung ermitteln soll. Die DebugLog-Datei soll vielmehr zur Überprüfung an den Hersteller geschickt werden. Die möglichen Systemmeldungen werden im Einzelnen nicht definiert und kommentiert.

5.11.1.1 Debug Log

Log Destination	Hier wird eingestellt, in welchem Speicher die Datei mit den Medlungen abgelegt wird.
-----------------	---

Mögliche Ziele sind:		
Auswahl	Ziel	Anmerkung
RAM	interner RAM Speicher	Die so aufgezeichneten Meldungen gehen nach einem „Power Down“ oder einem Reset verloren
Internal FLASH	interner FLASH Speicher	Nach einem „Power Down“ oder einem Reset werden die folgenden Meldungen an das Ende einer evt. schon vorhandenen Debugdatei geschrieben. Die maximale Größe der Datei beträgt 16 MByte. Wenn die 16MByte erreicht sind, wird die aktuelle Datei komprimiert und abgespeichert. Danach werden die Meldungen in einer neuen Datei gespeichert.
USB	Externer USB-FLASH Speicher	In diesem Modus wird nach jedem Reset eine durchnummerierte neue Debug-Datei angelegt. Also „DebugLog0.dat“, „DebugLog1.dat“ usw. Die Größe der Datei ist nur begrenzt von der Kapazität des USB-Speichers.

5.11.1.2 Debug Information

Neben dem eigentlichen Text der Meldung kann man festlegen welche zusätzlichen Informationen mit angegeben werden.

Nr.	Information	Anmerkung
1	Absolute Timestamp	Zeitangabe im Format „Tag.Monat Stunde:Minute:Sekunde.Mikrosekunde“ Wenn keine Zeitangabe über das Netzwerk empfangen wurde (NTP), wird hier die vergangene Zeit seit dem Systemstart angegeben.
2	Relative Timestamp	Zeitangabe als Zähler der vergangenen Millisekunden seit dem Start.
3	Repeat Counter	Zähler der angibt, wie oft diese Meldung seit dem Systemstart ausgegeben wurde.
4	Thread	Name oder ID des Prozesses, der diese Meldung ausgibt
5	Source file name	a) Name der Programmdatei und b) Nummer der Programmzeile, die diese Meldung erzeugt hat.
6	Klasse	Es gibt die Klassen: ERROR WARN INFO TRACE die entsprechend den Debug-Einstellungen (Default, Detailed, Maximum) aktiv sind.
7	Meldung	

Beispiel einer Ausgabezeile:

13894468 8152 696 9.3. 12:57:03.903116 MMqttCIKA Mqtt.c [1705] INFO: ID_00:0E:8E:64:D4:CC: Send PING

Elemente:

2	3	1	4	5a	5b	6	7
13894468	8152	9.3. 12:57:03.903116	696	MMqttCIKA Mqtt.c	[1705]	INFO:	ID_00:0E:8E:64:D4:CC Send PING

5.11.1.3 Syslog Server

Diese Meldungen können auch an einen Syslog-Server verschickt werden. Dazu wird die IP-Adresse dieses Servers definiert. Mit der Angabe „0.0.0.0“ ist diese Funktion nicht aktiv.

Um einen Syslog-Server verwenden zu können, sollte dieser über den LAN-Anschluss erreichbar sein. Syslog-Meldungen über WLAN an einen Server zu senden ist nicht zu empfehlen, weil diese den Datenverkehr über WLAN erheblich erhöhen können. Zudem gehen die Meldungen bei einer Störung auf der WLAN-Verbindung in der Regel verloren.

Debug Log
Log Destination:
[Select Destination for debug log file.](#)

Debug Information
Absolute Timestamp
[Check this box to enable absolute timestamp in logfile.](#)
Relative Timestamp
[Check this box to enable relative timestamp in logfile.](#)
Repeat Counter
[Check this box to enable repeat counter in logfile.](#)
Thread
[Check this box to enable thread name/id in logfile.](#)
Source file name
[Check this box to enable source file name in logfile.](#)

Syslog Server
IP of Syslog Server:
[IP of Syslog-Server.](#)

Abbildung 5.10: Debug Log Parameter

5.11.1.4 Traffic Dump Configuration

Mit der Funktion „Traffic Dump Configuration“ kann der Datenverkehr auf der LAN- und (oder) der WLAN-Schnittstelle aufgezeichnet werden. Die dabei erzeugten Dateien können mit bekannten Programmen wie z.B. *Wireshark* analysiert werden.

Traffic Dump Configuration

Dump Wireless [Check this box to enable dump of wireless packets in monitor mode.](#)

Monitor Dump Destination: [Select destination for WLAN monitor mode dump.](#)

Filter: [Select method for filtering packets.](#)

Dump Control: [Select desired action if dumping is enabled but flash is full.](#)

Dump LAN [Check this box to enable dump of ethernet packets.](#)

Monitor Dump Destination: [Select destination for ethernet monitor dump.](#)

Dump Control: [Select desired action if dumping is enabled but flash is full.](#)

Abbildung 5.11: Traffic Dump Configuration

Parameter	Funktion
Dump Wireless	Hiermit wird die Aufzeichnung der Datenpakete auf der WLAN-Seite aktiviert
Monitor Dump Destination	Einstellung des Speicherplatzes für die WLAN - Aufzeichnungen
	1) Internal Flash Interner Flashspeicher (ca. 400MByte)
	2) USB Externer USB-Speicher (je nach Kapazität es Speicher-Sticks)
Filter	Um über einen möglichst langen Zeitraum die WLAN-Daten aufzuzeichnen, kann man hier einen Filter aktivieren, der nur die von der "eigenen" WLAN-Funkkarte gesendeten und empfangenen Daten speichert. Alternativ kann man auch einen selbst definierten Filter angeben. Dazu sollte man sich aber mit dem Filterformat des pcap-Moduls vertraut machen. Folgende Optionen sind auswählbar: 1) no Filter 2) only own traffic 3) Custom
Dump Control	Mit „Dump Control“ kann man einstellen was passiert wenn die Speichergrenze des internen Flash oder des USB-Speichers erreicht wird. 1) Die Aufzeichnung wird gestoppt 2) Die älteste Aufzeichnung wird gelöscht und die Aufzeichnung wird mit einer neuen Datei fortgesetzt.

Filesize (wird nur angezeigt wenn „Monitor Dump Destination“ = USB)	Wenn die Aufzeichnungen im USB-Speicher abgelegt werden, kann man hier die maximale Größe der Datei festlegen: Small = 8 MByte Medium = 32 MByte (Default) Large = 128 MByte	
Dump LAN	Hiermit wird die Aufzeichnung der Datenpakete auf der LAN-Seite aktiviert	
Monitor Dump Destination	1) Internal Flash	Interner Flashspeicher (ca. 400MByte)
	2) USB	Externer USB-Speicher (je nach Kapazität es Speicher-Sticks)
Dump Control	Mit „Dump Control“ kann man einstellen was passiert wenn die Speichergrenze des internen Flash oder des USB-Speichers erreicht wird. 1) Die Aufzeichnung wird gestoppt 2) Die älteste Aufzeichnung wird gelöscht und die Aufzeichnung wird mit einer neuen Datei fortgesetzt.	
Filesize (wird nur angezeigt wenn „Monitor Dump Destination“ = USB)	Wenn die Aufzeichnungen im USB-Speicher abgelegt werden, kann man hier die maximale Größe der Datei festlegen: Small = 8 MByte Medium = 32 MByte (Default) Large = 128 MByte	

Während der Aufzeichnung wird jeweils bei einer Größe von 32MByte (oder 8 oder 128MByte) die aktuelle Aufzeichnungsdatei geschlossen und eine neue Datei geöffnet. Die abgelegte Datei wird anschließend komprimiert und als *.gz -Datei in das Filesystem geschrieben, Die Originaldatei wird danach gelöscht. Je nach Komprimierungsrate der Daten kann so über einen langen Zeitraum der Datenverkehr mitprotokolliert werden.

Die komprimierten Dateien können anschließend von der „Home“ - Webseite des MC heruntergeladen werden. Die Liste der Dump-Dateien befindet sich am Ende der „Home“ Seite noch unter der Liste der Access Points. Die Erklärung für die Zusammensetzung der Dateinamen wird hier erklärt -->Fehler: Verweis nicht gefunden

Wireless Dump	
Capture byte count	2666376KByte
Recv count	16462248
Drop count	24634/12616 (If 0)
Recent Dumpfiles	391002_WLANDump_0140_20000101_073944_843916.pcap.gz (21687 KByte)
Recent Dumpfiles	391002_WLANDump_0141_20000101_074048_360020.pcap.gz (18244 KByte)
Recent Dumpfiles	391002_WLANDump_0142_20000101_074233_462674.pcap.gz (21912 KByte)
Recent Dumpfiles	391002_WLANDump_0143_20000101_074310_600030.pcap.gz (16050 KByte)
Recent Dumpfiles	391002_WLANDump_0144_20000101_074604_862172.pcap.gz (19922 KByte)
Recent Dumpfiles	391002_WLANDump_0145_20000101_074731_698195.pcap.gz (19984 KByte)
Recent Dumpfiles	391002_WLANDump_0146_20000101_074851_473225.pcap (26937 KByte)
Ethernet Dump	
Capture byte count	89640KByte
Recv count	79175
Drop count	0/0 (If 0)
Recent Dumpfiles	391002_EthernetDump_0000_20000101_074003_654321.pcap.gz (16143 KByte)
Recent Dumpfiles	391002_EthernetDump_0001_20000101_074251_645069.pcap.gz (16549 KByte)
Recent Dumpfiles	391002_EthernetDump_0002_20000101_074643_559405.pcap (23742 KByte)

Abbildung 5.12: Wireless und Ethernet Dump Dateien

Als zusätzliche Information wird angegeben, wie viele Bytes und Datenpakete im aktuellen Dump gespeichert sind. Dazu gibt es noch eine Information über die Anzahl der Datenpakete die verworfen wurden (Drop Count). Die Dateinamen können angeklickt und damit heruntergeladen werden.



Diese Art des Mitschneidens des Datenverkehrs auf den Schnittstellen beansprucht insbesondere den FLASH-Speicher ganz erheblich und **sollte nur zur Fehlerdiagnose aktiviert werden. Im produktiven Einsatz sollte diese Funktion deaktiviert sein.**

Die Dump-Dateien können über die Funktion: „Statistics -> SystemLog -> Reset System Log“ gelöscht werden.

5.11.1.4.1 Debug-Dateien mit dem MC-Config Programm vom MC herunterladen

Um alle Log-Dateien in einem Vorgang vom MC herunterzuladen, kann man beim MC-Config Programm über das Kontext-Menü (MC Eintrag rechts anklicken) folgendes Kommando auswählen:

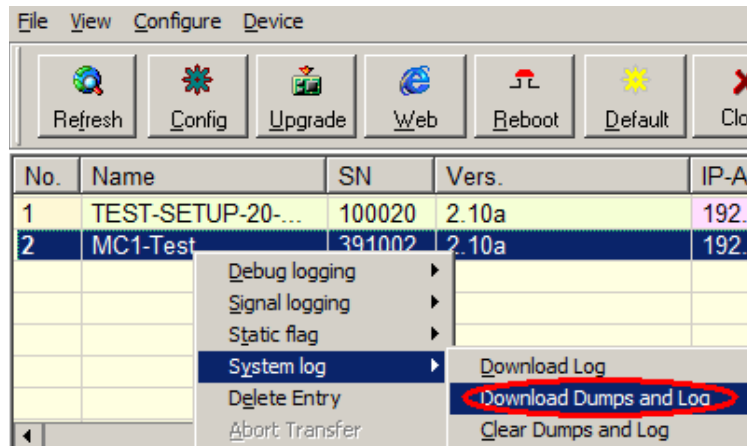


Abbildung 5.13: Download Dumps and Logs mit dem MC-Config-Programm

Ab der MC-Firmware 2.10b und der MC-Config Version 2.0.2.32 öffnet sich ein Dialog zur Festlegung des Ordners in dem die Dateien angelegt werden. Danach öffnet sich ein Dialog, in dem man die Log- und Dump-Dateien zum Herunterladen auswählen kann. Vor dem Öffnen dieses Dialogs werden alle aktiven Dump Prozesse gestoppt. Die noch vorhandenen pcap-Dateien werden komprimiert. Dieser Vorgang kann einige Zeit dauern. In der Spalte „Status“ wird dieser Zustand angezeigt.

Danach wird folgender Dialog angezeigt:

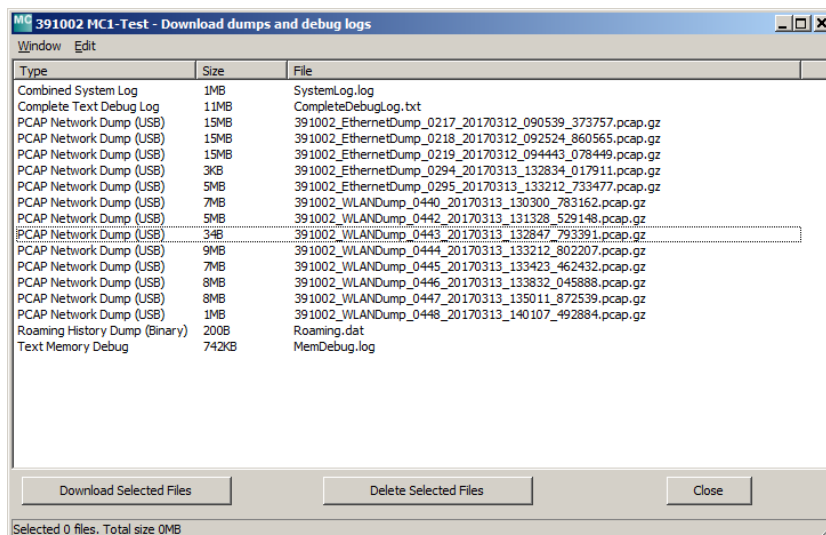


Abbildung 5.14: Dateiauswahl zum Herunterladen oder zum Löschen

In dieser Auswahl wird immer die Datei „SystemLog.log“ aufgeführt, die viele Informationen zum aktuellen Status des MC's mit den letzten Systemmeldungen und den aktuellen Configdaten beinhaltet.

Diese Datei ist immer wichtig wenn es um die Analyse von Fehlersituationen geht.

Die Datei „CompleteDebugLog.txt“ enthält die Systemmeldungen, die während des Betriebs abhängig von den Einstellungen die unter „Logging“ gemacht wurden, entstanden sind. Diese Datei wird bis zu einer Länge von 16MByte aufgefüllt. Wenn diese Größe erreicht ist, wird sie in „CompleteOldDebugLog.txt“ umbenannt. Eine schon vorhandene

„CompleteOldDebugLog.txt“ Datei wird vorher gelöscht.

Weitere Systemmeldungen werden dann in eine neu erzeugte „ CompleteDebugLog.txt“ geschrieben.

Die Dump-Dateien werden in der Reihenfolge wie sie geschrieben wurden aufgelistet. Zuerst die LAN-Dump-Dateien dann die WLAN-Dump-Dateien. Sofern ein Zeitserver (--> „Realtime Clock“) genutzt werden konnte, taucht in den Dateinamen der Dump-Dateien das Datum und die Uhrzeit des Startzeitpunkts auf. Das ist sehr hilfreich, wenn man damit genau die Datei auswählen kann, die den aufgetretenen Fehlers dokumentiert haben könnte.

Der Dateiname setzt sich wie folgt zusammen:

Element	Bedeutung	Anmerkung
nnnnn_	Seriennr. des MC-Geräts	
WLAN(Ethernet)Dump		
xxxx	Nummerierung der Datei	Das ist wichtig, wenn kein Zeitserver eingerichtet ist und der MC zwischendurch neu startet.
YYYYMMDD	Datum der Aufzeichnung	Ohne Realtime Clock startet der MC mit dem Datum 01.01.2000
_hhmmss_uuuuuu	Zeitpunkt des Starts	Angabe von Stunde-Minute-Sekunde-Microsekunde Ohne Realtime Clock startet die Uhrzeit bei 00.00.00_000000

Aus dieser Liste kann man eine oder mehrere Dateien markieren und diese entweder herunterladen oder auch löschen.

Es werden sowohl Log- und Dump-Dateien in der Liste gezeigt, die im internen Flash als auch im evt. aufgesteckten USB-Stick gespeichert sind. Dateien auf dem USB-Stick werden mit „(USB)“ gekennzeichnet.

5.11.1.5 Debug Configurations

Hiermit kann man für die verschiedenen Programmteile die Intensität der Systemmeldungen definieren. Im Programm sind Meldungen eingebettet, die mit einem bestimmten Debug-Level gekennzeichnet sind.

Folgende Debug-Level sind definiert:

Level	Funktion
ERROR	Auftreten eines Fehlers, der eine gewünschte Funktion verhindert.
WARN	Auftreten einer Bedingung, die eine gewünschte Funktion verzögert
INFO	Meldung, die ein auftretendes Ereignis dokumentiert
TRACE	Meldung, die den Ablauf einer Funktion dokumentiert

Für folgende Programmteile können individuell Debug-Level eingestellt werden:

Modul	Funktion
Wireless	Meldet Vorgänge im Zusammenhang mit der WLAN-Schnittstelle. Der Schwerpunkt ist dabei auf das Erfassen der Access Points und die Roamingvorgänge gelegt.
WPA Supplicant	Hier können Vorgänge bei der Authentifizierung dokumentiert werden.
DHCP	Meldungen, die der DHCP-Client oder -Server generiert
Serial	Meldungen, die das Modul zur Ansteuerung der seriellen Schnittstelle generiert
Relay	Meldungen, die das Modul zur Ansteuerung des Relais generiert
Aux-Input	Meldungen, die das Modul zur Ansteuerung des Digitaleingangs generiert
Base System	Meldungen, die das allgemeine Betriebssystem generiert

Network Bridge	Meldungen, die das Bridge-Module generiert.
----------------	---

Die einzelnen Programmteile haben 4 Debug-Level:

Level	Ausgegebene Meldungen
Default	ERROR
Information	ERROR + WARN
Detailed	ERROR + WARN + INFO
Maximum	ERROR + WARN + INFO + TRACE

Das Level „Maximum“ sollte wirklich nur für das Programm-Modul aktiviert werden, bei dem auch ein Problem besteht. Dieses Level kann unter Umständen eine so große Anzahl von Debugmeldungen generieren, dass die Performance der primären Anwendung darunter leidet.

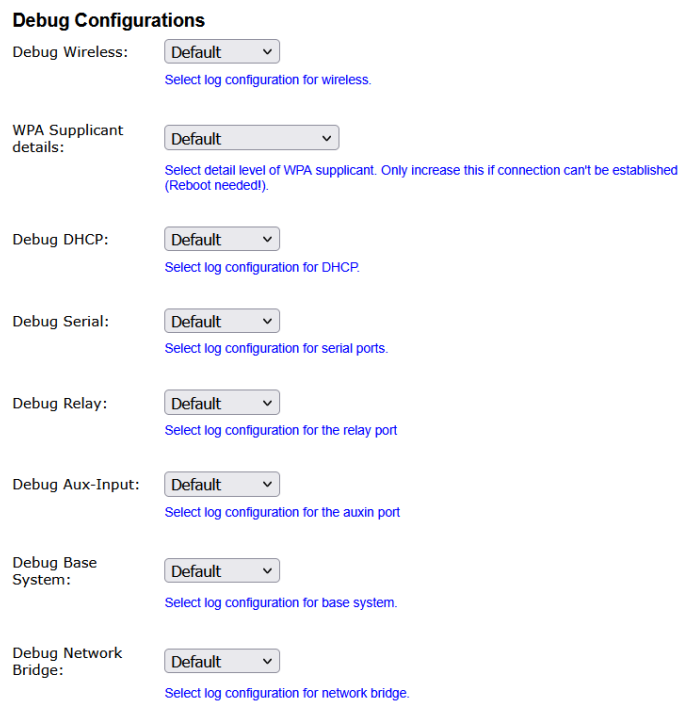


Abbildung 5.15: Debug Configurations

6 Systemmeldungen: Statistics Menü

Unter diesem Menüpunkt findet man Möglichkeiten, die Aktivität des MC bezüglich der LAN + WLAN Schnittstelle zu bewerten und gespeicherte Systemmeldungen dazustellen und zu speichern.

6.1 Statistics - System Log

Unter diesem Menüpunkt werden die Systemmeldungen dargestellt, die im MC gespeichert sind. Welche Meldungen gespeichert werden hängt von den Einstellungen unter „Configuration->Logging“ ab. Dort kann man die „Intensität“ der Ausgabe für einige Software-Module getrennt justieren.

Die Taste „Download System Log“ bewirkt, dass die letzten Meldungen und die aktuelle Konfiguration in einer Datei zusammengefasst und vom MC heruntergeladen werden.

Die Taste „Reset System Log“ löscht alle Meldungen und ggf. auch die Dateien, die beim Mitschnitt des Datenverkehrs auf der WLAN bzw. LAN-Schnittstelle entstanden sind.

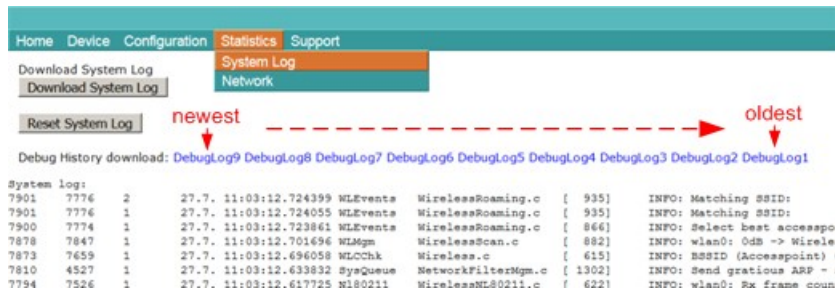


Abbildung 6.1: Beispiel einer System Log Ausgabe

Ab Firmware 2.11p wird unter „Debug history download“ eine Liste mit Links angezeigt. Über diese Links können die DebugLog-Dateien vom MC-Gerät heruntergeladen werden. Der erste Link (newest) zeigt auf die aktuelle DebugLog.dat Datei. Dies ist eine unkomprimierte Textdatei. Die folgenden Links zeigen auf ältere Aufzeichnungen, die als komprimierte Dateien gespeichert sind. Diese Dateien haben folgende Namen:
 DebugLog.dat.xxxxx.old.gz
 xxxxx ist eine von links nach rechts abwärts zählende Nummerierung.

6.2 Statistics - Network

Dieses Untermenü zeigt Statistiken der Netzwerkschnittstellen. Unter „Network Interface eth0“ werden statistische Angaben für die LAN-Schnittstelle des MC gemacht. Das gleiche für die WLAN-Schnittstelle findet man unter „Network Interface wlan0“
 „Network State Information“ zeigt welche Ports auf dem MC geöffnet sind und welche Verbindungen aktuell bestehen.

Network Interface eth0

Tx KBytes	14
Tx Frames	240
Rx KBytes	34
Rx Frames	130
Tx KBytes/Sec	0
Rx KBytes/Sec	0



Network Interface wlan0

Tx KBytes	704
Tx Frames	2819
Rx KBytes	17976
Rx Frames	13235
Tx KBytes/Sec	12
Rx KBytes/Sec	299



Network State Information

Local Port Entry 1	TCP 17784 (UCP)
Local Port Entry 2	UDP 17784 (UCP)
Local Port Entry 3	UDP 68 (DHCP)
Local Port Entry 4	TCP 17785 (Debug TCP Dump)
Local Port Entry 5	UDP 162 (SNMPTrap)
Local Port Entry 6	UDP 161 (SNMP)
Local Port Entry 7	TCP 80 (Webserver)
Local Port Entry 8	UDP 9000 (Relay)

Abbildung 6.2: Beispiel einer Statistics Network Ausgabe

7 Konfiguration der MC-Geräte mit einem USB-Speicherstick

Ab Firmware 2.12a gibt es 2 Möglichkeiten einen USB-Stick zur Konfiguration des MC zu benutzen:

1. Übertragung einer Konfigurationsdatei vom USB-Stick auf das MC Gerät bei einem „Default-Reset“, der mit dem Resettaster initiiert wird.
2. Ständig eingesteckter USB-Stick auf dem sowohl die Konfiguration und ggf. auch die Firmware für ein MC Gerät gehalten wird (**wird nicht mehr unterstützt ab Firmware 2.15.1**) .

7.1 Übertragung einer Konfigurationsdatei bei einem „Default-Reset“

Wenn ein „Default-Reset“ über den **Resettaster** durchgeführt wird, prüft der MC ob ein USB-Stick vorhanden ist. Wenn ja, wird im Root-Verzeichnis des USB-Sticks nach einer Datei „Default.cfg“ gesucht. Sofern diese Datei vorhanden ist, wird diese Konfiguration nach dem Neustart für das MC-Gerät übernommen.

7.2 Anwendung für den Config-USB-Stick

 **Diese Funktion wird ab der Firmware 2.15.1 nicht mehr unterstützt. Vorgaben der EN18031 (RED-DA) werden mit dieser Funktion verletzt!**

Es ist möglich, USB-Speichersticks so zu präparieren, dass diese beim Bootvorgang von dem MC als USB-Config-Stick erkannt werden. Auf dem USB-Config-Stick ist eine Config-Datei mit einem kompletten Setup und ggf. auch eine Datei mit einer bestimmten Firmware für den MC abgelegt.

Ziel ist es, ein defektes MC-Gerät schnell ohne Konfigurationsaufwand durch ein anderes MC-Gerät zu ersetzen, indem man einfach den USB-Config-Stick vom defekten MC-Gerät in das Ersatzgerät steckt. Der Ersatz-MC prüft beim Bootvorgang ob sich auf dem Stick eine Firmwaredatei befindet, die sich von der Firmware im Ersatz-MC unterscheidet. Wenn dem so ist, wird die Firmware vom Stick zunächst in den Ersatz-MC übertragen und geflasht. Nach dem Reboot wird die Config-Datei des USB-Config-Stick für den weiteren Betrieb verwendet. Der Ersatz-MC wird also nach dem Austausch exakt mit der gleichen Firmware und der gleichen Konfiguration wie der Original-MC arbeiten.

7.2.1 Initialisierung eines USB-Speichersticks

Die Initialisierung des USB-Speichersticks erfolgt über das MC-Config-Programm. Diese Funktion wird durch einen Parameter freigeschaltet, der als Argument beim Start des MC-Config-Programms angegeben wird. Dieses Argument lautet: InitUsbConfigStick (Groß- und Kleinschreibung beachten!)

Damit taucht eine zusätzliche Auswahl „Init USB Config Stick“ im Kontextmenü auf.

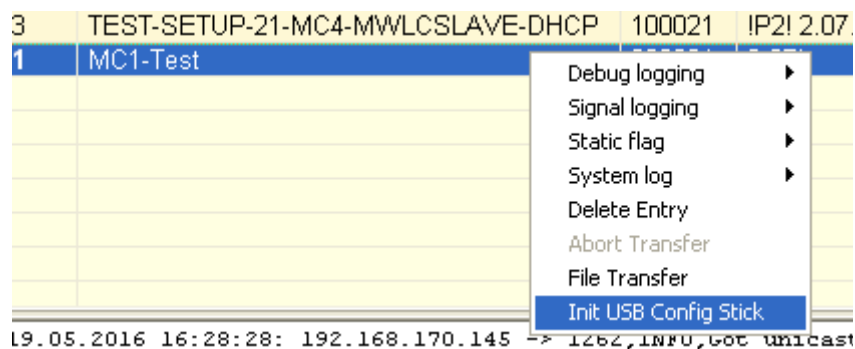


Abbildung 7.1: Init USB Config Stick

 **Achtung!** Bei der Initialisierung des USB-Speichersticks werden alle Daten auf dem Stick gelöscht!

Dieses Kommando **formatiert** den USB-Speicherstick neu (Ext4-Format) und legt dort bestimmte Dateien an, die diesen speziellen Stick als Config-Stick erkennbar machen. Eine dieser Dateien ist die aktuell auf dem MC Gerät vorhandene Config-Datei. Nach der Übertragung der Dateien wird der MC neu gestartet. Beim Bootvorgang wird dieser Stick dann als Config-Stick erkannt und die dort abgelegte Config-Datei wird für den weiteren Betrieb verwendet.

Es ist so gedacht, dass der USB-Stick immer am MC-Gerät eingesteckt bleibt. Dadurch ist sichergestellt, dass eine Änderung der Konfiguration im Config-Stick stattfindet ebenso wie eine Änderung der MC-Firmware auch im USB-Stick

abgelegt wird. Somit wird ein anderes MC-Gerät, dass mit diesem Config-Stick gestartet wird, die gleiche Funktion wie das MC-Gerät haben, von dem der Config-Stick abgezogen wurde.

Wird der USB-Stick entfernt, macht der MC sehr bald darauf einen Reset. Der folgende Bootvorgang wird gestoppt, bis ein Config-USB-Speicherstick erkannt wird. Bis dahin bleibt der MC blockiert. Dieser Zustand wird mit einem blauen Flackern der Power-LED signalisiert. Möchte man den MC wieder ohne USB-Config-Stick betreiben, muss man den MC über den Resetbutton zunächst auf „Factory-Default“ setzen (2.2).

8 REST-API

Ab der Firmware 2.12p ist es möglich, per HTTP(S) mit GET und POST folgende Funktionen durchzuführen:

- 1) Download der Config-Datei
- 2) Upload einer Config-Datei
- 3) Upload einer Firmware
- 4) Statusabfrage
- 5) Zertifikats-Upload
- 6) Download der WLAN + LAN - Mitschnitte ((W)LAN-Dump-Dateien)
- 7) Download der Systemlog-Datei
- 8) Download des CA-Zertifikats vom OpenVPN-Server
- 9) Download einer Konfigurationsdatei für einen OpenVPN-Client

Funktion	URL	Methode	Ergebnis
Download der aktiven Config-Datei	http(s)://<MC_IP>/API/Cfg/GetRunning	GET	Text
Download der Default-Config-Datei	http(s)://<MC_IP>/API/Cfg/GetDefault	GET	Text
Upload einer Config-Datei	http(s)://<MC_IP>/API/Cfg/Set	POST	
Upload einer Firmware-Datei	http(s)://<MC_IP>/API/Firmware/Upgrade	POST	
Statusabfrage (siehe unten)	http(s)://<MC_IP>/API/Status	GET	JSON
Upload eines Zertifikats	http(s)://<MC_IP>/API/Cfg/ImportCertificate	POST	
Download der Dateiliste der vorhandenen WLAN+LAN+Mitschnitte	http(s)://<MC_IP>/API/Debug/CaptureFiles	GET	JSON
Download einer Datei	http(s)://<MC_IP>/API/Debug/CaptureFile/<FileName>	GET	Binär
Download der Systemlog-Datei	http(s)://<MC_IP>/API/Debug/Get/SystemLog	GET	Text
Download des CA-Zertifikats vom VPN-Server	http(s)://<MC_IP>/API/OpenVPNServer/GetCACert	GET	Text
Download der Konfigurationsdatei für den VPN-Client	http(s)://<MC_IP>/API/OpenVPNServer/GetClientConfig	GET	Text

Statusabfrage

Die Abfrage „http(s)://<MC_IP>/API/Status“ liefert aktuell Informationen die in folgenden Segmenten aufgeteilt sind:

Segment	Info	Elemente
Device	Geräteinformationen	Seriennr, Firmwareversion, Uptime, LinuxVers, WLAN-Hardware
Network	Infos zu den LAN-Port(s)	Link-Status (up / down)

CertInfo	(wenn vorhanden) Infos zu den geladenen Zertifikaten	Gültigkeitszeitraum, Zertifikats-Info,...
Wireless	WLAN-Schnittstelle	Accesspoints-Liste, Status der WLAN-Verbindung, Infos zu den WLAN-Funkkanälen
Input	AUX-IN digitaler Eingang	Status, Mode ...
Relay	Relais Schnittstelle	Status (ON-OFF), Mode
Serial	Serielle Schnittstelle	Mode, Format, Status, RX-Tx-Statistik
MQTT	MQTT-Clients	Wenn aktiviert

Diese Statuswerte lassen sich auch einzeln abrufen, indem man genau das gewünschte Element adressiert:

z.B.: „[http\(s\)://<MC_IP>/API/Status/Network/LAN/Port/0/State](http(s)://<MC_IP>/API/Status/Network/LAN/Port/0/State)“ = Linkstatus LAN-Port 1

liefert die Info „up“ oder „down“

oder „[http\(s\)://<MC_IP>/API/Status/Wireless/Connection/Connected](http(s)://<MC_IP>/API/Status/Wireless/Connection/Connected)“

liefert die Info „true“ oder „false“

REST-API Abfragen mit curl

Mit dem Befehlszeilentool „curl“ kann man die Funktionen der REST-API per Script automatisch oder über die Kommandozeile auslösen. „curl“ verarbeitet auch die Übergabe der evt. gesetzten User/Passwort Angaben.

So würden die Kommandozeilen für die verschiedenen Funktionen aussehen:

Funktion	Kommando
Cfg/GetRunning	<code>curl -N -u user:password -k --output <destination file > "https://<MC_IP>/API/Cfg/GetRunning"</code>
Cfg/GetDefault	<code>curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Cfg/GetDefault"</code>
Cfg/Set	<code>curl -N -u user:password -k -X POST -F "image=@<config file>" "https://<MC_IP>/API/Cfg/Set"</code>
Firmware Upgrade	<code>curl -N -u user:password -k -X POST -F "image=@<firmware file>" "https://<MC_IP>/API/Firmware/Upgrade"</code>
Status	<code>curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Status"</code>
Cfg/ImportCertificate	<code>curl -N -u user:password -k -X POST -H "Content-Type: multipart/form-data" -F "CertData=@<CertFile>" -F "Type=WEB" -F "Command=Import" -F "Password=<Password>" "https://<MC_IP>/API/Cfg/ImportCertificate"</code>
Debug/CaptureFiles	<code>curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Debug/CaptureFiles"</code>
Debug/CaptureFile	<code>curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Debug/CaptureFile/<FileName>"</code>
Debug/Get/SystemLog	<code>curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Debug/Get/SystemLog"</code>
VPNServer / GetCACert	<code>curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/OpenVPNServer/GetCACert"</code>
VPNServer / GetClientConfig	<code>curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/OpenVPNServer/GetClientConfig"</code>

mit der „Cfg/Set“ Funktion können auch Config-Dateien mit nur einzelnen Parametern übertragen werden.

Wenn z.B. eine Datei mit dem Inhalt:

```
[Wireless]
Enabled=false
```

übertragen wird, schaltet der MC die WLAN-Schnittstelle aus.

Eine Datei mit dem Inhalt:

```
[Wireless]  
Enabled=true
```

schaltet die WLAN-Schnittstelle wieder ein.

Weitere Informationen über das curl Tool finden Sie unter: <https://curl.haxx.se/>

9 Open Source Compliance Information

Version: MC WLAN Client Adapter

To whom it may concern,

Written Offer

This product contains software whose rightholders license it under the terms of the GNU General Public License, version 2 (GPLv2), version 3 (GPLv3) and/or other open source software licenses. If you want to receive the complete corresponding source code we will provide you and any third party with the source code of the software licensed under an open source software license if you send us a written request by mail or email to the following addresses:

Email: modas oss support team: opensource@modas.de

Postal:

modas mobile Datensysteme GmbH
Belziger Str, 69-71
10823 Berlin/Germany

detailing the name of the product and the firmware version for which you want the source code and indicating how we can contact you.

PLEASE NOTE THAT WE WILL ASK YOU TO PAY US FOR THE COSTS OF A DATA CARRIER AND THE POSTAL CHARGES TO SEND THE DATA CARRIER TO YOU. THE AMOUNT CAN BE VARIED ACCORDING TO YOUR LOCATION AND MODAS OSS SUPPORT TEAM WILL NOTIFY THE EXACT COST WHEN RECEIVING THE REQUEST. THIS OFFER IS VALID FOR THREE YEARS FROM THE MOMENT WE DISTRIBUTED THE PRODUCT AND VALID FOR AS LONG AS WE OFFER SPARE PARTS OR CUSTOMER SUPPORT FOR THAT PRODUCT MODEL.

FOR MORE INFORMATION SEE ALSO:

<http://download.modas.com/Source>