

MC

802.11 a/b/g/n

Wireless LAN-Bridge
&
Serial Client Adapter

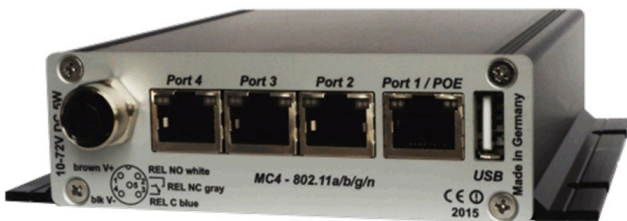
Manual



MC1



MC2



MC4



Table of Contents

1	Technical Description.....	5
1.1	Ports of the MC1.....	6
1.2	Ports of the MC2.....	7
1.3	Ports of the MC4.....	8
1.4	Meaning of the LEDs.....	8
1.5	Technical Properties.....	9
1.6	Wireless LAN – Interface.....	9
2	Initial setup.....	10
2.1	Setup of the MC.....	10
2.1.1	Setup with the MC-Config program.....	10
2.1.2	Startup via the MC WEB-Interface.....	12
2.2	Reset to factory settings.....	12
3	MC Web interface information page.....	13
3.1	System Information.....	13
3.2	Wireless Status Information.....	13
3.3	Wired LAN Status Information.....	16
3.4	Serial1.....	16
3.5	Relay Status Information (Optional).....	17
3.6	Network Information.....	17
3.7	Access point list.....	18
3.8	HTTPS Webinterface.....	18
3.9	Storage Status Information.....	19
3.10	WLAN und LAN-Dump-Dateien.....	19
4	Firmware and configuration management: Device Menu.....	20
4.1	Firmware.....	20
4.2	Configuration Management.....	21
4.3	Network Test.....	22
5	Configuration.....	23
5.1	Admin.....	24
5.2	Network.....	25
5.2.1	IP Address.....	25
5.2.2	Bridge.....	26
5.2.2.1	Bridge-Mode OFF.....	26
5.2.2.2	LAN-Client-Cloning.....	27
5.2.2.3	NAT and Single Client NAT.....	28
5.2.2.3.1	Forwarding rules for NAT.....	30
5.2.2.3.2	DHCP-Server.....	30
5.2.2.3.3	Static DHCP Server entries.....	31
5.2.2.4	Level 2 Pseudo-Bridge Mode.....	32
5.2.2.5	MWLC Mode.....	34
5.2.2.5.1	MWLC-Master.....	35
5.2.2.5.2	MWLC-Slave.....	35
5.2.3	Bridge not active Mode.....	36
5.2.4	MQTT Client.....	37
5.3	Wireless.....	39
5.3.1	Main Parameter.....	40
5.3.1.1	Wireless Mode.....	40
5.3.1.2	SSID-Profiles.....	40
5.3.1.3	Phy Mode.....	40
5.3.1.4	Country selection.....	40
5.3.1.5	Enable sleep mode.....	40
5.3.1.6	802.11bg bitrate setting.....	40
5.3.1.7	802.11a bitrate setting.....	40
5.3.1.8	Power selection.....	40
5.3.1.9	Antenna gain.....	40
5.3.1.10	Antenna selection.....	40
5.3.1.11	Filter SSID.....	40
5.3.1.12	Wireless Status Information Service.....	41
5.3.2	SSID Profile.....	41

5.3.2.1	SSID Profile.....	41
5.3.2.2	Profile change action.....	41
5.3.2.3	Connect Action.....	42
5.3.2.4	Security Parameter.....	42
5.3.2.5	EAP.....	43
5.3.2.6	Certificates.....	44
5.3.3	SCEP.....	44
5.3.4	Roaming.....	44
5.3.4.1	Roaming Parameter.....	44
5.3.4.1.1	AP Density.....	44
5.3.4.1.2	Channels for Roaming.....	45
5.3.4.1.3	Min scan interval.....	45
5.3.4.1.4	Max scan interval.....	45
5.3.4.1.5	AP Scoring.....	45
5.3.4.1.6	Blacklist Timer.....	45
5.3.4.2	Background Scanning.....	45
5.3.4.3	Connection Watchdog.....	46
5.3.4.4	Ping-Test.....	46
5.3.4.5	Preferred / avoided access points.....	47
5.4	Function of the serial interface.....	48
5.4.1	Parameter of the serial interface.....	48
5.4.2	Network-Configuration Parameter.....	49
5.4.3	„Keep alive“-Parameter.....	49
5.4.4	„Handshake-Mode“ Parameter.....	49
5.4.5	Enable dump.....	50
5.5	Printer server configuration.....	50
5.6	Relay Configuration.....	50
5.6.1	Delayed switching on and off of the relay.....	51
5.7	Realtime Clock Configuration.....	51
5.8	Input Configuration.....	52
5.8.1	Input query in UDP mode.....	52
5.9	Logging Configuration.....	53
5.9.1	Logging system messages.....	53
5.9.1.1	Debug Log.....	53
5.9.1.2	Debug Information.....	53
5.9.1.3	Syslog Server.....	54
5.9.1.4	Traffic Dump Configuration.....	55
5.9.1.4.1	Downloading Debug Files with the MC-Config Program.....	57
5.9.1.5	Debug Configurations.....	58
6	Statistics Menu.....	60
6.1	Statistics - System Log.....	60
6.2	Statistics - Network.....	61
7	Configuration of MC devices with an USB memory stick.....	62
7.1	Transfer of a configuration file during a "default reset".....	62
7.2	Application for the Config-USB-Stick.....	62
7.2.1	Initializing a USB memory stick.....	62
8	REST-API.....	63
9	Open Source Compliance Information.....	65
10	Statements and instructions according to FCC and Industry Canada Rules.....	66
10.1	Information for host integrators of the radio module.....	66
10.1.1	Labeling instructions for host devices.....	66
10.1.2	RF Exposure / collocation requirements.....	66
10.1.3	Information to end user.....	66
10.2	FCC and Industry Canada warning statements and special instructions.....	66

Table of Figures

Figure 1.1: Overall System (example).....	5
Figure 1.2: Ports and LED's of the MC1-SL-M12.....	6
Figure 1.3: WK8 power connector (with relay + digital input).....	7
Figure 1.4: M8 power connector with optional M8 connector for one relay and digital input.....	7
Figure 1.5: MC2 plug assembly on the back panel.....	7
Figure 1.6: MC4 plug assembly on the back panel.....	8
Figure 2.1: Setting for the initial configure of the MC.....	10
Figure 2.2: Initial setup with the MCConfig program.....	11
Figure 2.3: Screenshot of the MC-Config program.....	11
Figure 3.1: Access point list.....	18
Figure 3.2: Storage Status Information.....	19
Figure 3.3: WLAN- and LAN-Dump files.....	20
Figure 4.1: Firmware Update Dialog.....	20
Figure 4.2: Configuration Management.....	21
Figure 4.3: Network Test.....	22
Figure 5.1: LAN Client Cloning Mode.....	28
Figure 5.2: NAT-Mode (sample configuration).....	28
Figure 5.3: Level 2 Bridge (sample configuration).....	32
Figure 5.4: MWLC-Mode sample configuration.....	34
Figure 5.5: Parameters for the ping test function.....	47
Figure 5.6: Preferred or avoided AP list.....	48
Figure 5.7: Debug Log Parameter.....	54
Figure 5.8: Traffic Dump Configuration.....	55
Figure 5.9: Wireless und Ethernet dump files.....	57
Figure 5.10: Download Dumps and Logs with the MC-Config-Program.....	57
Figure 5.11: File selection for download or deletion.....	58
Figure 5.12: Debug Configurations.....	60
Figure 6.1: Example of a System Log Output.....	60
Figure 6.2: Example of an Statistics Network Screen.....	61
Figure 7.1: Init USB Config Stick.....	62

1 Technical Description

The MC is a WLAN adapter for connecting devices with Ethernet, USB or serial interfaces to 802.11 a/b/g/n wireless networks. The MC connects all devices of the LAN segment to which it is connected to a network accessible via WLAN via the Ethernet interface.

Via the serial interface, the MC can receive and send data that is sent or received by a communication partner connected via the network (WLAN or LAN). This communication partner can be an MC or a computer that receives or sends this data via a suitable application. Among other things, printers can be connected via the USB interface. The MC can work as a print server. The USB port can also be used for extensions, e.g. to provide additional serial or I/O interfaces.

The different device variants MC1, MC2 and MC4 differ essentially in the number of LAN ports. The MC4 has no RS232 connection. All variants work with the same firmware.

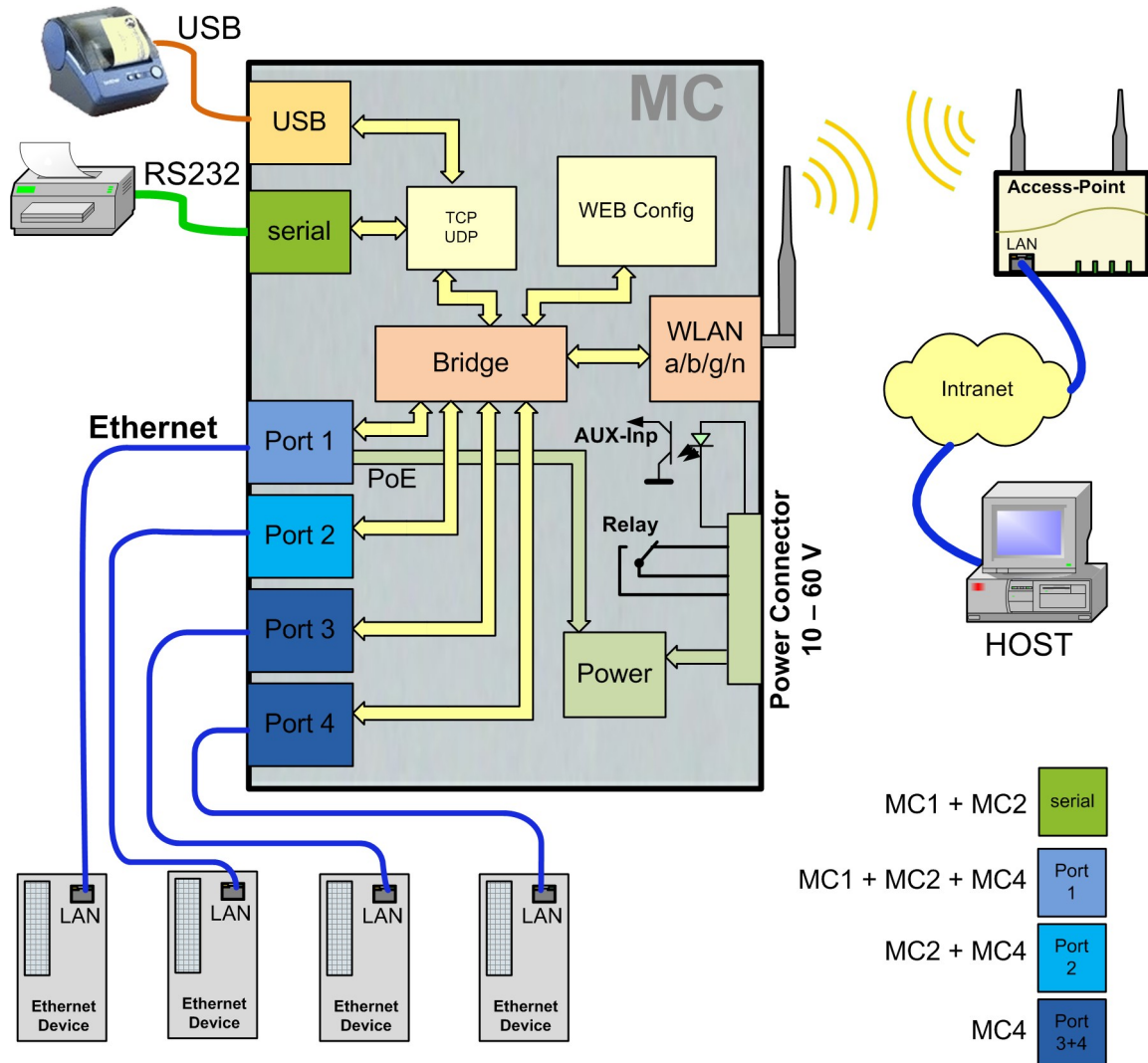


Figure 1.1: Overall System (example)

The central component of the MC is an ARM® Cortex®-A9 processor, which controls all functions. The interfaces are:

- 1) Mini-PCI-Express Socket
- 2) Ethernet-Interface with 1-4 Ports 10/100/1000 Mbit/s + Auto-MDIX (auto crossover function)
- 3) 1 x serial Port with six control lines (RTS, CTS, DTR, DSR, DCD, RI)
- 4) 1 x USB2 – Port e.g. for printers or port extensions
- 5) optional: relay switching contact + input with opto coupler

The Ethernet connection is designed as an RJ45 plug. LAN port 1 has a PoE function (IEEE 802.3af), so that the MC can be powered via this port.

The serial interface is connected via a 9pin. D-SUB plug. The PIN assignment is selected so that it can be connected to the COM port of a PC via a 1 to 1 serial cable. The exact assignment can be seen in Figure 2.

For power supply the MC requires a voltage source in the range between 10-60V. The typical power consumption is approx. 3.0 watts (WLAN + LAN port active)

1.1 Ports of the MC1

The following figures show how the LEDs and ports of the MC are arranged.

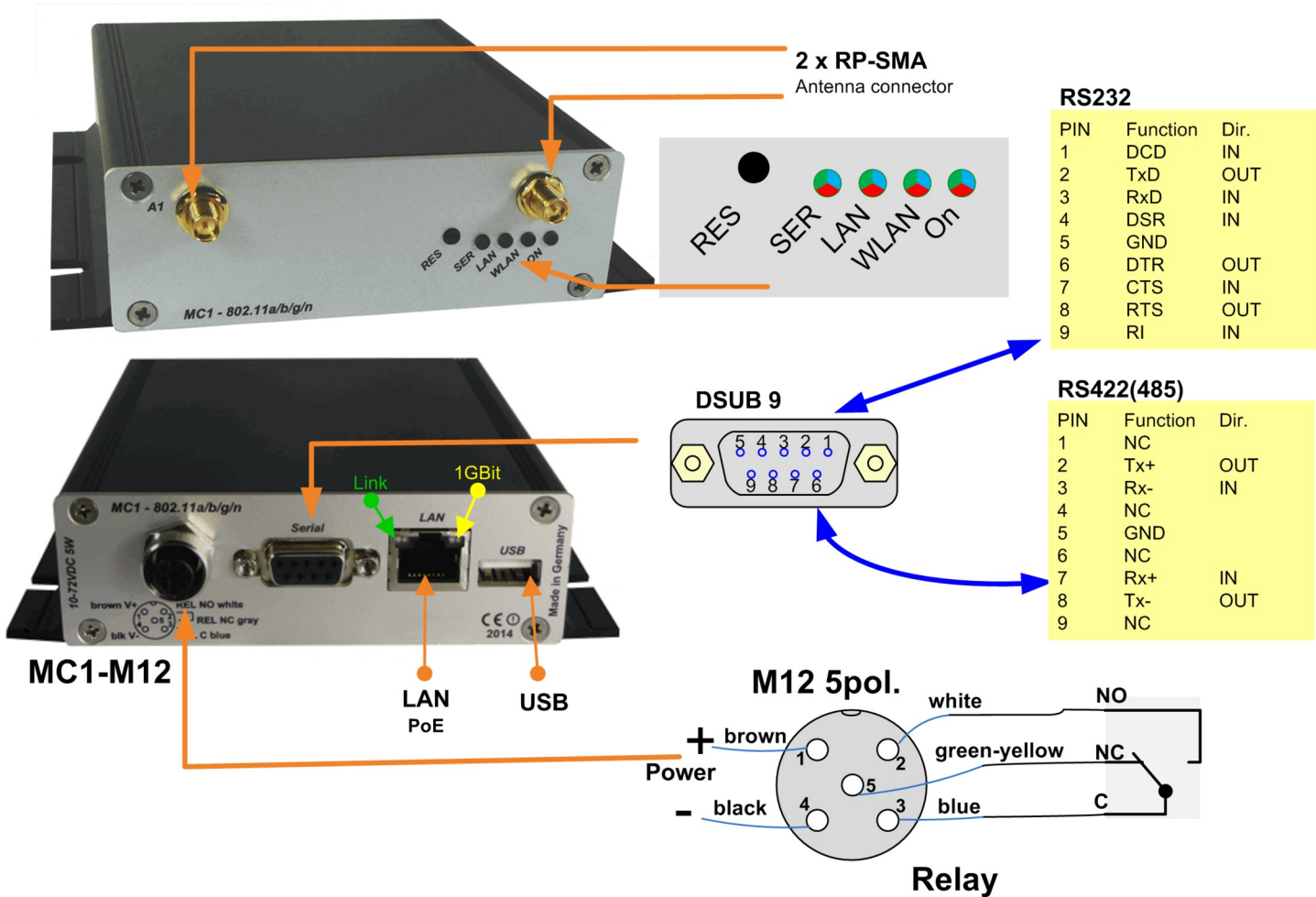
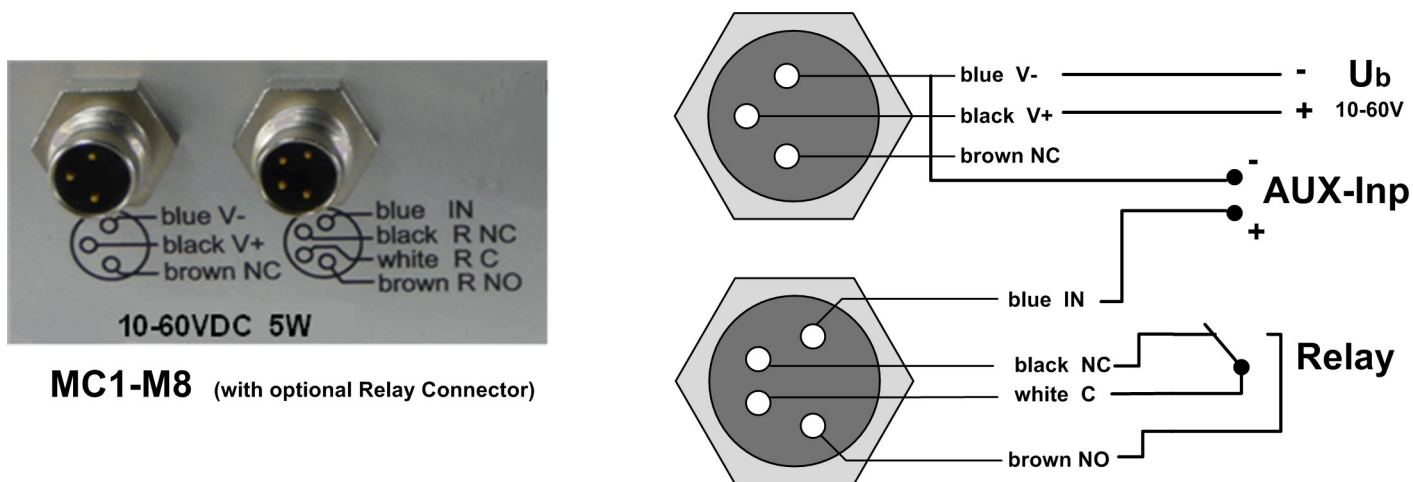
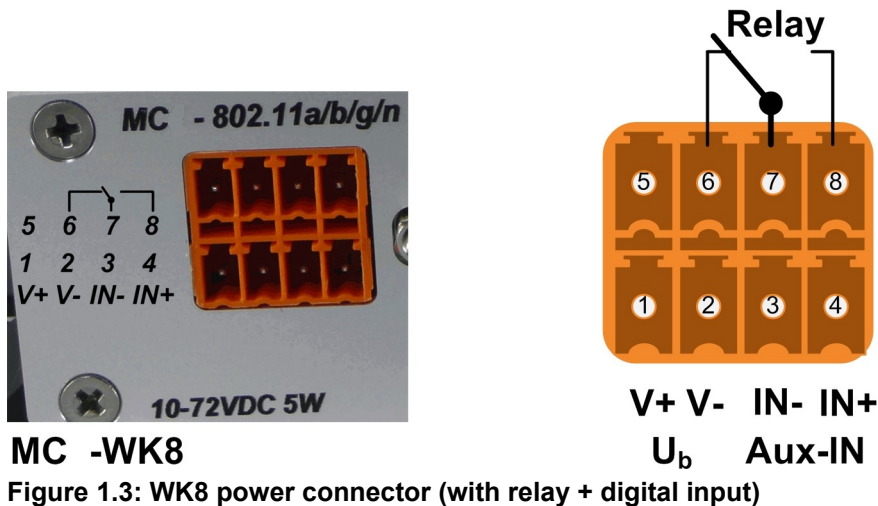


Figure 1.2: Ports and LED's of the MC1-SL-M12

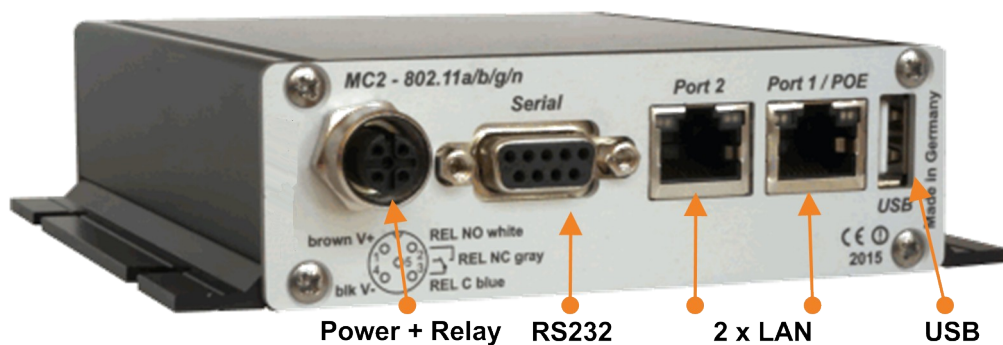
Figure Fehler: Verweis nicht gefunden shows the MC1 in its standard design with one serial Port, a 5pin M12 connector for power supply and a relay switching contact.

There are different option for the power connector of the MC devices:



1.2 Ports of the MC2

The front panel of the MC2 is identical to the MC1.
The MC2 back panel has the following plug assembly:



The MC2 is also available with the options MC2-Sx-**WK8** and MC2-Sx-**M8**.

1.3 Ports of the MC4

The front panel of the MC2 is identical to the MC1.
The MC4 back panel has the following plug assembly:

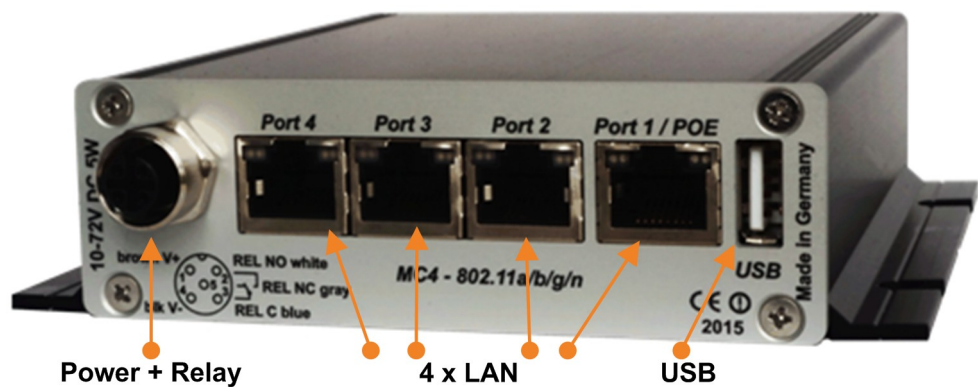


Figure 1.6: MC4 plug assembly on the back panel

The MC4 is also available with the options MC4-Sx-**WK8** and MC4-Sx-**M8**.

1.4 Meaning of the LEDs

The 4 LEDs on the front represent the operating state of the MC. All LEDs can shine in three different colors: red, yellow, blue. If all three colors are on, the LEDs color is white.
All 4 LEDs light up white once after switching on or after a reset. If the LEDs WLAN + LAN + SER flash blue, either a new firmware is flashing or a new configuration is activated.

LED	State	Mode
On	Off	No or not enough power
	Green	Sufficient voltage connected
	Green + blinking orange (red & green)	Standard mode MC ready
	bright blue flickering	The MC device has previously worked with a USB config stick and is now waiting for this stick to be plugged in again. --> 7.2.1
WLAN	Off	WLAN option off
	Blinking red	MC is looking for suitable APs or is currently authenticating
	Green	Wireless LAN connection works. Short orange blinking shows activity (sending or receiving of data)
LAN	Off	No device connected to the LAN-Port
	Green	Device connected to LAN-Port. Short orange blinking shows activity (sending or receiving of data) at the interface.
Serial	Off	The interface is inactive.

TCP-Mode	Green or Blinking orange	A partner-device is connected to the interface. Short orange blinking shows activity (sending or receiving of data) at the interface.
	Blinking green	The interface is in TCP-Server-Mode and awaits a connection.
	Blinking red	The interface is in TCP-Client-Mode and is trying to establish a connection to the configured server.
Serial UDP-Mode	Off	The interface is inactive.
	Green	The interface is initialized and ready to receive or transmit data.
	Green and blinking white	White blinking shows activity (sending or receiving of data). If continuous data is exchanged, the LED light permanently white.

Table 1: LED-Modes

1.5 Technical Properties

Specifications:	
<i>Ethernet</i>	1, 2 or 4 x 10/100/1000 MBit Auto MDI/MDIX
<i>Serial</i>	1 x RS232, 300-460,8 KBit/s, RTS, CTS, DSR, DTR, RI, DCD or (optional) RS485
<i>USB</i>	1 x USB 2.0
<i>Relay</i>	1 x Switch over, max 1A@24V, max 125VAC
<i>Signal Input</i>	1 x galv. separated 10 – 60V
<i>Antenna Connectors</i>	2 x RPSMA (optional TNC or RPTNC)
<i>Power Supply</i>	10 – 60VDC or 802.3af PoE via LAN Port 1
<i>Energy</i>	<= 5W (typically 3W)
<i>Temperature</i>	0-60°
<i>Dimensions</i>	105x125x35mm
<i>Weight</i>	ca. 400g

1.6 Wireless LAN – Interface

Wireless LAN-Interface:	
<i>Technology</i>	802.11 a/b/g/n WLAN (2.4 + 5 GHz Band)
<i>Antennas</i>	2 Antennas (2T2R MIMO)
<i>Encryption</i>	WEP (64, 128bit) + TKIP/AES
<i>Security</i>	802.11i WPA(2)(3) – PSK 802.1x EAP-PEAP, -TLS, -TTLS, -LEAP
<i>Channels</i>	802.11b/g/n ETSI 1-13, USA/Canada 1-11 802.11a/n ETSI 19 + 5, USA/Canada 25 (U-NII-1 + UNII-2A + U-NII-2C+U-NII-3)
<i>Data Rates</i>	ModeData Rate

	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
Transmission Power	802.11b/g 17 dBm	802.11a 15 dBm
	802.11gn 16 dBm	802.11an 15 dBm

Table 2: Properties of the Wireless LAN-Interface

2 Initial setup

Please connect the MC via the Ethernet-Port with a PC using a patch cable for the initial setup.

When turning on power supply voltage, all LEDs briefly blink white. After that only the ON-LED lights up green, which soon starts blinking orange (red & green) and green. After about 15 seconds the application is ready and the LEDs indicate the modes described above.

2.1 Setup of the MC

2.1.1 Setup with the MC-Config program

For its initial setup the MC is only able to communicate via its LAN-Port because typically there is no wireless network with a suitable SSID.

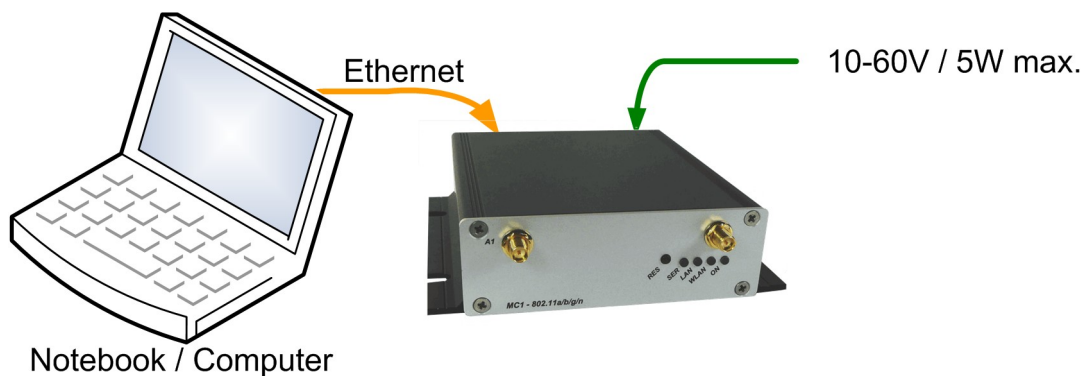


Figure 2.1: Setting for the initial configure of the MC

To do the „first time setup“ the MC has to be connected via the LAN-Interface to the computer (PC) that runs the MC-Config-Program.

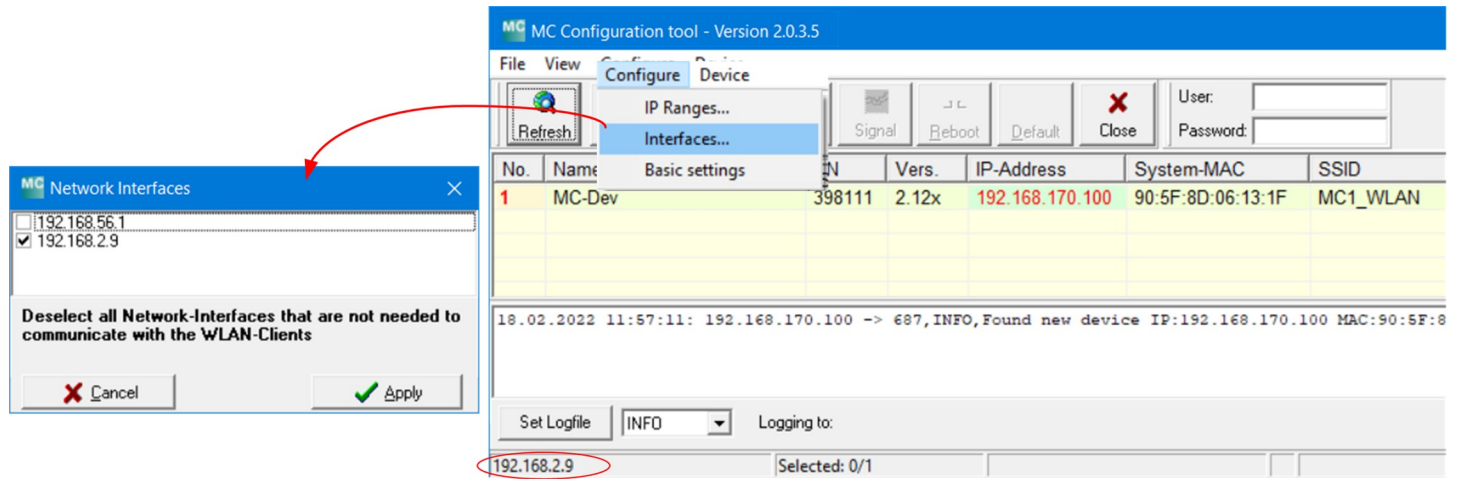


Figure 2.2: Initial setup with the MCConfig program

What to take into account:

- The connected PC (Notebook) should have a fixed IP-Address on its LAN-Port (no DHCP).
- This IP should show up in the status field at the bottom left of the MC-Config program.
- If several IP addresses are listed there, you can specifically activate only the relevant interface with "Configure" → "Interfaces".
- After changing this setup, press the "Refresh" button on the MC-Config program again.
- An active Firewall on the PC might prevent communication with the MC.

After launch, the MC-Config-Application first detects all network interfaces, that are currently active on the PC. A Broadcast-UDP-Request is then sent out to all these interfaces and the MC devices will respond. The responding devices will be registered and listed in the application.

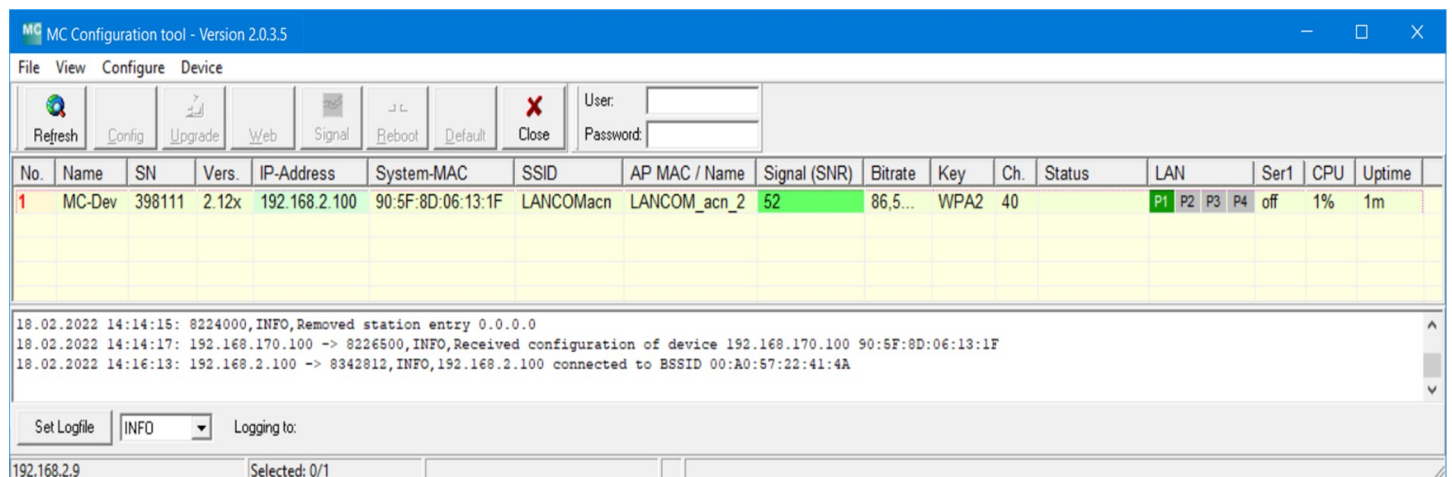


Figure 2.3: Screenshot of the MC-Config program

In addition to the device data such as name, serial number, firmware version, IP address and MAC address, WLAN connection data is also displayed. Initially, you can only see the set SSID. If there is a connection to an access point, the MAC address and, for certain WLAN systems, the name of this AP is also displayed. The signal strength is displayed as SNR value in dBm with a corresponding background color. The SNR values can be interpreted as follows:

- Signal ≥ 40 → Very good connection
- Signal ≥ 30 → Good connection
- Signal ≥ 20 → Connection still sufficient
- Signal < 20 → connection is restricted, the bit rates are reduced to transfer data.

A more detailed description of how to operate the MC-Config program can be found in a separate manual.

2.1.2 Startup via the MC WEB-Interface

If you do not want to or cannot use the MC-Config program, the MC devices can also be put into operation using a WEB browser. To do this, you must set the LAN interface of the startup computer to a fixed IP address. The IP 192.168.170.1 with the subnet mask 255.255.255.0 would be suitable, for example.

If the MC starts with the default setting (see -> 2.2), you can access the home page of the MC by using the WEB browser and entering the address 192.168.170.100. From there you can then make the necessary settings.

2.2 Reset to factory settings

By pressing the reset-button for a long time, the MC can be set back to its factory settings. When keeping the reset button pressed, the MC goes through different sequences that are visualized by all four LEDs lighting up in the same color. The LED-sequences start with lighting up in white, then blue, then red and then green; restarting with white again. Holding the reset button pressed after the third time the all LEDs light up blue, the device is set back to its factory settings. All LEDs are off during the reset to factory settings. After that, the reset button can be released. When the reset button is released before the factory reset was initiated, then the MC needs to be restarted by briefly pressing the reset button again.

The MC can be reset to the factory settings by holding down the reset button. If you press and hold the reset button, the MC runs through sequences which are indicated by changing colors on all 4 LEDs. Starting with white the color changes to blue --> red --> green and then starts again from the beginning with white. When the 3rd time appears blue and you keep pressing the reset button, the settings are reset. All LED's will be switched off. Afterwards the reset button can be released. If the reset button is released before the 3rd "blue phase", the MC must be restarted by shortly pressing the reset button again.

The MC has the following (important) factory settings:

Device Name: „MC-Dev“
SSID = „MC_WLAN“
Encryption mode = no encryption
MODE= 802.11 a/b/g/n (2.4 + 5 GHz)

IP = 192.168.170.100
Netmask = „255.255.255.0“
Gateway = 192.168.170.1

user = „“ (empty)
password = „“ (empty)

Serial 1: inactive
Relay: inactive
Input: inactive

3 MC Web interface information page

After you have connected to the MC's http server via the web browser, a page with information about the MC and the current status of the device is displayed first. This web page can be displayed without querying the values set for "User" + "Password", if applicable.

For all other pages, this information will be queried once, if set.

3.1 System Information

This section contains general information about the device:

Information	Remark
Device Name	This parameter is configured at → Admin and appears in the MC-Config program as the device name.
Uptime	This is the time that has passed since the MC was last switched on or reset
Realtime clock (UTC)	Here the device-internal time is displayed. At the start the MC sets the internal clock to the time: 01.01.2000 at 00:00:00 o'clock. If a time server is configured (Configuration -> Real Time Server) the MC tries to reach it and obtain the UTC information. If this is successful, the MC sets the internal clock accordingly. This time specification is used for debug output.
Serial number	The serial number assigned by the manufacturer.
Firmware Version	The currently installed firmware on the device.
Kernel Version	The operating system of the MC is based on Linux. The version number indicated here indicates the Kernel version, which is merged up-to-date into the firmware. Please pay attention to this note: --> 9

System Information

Device Name	MC-Dev
Uptime	0 Week(s) 0 Day(s) 02:35:26
Realtime clock (UTC)	11.09.2020 12:32:17
Serial number	311284
Firmware Version	2.12r
Kernel Version	Linux version 4.9.223+

3.2 Wireless Status Information

This section contains information about the Wireless LAN state:

Operation Mode	The MC can be used as a client in a Wireless LAN Infrastructure or as a device in Adhoc Mode.
AP Mac Address	This is the MAC-Address of the access point (AP) the MC is connected to. If the AP transmits

(BSSID)	a device name, then the name will also be displayed here.																								
SSID (Network Name)	This is the name of the Wireless LAN network the MC is supposed to or has connected to.																								
Connection state	<p>State of the connection to the AP. The shown status information depends on the configured authentication method:</p> <table border="1"> <tr><td>Idle</td><td>no connection active</td></tr> <tr><td>Disconnected</td><td>previously existing connection was interrupted</td></tr> <tr><td>EAP Success</td><td>completed EAP authentication</td></tr> <tr><td>KeyCompleted</td><td>key exchange completed</td></tr> <tr><td>Connected</td><td>WLAN connection established</td></tr> <tr><td>Authenticate</td><td>Authentication in process</td></tr> <tr><td>Associate</td><td>Association in process</td></tr> <tr><td>Associated</td><td>Association ready</td></tr> <tr><td>EAP Started</td><td>EAP Authentication in process</td></tr> <tr><td>Timeout</td><td>Timeout in EAP Authentication process</td></tr> <tr><td>EAP Failed</td><td>EAP Authentication failed</td></tr> <tr><td>EAP Select Method</td><td>EAP Authentication in process</td></tr> </table>	Idle	no connection active	Disconnected	previously existing connection was interrupted	EAP Success	completed EAP authentication	KeyCompleted	key exchange completed	Connected	WLAN connection established	Authenticate	Authentication in process	Associate	Association in process	Associated	Association ready	EAP Started	EAP Authentication in process	Timeout	Timeout in EAP Authentication process	EAP Failed	EAP Authentication failed	EAP Select Method	EAP Authentication in process
Idle	no connection active																								
Disconnected	previously existing connection was interrupted																								
EAP Success	completed EAP authentication																								
KeyCompleted	key exchange completed																								
Connected	WLAN connection established																								
Authenticate	Authentication in process																								
Associate	Association in process																								
Associated	Association ready																								
EAP Started	EAP Authentication in process																								
Timeout	Timeout in EAP Authentication process																								
EAP Failed	EAP Authentication failed																								
EAP Select Method	EAP Authentication in process																								
Security	Active encryption and authentication method																								
Connection time	Duration of the connection between MC and the current AP																								
Bitrate	The bit rate that is used to send data to the AP.																								
Channel/Frequency	This is the channel number and frequency that is used for the connection to the AP																								

SNR (Signal-to-Noise Ratio)	<p>The SNR can be valued as follows :</p> <table border="1"> <tr><th>SNR</th><th>State</th></tr> <tr><td>>= 40</td><td>very good condition</td></tr> <tr><td>>= 30</td><td>good condition</td></tr> <tr><td>>= 20</td><td>with this SNR the MC will start to scan for APs with a stronger signal</td></tr> <tr><td>>= 10</td><td>weak signal! The MC will frequently scan for APs with a stronger signal. The data throughput will be interfered</td></tr> <tr><td>< 10</td><td>very weak signal. The connection can get lost.</td></tr> <tr><td></td><td></td></tr> </table> <p>Additionally statistical SNR values are displayed: Min xx dB Max yy dB, 24h: Min aa dB Max bb dB xx + yy = minimum and maximum SNR values when connecting to the current AP aa + bb = minimum and maximum SNR values within the last 24 hours</p>	SNR	State	>= 40	very good condition	>= 30	good condition	>= 20	with this SNR the MC will start to scan for APs with a stronger signal	>= 10	weak signal! The MC will frequently scan for APs with a stronger signal. The data throughput will be interfered	< 10	very weak signal. The connection can get lost.		
SNR	State														
>= 40	very good condition														
>= 30	good condition														
>= 20	with this SNR the MC will start to scan for APs with a stronger signal														
>= 10	weak signal! The MC will frequently scan for APs with a stronger signal. The data throughput will be interfered														
< 10	very weak signal. The connection can get lost.														
Signal	Signal level														
Noise	Noise level														
Channel Usage	<p>The radio card provides a value that indicates the utilization of the current channel in %. This value is displayed here in color. Green → low utilization Orange → moderate utilization Red → high utilization</p>														

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	40: 5.200GHz
	46dB (Min 40dB Max 48dB, 24h: Min 23dB Max 48dB)
	
Signal	-49 dBm
Noise	-95 dBm
Channel Usage 5GHz	5%

Table 3: Wireless Status Information

3.3 Wired LAN Status Information

This section shows the current status of the LAN ports

Wired LAN Status Information

LAN link state

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

LAN link state	state of the LAN-Port	Link	down → no LAN cable with an active Ethernet client connected up → LAN cable with an active Ethernet client connected
		Speed	10, 100, 1000 MBit → transfer rate
		Duplex	Half, Full → Simultaneous sending and receiving possible (Full) or not (Half)
		MDI-X	Straight, Cross → MDI-X State

Table 4: Wired LAN Status Information

3.4 Serial1

This section shows the current status of the serial Ports

Serial 1

State	Serial Port is active
Device	/dev/ttymx0
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	Meaning	Comment
State		The port has to be activated.
Device	Device definition	This specification refers to the hardware interface of the serial port. The normally used processor internal device is: /dev/ttymx0
Network Connection	Mode and state	The configured port mode is shown here followed by the current state of the connection with IP and port of the connected device.
Baudrate Parity Databits	transmission parameter	These are the configured parameters of the serial interface. Meaning: aaaa - b - c aaaa = baudrate b = parity (n = none, o = odd, e = even) c = databits (7 or 8)

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	Statistical information	The values displayed here show how many bytes or data packets were sent or received via the serial interface.
--	-------------------------	---

Table 5: Status of the serial interface

3.5 Relay Status Information (Optional)

In this section the current state of the relay is displayed. If the relay function is disabled, this section will not appear.

Relay	Mode	Function
	TCP (UDP)	The relay function is active and listening on the configured port
	Internal	The relay is controlled by the digital input.
	serial Trigger	The relay turns on when data is being received that is sent over the serial interface. Thus, e.g. A wake-up function can be realized for the received device connected to the MC. The relay switches off again if no data are sent over the serial interface longer than "timeout".
	WLAN Status	The relay switches on if a WLAN connection is available.
Current State	ON or OFF	

Table 6: Relay status

3.6 Network Information

This section displays information on the active network interfaces.
The shown information depends on the configured bridge mode.

Bridge - Mode	Shown Information (for a sample setting)
LAN Client Cloning	<p>Network Information Interface wlan0 (IPv4) IP 192.168.170.255 Broadcast 192.168.170.255 Netmask 255.255.255.0 MAC 00:E0:00:17:C7:B1</p> <p>Bridge Bridge Type LAN Client Cloning Client IP 192.168.170.127 (Autodetected) Client Netmask 255.255.255.0 (Configured value) Client Gateway 192.168.170.1 (Autodetected) Client MAC 00:E0:00:17:C7:B1 (Autodetected) Original WLAN Card MAC 00:0E:8E:64:E6:D7 LAN MAC 90:5F:8D:05:A5:CB</p>
NAT or Single Client NAT	<p>Network Information Interface Wireless (IPv4) IP 192.168.170.102 (Static IP) Broadcast 192.168.170.255 Netmask 255.255.255.0 MAC 00:0E:8E:8B:7B:09</p> <p>Network Information Interface Wireless (IPv4) IP 192.168.170.102 (Static IP) Broadcast 192.168.170.255 Netmask 255.255.255.0 MAC 00:0E:8E:8B:7B:09 Interface LAN (IPv4) IP 192.168.170.102 Broadcast 192.168.170.255 Netmask 255.255.255.255 MAC 90:5F:8D:05:F3:D0 Routing Default gateway 192.168.170.249 on Wireless</p> <p>Bridge Bridge Type Level 2 Bridge</p> <p>Level 2 Bridge Status Bridge Entry 1 LAN1: 00:1B:B1:05:77:B2 192.168.170.69 (1sec) Bridge Entry 2 LAN2: 00:E0:4C:05:13:14 192.168.170.30 (7sec)</p>
Level 2 Pseudo-Bridge	

Table 7: Network Information

3.7 Access point list

This section displays a list of Access Points (AP) registered by the MC. The list entry of the currently connected AP is highlighted in gray and is always displayed first. The AP's with a matching SSID that are potentially eligible for a connection follow. These AP's are displayed with green letters. After that AP's with different or unknown SSID (hidden) are listed. The information under "Security" gives information about the authentication methods the AP expects. If an AP offers the SSID matching the MC, but the "Security" settings of the AP prevent the MC from connecting to the AP, the "Security" information is displayed in red letters.

The same applies to the "Channel/Frequency" column if the AP is working on a channel that is not included, e.g. by specifying a channel list under Configuration->Wireless->Roaming.

In the column "Extra Information" the following is indicated:

- Country setting (DE)
- Number of clients / channel utilization (5/2%)
- Transmission power limitation (17dBm) (If available)
- 802.11k info with the number of specified neighbor AP's (802.11k (1))
- Roaming operations (a / b) a= failed b= successful
- Noise level (-95dBm). This value + SNR gives the measured signal level. (-95 + 48 = -47dBm)

Accesspoint List

BSSID	SSID	Security	SNR	AP Name	Channel/Frequency	Max Bitrate	Last Seen	Extra Information
54:4A:00:C7:10:1F	WLC_INT	[WPA2-PSK-TKIP+CCMP] [WPA-PSK-TKIP+CCMP]	38dB	CAP-3502E-V	100: 5500MHz	54.0 + 11n: BW 40MHz	0	DE 5/3% 17dBm Roam 0/14
68:86:A7:13:81:1F	WLC_INT	[WPA2-PSK-TKIP+CCMP] [WPA-PSK-TKIP+CCMP]	42dB	CAP-3502E-H	60: 5300MHz	54.0 + 11n: BW 20MHz	1	DE 5/1% 17dBm Roam 0/13
68:86:A7:13:81:10	WLC_INT	[WPA2-PSK-TKIP+CCMP] [WPA-PSK-TKIP+CCMP]	38dB	CAP-3502E-H	11: 2462MHz	54.0 + 11n: BW 20MHz	1	DE 0/50% 2dBm
54:4A:00:C7:10:10	WLC_INT	[WPA2-PSK-TKIP+CCMP] [WPA-PSK-TKIP+CCMP]	32dB	CAP-3502E-V	6: 2437MHz	54.0 + 11n: BW 20MHz	1	DE 1/44% 5dBm
02:A0:57:22:34:96	LANCOMbgn_EAP	[WPA2-EAP-TKIP+CCMP-preauth] [WPA-EAP-TKIP+CCMP]	44dB	LANCOM_acn_2	1: 2412MHz	54.0 + 11n: BW 40MHz	317	DE 0/50%
68:86:A7:13:81:1A	RadiusTest_FT	[WPA2-FT-EAP-CCMP]	44dB	CAP-3502E-H	60: 5300MHz	54.0 + 11n: BW 20MHz	1	DE 5/1% 17dBm
00:A0:57:22:34:96	LANCOMbgn	[WPA2-PSK-TKIP+CCMP] [WPA-PSK-TKIP+CCMP]	43dB	LANCOM_acn_2	1: 2412MHz	54.0 + 11n: BW 40MHz	317	DE 0/50%

Figure 3.1: Access point list

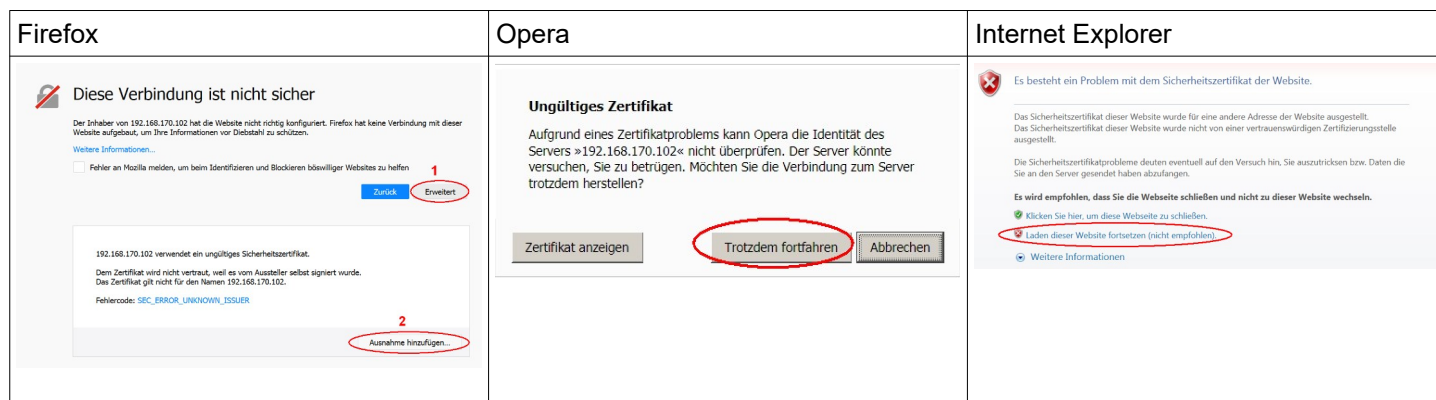
Neighbor (11sec):	
Ch44	
Last Seen	Extra
0	DE 4/2% 802.11k (1) Roam 0/2 -95dBm

In the "Extra Information" column, additional information is displayed when the cursor is placed over the individual data. So you can additionally display the list of neighboring AP's.

3.8 HTTPS Webinterface

The websites of MC devices can also be accessed via HTTPS (Hypertext Transfer Protocol Secure). This enables an encrypted data exchange between MC and web browser. The HTTPS server on a configurable TCP port (default 443) is activated under "Admin". For this access, the MC uses a self-generated server certificate that must be confirmed in the web browser during the first connection.

The browser's confirmation message varies depending on the browser type.



The links in the red marked areas lead to the browser accepting the certificate and establishing the connection to the HTTPS web server of the MC.

To avoid this procedure, you can also load your own registered server certificate onto the MC. This is done in the "Admin" section → 5.1 (Webserver certificate)

3.9 Storage Status Information

A USB memory stick can be connected to the MC, which can be used to store debug messages or recordings on the WLAN or LAN interfaces.

If such a USB memory stick is plugged in, the status of this memory is displayed at the end of the home page.

Storage Status Information

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

Figure 3.2: Storage Status Information

Before removing the memory stick, the user should disconnect the memory from the system using the "Unmount" function so that the content remains consistent. In particular, if the USB stick is formatted as a FAT file system, errors may occur in the USB stick's file system when it is switched off without prior "unmounting".

If the USB stick is used to record debug messages and (or) (W)LAN recordings (see: 5.9), the USB stick should be formatted with the EXT4 file system. This file system is more robust in terms of data consistency if the MC is suddenly switched on and off.

Therefore the function "Format as EXT4 Filesystem" is offered here. This formats the currently inserted USB stick with the EXT4 format. **However, this will delete all existing files on the USB stick.**

3.10 WLAN und LAN-Dump-Dateien

If logging of communication on the WLAN or (and) LAN interface is enabled (see "Configuratio" → "Logging" → "(W)LAN Dump", the resulting files are listed here. The files contain the recorded data in compressed form of type ".gz". Only the files that are currently being written are of type ".pcap". You can find more information here → 5.9.1.4

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)

Figure 3.3: WLAN- and LAN-Dump files

4 Firmware and configuration management: Device Menu

Under this menu item it is possible to transfer a firmware to the MC and save or restore the configured parameters as a file.

4.1 Firmware

with this dialog a firmware file can be uploaded to the MC




It is very important that the power supply of the MC is not interrupted at this stage and also the reset key is not actuated.

Upgrade firmware file Keine Datei ausgewählt

Figure 4.1: Firmware Update Dialog

4.2 Configuration Management

with this menu item following functions are supported:

Reset configuration to defaults	<p>With this button all parameters can be set to the factory default values. The user has to confirm this setting with the button “Save & apply”. With the button “Cancel changes” the changes will be declined.</p> 
Download running configuration	<p>With this button the running configuration can be stored to a file. “Running configuration” means the configuration that is currently active on the MC without the changes made with the actual session.</p>
Download new configuration	<p>With this button the new configuration can be stored to a file. “New configuration” means the configuration that is currently active on the MC with the changes made with the actual session.</p>
Reboot device	<p>With this button the MC will make a reboot. Changes made in the actual session will get lost.</p>
Upload configuration file	<p>With this dialog a config file can be selected and uploaded to the MC. If parameters of the current configuration are changed with this upload, a dialog box will appear to “Save & apply” the new setting or to cancel the changes.</p>

Reset configuration to default values. All current configuration settings will be lost!

Reset configuration to defaults

Download of the running configuration.

Download running configuration

Download of the new configuration which is not yet activated.

Download new configuration

Reboot device

Reboot device

Upload configuration file: Durchsuchen... Keine Datei ausgewählt.

Upload

Figure 4.2: Configuration Management

4.3 Network Test

(from Firmware 2.14b)

On this page you can test network connections to specific hosts.

This can be used, for example, to test the parameters for setting up the network interfaces.

Here you can also check whether certain ports (TCP or UDP) on certain IP addresses can be reached via the WLAN.

The following functions are available:

Function	Description
Icmp Trace	Ping test to an IP or hostname. The individual stations leading to the destination address are listed.
Tcp Connect	This allows a TCP connection to a host to be established on the specified port. The connection will be closed immediately afterwards.
Tcp/Tls Connect	This can be used to establish a TCP/TLS connection to a host on the specified port. If the connection is successful, data from the received CA certificate of the server is displayed.
Udp Send	This function can be used to send a datagram to the specified host on the specified port with the content "Payload".
Filter TCP RX	This function is used to monitor on the specified port whether a TCP connection is established via WLAN to this port. Only the establishment of the connection is reported.
Filter UDP RX	This function is used on the specified port to monitor whether UDP data is being sent to this port via WLAN. When the first UDP packet arrives, information about the sender is output. Only the first UDP packet from a host with a specified source+destination port combination is registered. Clear Results" followed by "Filter UDP RX" restarts the filter.
Clear Results	This clears the outputs and resets the filters (TCP(UDP) RX).
Copy to Clipboard	This copies the output of the test function to the clipboard

Hostname or IP: Port: Payload:

Figure 4.3: Network Test

5 Configuration

The “Configuration” menu has a collection of items to get to the configuration dialogs for all of the MC functions. Depending on the build-in options of the MC some of this submenu items will not appear.

Menu Item	Chapter	important parameter	requirement
Admin	5.1	Device name, User, Password	
Network	5.2	IP-Address, Bridge-Mode	
Wireless	5.3	SSID, Security	
Serial Ports	5.4	Baudrate, Mode ...	Serial Port
Printer Server	5.5	USB-Printer Mode	USB-Port
Relay	5.6	Relay-Mode	Relay Option
Realtime clock	5.7	NTP-Server-IP	
Input	5.8	Input-Mode	Digital input
LAN-Port		LAN-Port Parameter	
Logging	5.9	Debug-Messages	

The individual web pages for configuration are presented and explained in detail on the following sites.

5.1 Admin

[Home](#) [Device](#) [Configuration](#) [Statistics](#) [Support](#) [Logout](#)

Device Name
Device Name:
This is the name that the bridge will use to identify itself to external configuration and IP-address-finding programs. This is not the same as the SSID. It is okay to leave this blank if you are not using these programs.

Security
Administrator Login
Admin name:
This is the admin user name that must be entered to get access to these pages.
Admin password:
This password must be entered to get access to these pages.
Monitor Login (Read Only Access)
Monitor name:
This is the monitor user name for read only access to these pages.
Monitor password:
This is the password of the monitor user for read only access to these pages.

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

Webserver
Enable Unencrypted (HTTP) ☒
Check this box to enable standard unencrypted webserver.
Webserver Port:
Configure a alternative webserver port to avoid a collision with a LAN-Client setup. Default is port 80
Enable Secure (HTTPS) ☒
Check this box to enable secure webserver over https.
Secure Webserver Port:
Configure a alternative secure webserver port to avoid a collision with a LAN-Client setup. Default is port 443

Configuration tool accessibility
MC-Config Port:
Port selection for MC-Config-Tool accessibility of the device.

Other Options
Serial port instances:
Number of serial port instances.

Power Save
Enable Power Save Interface ☐
Enable interface for remote controlled power down periods.

Debug Level:
Select debug level for power save function.

Webserver certificate
Certificate Password:
Enter certificate password.
Webserver certificate info
Information about loaded client certificate
Upload certificate file: Keine Datei ausgewählt.

Device name:

This name is displayed with the MC Config program and can also be sent to the DHCP server as the device name for DHCP.

Access protection:

To protect the configuration of the MC from being changed or read out, you can define an 'Admin' with 'Name' and 'Password' here.

For someone who should only see the configuration but not change it, you can define a user as 'Monitor' who can open the configuration but cannot make any changes to the parameter.

SNMP:

The Simple Network Management Protocol (SNMP) is a network protocol for monitoring and controlling network elements from a central station. The MIB file, which provides a device description, can be downloaded from the MC via a link. The 'Community name' is set to 'public' by default.

Webserver:

The web server of the MC can be accessed via HTTP or HTTPS. At this point you can (de)activate both protocols and define the port numbers for these protocols. Setting the port numbers can be important if you are working in NAT mode and LAN clients should also be accessible on these ports. For the HTTPS function, a customer-specific certificate for the web server can be uploaded at the bottom of this page.

Configuration tool accessibility:

With this setting the access for the MCConfig tool can be restricted.

- WLAN+LAN
- LAN
- none

Other options:

Here you can define how many serial ports are to be used. The number of serial ports can be extended by connecting suitable adapters to the MC-USB port.

Power Save:

With this option it is possible to set the MC to a power-saving mode for a certain time. During this time, the module consumes only about 1/3 of the typical power. In this state, however, the module cannot communicate. After the specified time has elapsed, the module reports back with a status datagram. If you want to use the function, contact the manufacturer.

Webserver certificate:

With this function it is possible to upload a certificate for the web server of the MC. This certificate replaces the device-internal self-generated certificate that generates a warning message when the MC web page is called via https.

5.2 Network

In this section the IP addresses of the MC and the properties of the bridge function are defined.

5.2.1 IP Address

HomeDeviceConfigurationStatisticsSupport

Admin

IP settings

NetworkIP address

Enable DHCP Client

☒

Check this box to enable the dhcp client for IP configuration. (Disabled for LAN-Client-Cloning)

Host Name:

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

☒

Check this box to enable fallback to static IP if the dhcp client fails.

Default IPv4 address:

Type the IP address of your bridge.

Default Subnetmask:

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

Gateway Address:

This is the IP address of the gateway that connects you to the internet.

Nameserver Address (DNS):

This is the IP address of the nameserver (DNS).

Backup DNS 1:

This is the IP address of the backup DNS 1.

Backup DNS 2:

This is the IP address of the backup DNS 2.

IPv6 settings

Enable IPv6 Support (experimental)

☒

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

Debug IPv6:

Detailed

Select log configuration IPv6

Enable Bridge

☐

Check this box to enable IPv6 bridge support. Forwarding router advertise with prefix

Enable DHCP:
By activating this option, the MC obtains the network settings via DHCP. Usually this will be done over an existing WLAN connection.
If the "Host Name" parameter is defined, this specification is included in the DHCP request. If this parameter is empty, the "Device Name" from the admin page is used.

Enable fallback to static IP:
If the assignment of the network parameters via DHCP fails, you can use this option to specify that the following network settings are accepted.

IPv4 , Subnetmask, Gateway, DNS:
Without DHCP, the network parameters that the MC uses via **WLAN** are set here. Only in "Pseudo Level 2 Bridge Mode" is this IP address also active via LAN.

IPV6 settings:
This activates the IPV6 functionality of the MC device. This function is still in the development stage. Users are welcome to contact modas to have functions implemented in this area. So far only the web server can be reached via IPV6.

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:

with this method, names of network devices within a local network can be resolved to IP addresses without the need for a DNS server. All DNS requests for the ".local" domain are sent via UDP to the mDNS multicast address 224.0.0.251 UDP port 5353.

Mircosoft operating systems use the LLMNR (Link Local Multicast Name Resolution) protocol for the same purpose. This protocol can also be activated and communicates via multicast IP 224.0.0.252 and UDP port 5355.

The following 3 parameters determine to which requests the device should respond.

5.2.2 Bridge

The MC supports 5 different bridge modes. The modes are characterized by how transparently the LAN clients on the MC are connected to the WLAN, which MAC address the LAN clients use in the WLAN and whether the LAN clients have their own IP address in the WLAN.

Bridge-Mode	LAN-Clients	IP's in WLAN	Transparency	Note
OFF	any number	1 (MC IP)	separate	If the brigde function is disabled, the LAN clients cannot communicate with other devices via the MC's WLAN interface.
LAN Client Cloning	1	1 (LAN Client IP)	all Ports	Only the LAN client IP is registered in the WLAN with the MAC address of the LAN client.
Single Client NAT	1 + x	1 (MC IP)	all Ports	In the WLAN only the IP of the MC is registered with the WLAN MAC address of the MC. Only one LAN client can be addressed via WLAN. On LAN side all other LAN clients can communicate with each other and with the WLAN.
NAT	any number	1 (MC IP)	Ports def. per Config	The LAN clients can only be reached via certain ports that are defined in the port forwarding table (NAT rules).
Level 2 Bridge	any number	n x LAN-Clients + 1	all Ports	In the WLAN, all LAN client IP's and the MC IP are registered with the WLAN MAC address of the MC.
MWLC-Mode	any number	1 (MC IP)	all Ports	Only the MC-IP is registered in the WLAN with its WLAN MAC address.

Table 8: Bridge modes

Depending on which bridge mode is selected, different parameters are displayed.

5.2.2.1 Bridge-Mode OFF

In this mode, the clients connected to the MC via the LAN port cannot communicate with other devices via WLAN. The MC has 2 IP addresses via which the MC internal functions such as relay, serial interface, web interface etc. can be accessed.

This mode should be selected if:

- 1) the WLAN interface is switched off
 - 2) if for example an application is to operate the MC only as a serial client with RS232 interface.
- This ensures that the LAN port on the MC cannot be used to access the WLAN side.

5.2.2.2 LAN-Client-Cloning

The "LAN Client Cloning" mode is used to connect a network device connected to the LAN port of the MC to a network as transparently as possible via WLAN. The MC takes over the MAC address and the IP address of the LAN client for communication via WLAN.

If the MC has several LAN ports and these are also connected, only the device on LAN port 1 is taken into account for transferring the MAC address. Other devices connected to the other LAN ports can communicate with each other, even with the "cloned" device. However, these other devices cannot communicate via WLAN.

Attention: The MC does not switch on the WLAN until Ethernet data with a MAC address has been registered at the LAN port.

HomeDeviceConfigurationStatisticsSupportLogout

Bridge mode configuration

NetworkBridge

Bridge active

☒

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

Bridge mode

LAN Client Cloning

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

LAN client Type

Autodetect

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

LAN Client IP

0.0.0.0

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

LAN Client Netmask

255.255.255.0

Subnet mask if not determined by DHCP.

LAN Client Gateway

192.168.170.249

Gateway if not determined by DHCP.

LAN Client DNS1

0.0.0.0

DNS Server if not determined by DHCP

LAN Client DNS2

0.0.0.0

DNS Server if not determined by DHCP

AddRemove

Bridge IP on LAN Port

0.0.0.0

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

30

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

MAC to clone

00:E0:4C:05:13:14

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

LAN-Client Type:

The LAN client can have a fixed IP setting or obtain the IP settings via DHCP via WLAN. Depending on this, here

- DHCP

- static

- autodetect

can be set.

With the options "Static" and "Autodetect" the parameters IP + Netmask + Gateway can be configured.

With "Autodetect" you can connect both "DHCP" and "Static" clients. **However, you must specify the values for the network mask and gateway IP of the network to which the LAN client connects.** The IP of the gateway is important because the MC uses this IP to be accessible via LAN. The "LAN client IP" should be specified if the LAN client is passive, i.e. it does not send any data packets with its IP address by itself. The MC uses an ARP request to check whether the specified IP can be reached via LAN. If so, this IP address is assigned to the WLAN interface of the MC. Thus, the MC and the LAN client can be reached via WLAN with this IP address.

DNS1 + 2:

If the MC needs a DNS to resolve e.g. the IP address of the NTP server, 2 DNS can be specified here.

Bridge-IP on LAN-Port:

If you want to reach the MC via the LAN side via an IP address other than the gateway IP, you can define it here.

IP Timeout:

The MC constantly checks whether the "cloned" IP is still accessible. If no response is received after "Ip Timeout" seconds, the WLAN interface of the MC is switched off and only switched on again until a response is registered again by the LAN Client IP.

Stay connected:

Sometimes it is necessary that the WLAN interface of the MC remains active even if the LAN client is switched off. For example, if the relay is used to switch off the LAN client. Then, of course, the WLAN connection must be hold so that the relay can be switched on again.

MAC to clone:

Here you can specify a specific MAC address to be cloned. This would make sense, for example, if 2 MAC addresses are active on LAN port1.

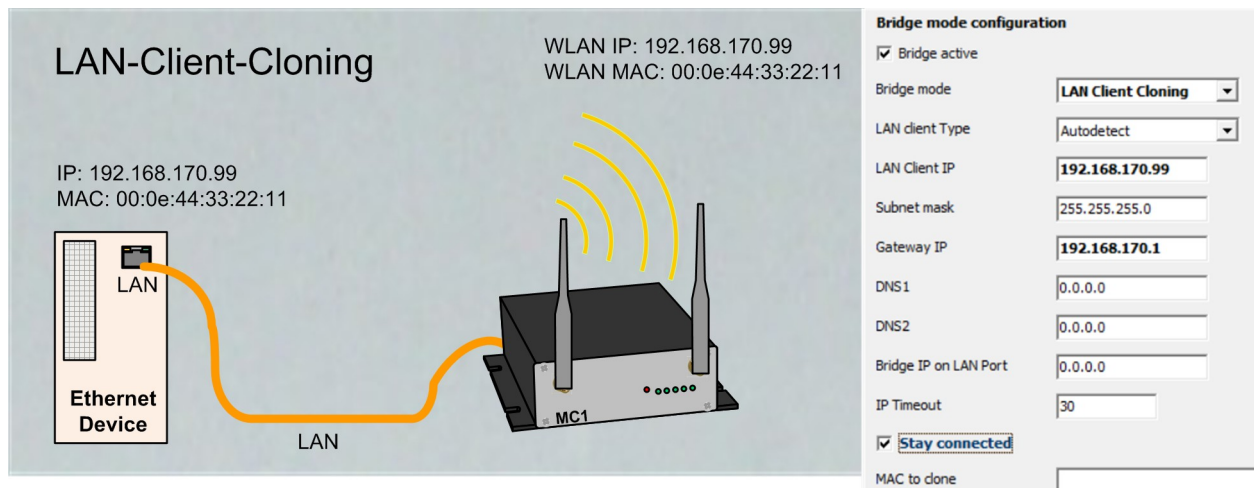


Figure 5.1: LAN Client Cloning Mode

The IP address of the LAN client is used to access the MC internal interfaces (website, serial, relay, USB). To avoid collisions with port numbers used on the LAN client, these must be adapted accordingly on the MC. Especially for the website of the MC there is the parameter "Web Server Port" under Configuration->Admin which can be changed if the LAN client also runs a web server on port 80 or 443 (https).

Advantages of LAN client cloning mode:

1. In the wireless network, the MC appears together with the LAN client only with an IP address

Disadvantages of LAN client cloning mode:

1. Only one LAN client can be connected to LAN port 1 of the MC.

5.2.2.3 NAT and Single Client NAT

In NAT mode, the MC works with different networks on the LAN and WLAN side. In WLAN the MC communicates with the IP settings as described in 5.2.1. On the LAN side, a separate network is defined. If connections to the LAN clients are to be established via WLAN, a table based on the port numbers is used to determine to which IP address on the LAN side the data is forwarded (NAT rules).

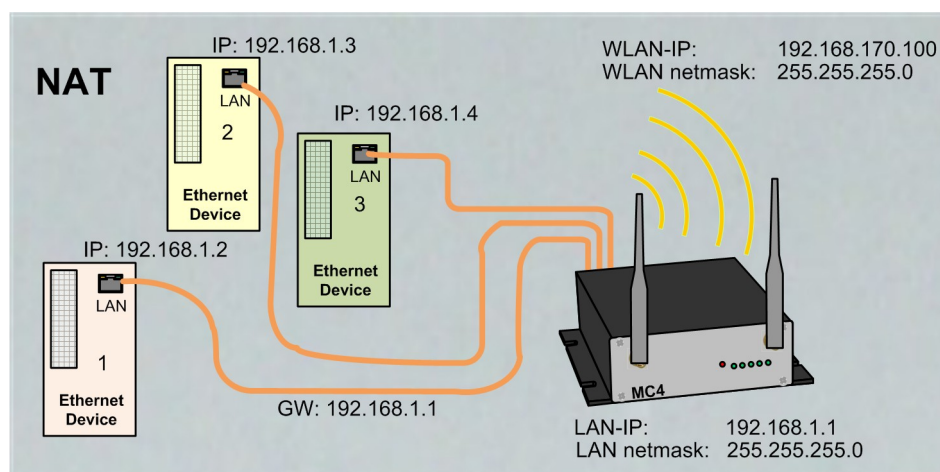


Figure 5.2: NAT-Mode (sample configuration)

If only one LAN client must be accessible via WLAN, the table can be omitted by specifying an IP address to which all incoming connection requests via WLAN are forwarded. In this case, the bridge mode is set to "Single Client NAT".

On the LAN side, a DHCP server can be activated that supplies the LAN clients with IP addresses. The distribution of the IP addresses can be defined with a reservation list via the MAC address of the LAN client or via the device name.

Home Device Configuration Statistics Support Logout

Bridge mode configuration

Bridge active

☒

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

Bridge mode

Single Client NAT

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

192.168.1.10

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

Local IP address:

192.168.1.1

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

Subnetmask:

255.255.255.0

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.

Enable MAC Authentication

☒

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

Radius server IPv4 address:

192.168.170.249

Type the IP address of the radius server.

Radius server port:

1812

Port for radius server.

Radius shared secret:

Shared secret for radius server.

Authentication Timeout:

3600

Timeout for authentication until reauthentication is required.

Radius Debug Level:

Default

Select log configuration for radius.

Autodetect LAN client: (Single Client NAT)

If only one LAN client is connected, it is not necessary to define the LAN client IP address when activating this function.

LAN Client IP: (Single Client NAT)

All connection requests from the WLAN side are forwarded to this IP specified here.

Local IP address:

With this IP address the MC communicates on the LAN side. LAN clients connected to the MC must configure this IP as gateway IP.

Subnet mask:

Subnet mask of the local network.

Forward DNS requests:

This option enables the forwarding of DNS requests from the local network to the DNS server of the WLAN side. This eliminates the need to configure a special DNS server on the LAN clients. Only the local IP of the MC must be configured on the LAN client.

MAC Authentifizierung (Only NAT-Mode)

To prevent any device plugged into the LAN port of the MC from connecting to the WLAN, it is possible to register the MAC address of the allowed devices. To do this, the permitted MC addresses must be entered into the network's radius server.

If you activate this option, parameters are displayed that define access to the radius server:

1. IP address
2. port number
3. Shared secret
4. Timeout of the authentication.

For troubleshooting, this authentication function can be monitored more closely with the "Radius Debug Level" parameter. With the setting "Detailed" or "Maximum" more or less detailed messages are written into the log file, which indicate which steps of the authentication were passed through.

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"/>
	<input type="button" value="Add"/> <input type="button" value="Remove"/>
DMZ IP:	<input type="text" value="0.0.0.0"/>
<small>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.</small>	
Enable NAT Loopback	<input type="checkbox"/>
<small>Enable NAT-Loopback (also known as Hairpinning).</small>	

5.2.2.3.1 Forwarding rules for NAT

This section defines rules for forwarding connection requests from the wireless side to the LAN clients.

The rules are formatted as follows:

<Protocol> : <Portdefinition> : <Client IP>

protocol is either **TCP** or **UDP**

Destination port definition as forwarding:

1) **Destination** port number does not change

- Single ports: **1234:** or: **123, 1234, 4545 :**

- Port Ranges: **8000-8010, 120-130 :**

1a) **Source** port number as forwarding criterion:

If the source port number is to decide to which IP the forwarding is to be made, this is marked with a leading '!' character before the port number.

- Single ports : **!1234 :** or : **!123, !1234, !4545 :**

Destination port definition as redirection:

2) Destination port number changes

- Single ports **:1234 > 3456 :**

Client-IP: **192.168.1.10**

You can create up to 30 of these rules.

In a rule definition, both port ranges and multiple port redirections can be defined by specifying them separated by commas.

For example, you can use the rule:

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

that all data for ports 3000 to 3010 + 4001 + 4004 + 5005 are forwarded to IP address 192.168.1.2.

It is not possible to redirect from one port range to another.

To specify the **source** port number as a criterion for assigning an IP address, you can specify the port number with a leading '!' character.

FTP Helper:

If a FTF server is operated on a LAN client, certain precautions must be taken because of the dynamic port usage, which the Linux kernel takes care of. For this one must activate this special procedure with the additional parameter "ftp" in the definition of the NAT rule.

e.g. with TCP:21:192.168.1.10:ftp

SNAT:

This option replaces the source IP of IP packets arriving via WLAN with the IP of the MC LAN port.

for example: TCP:12345:192.168.1.10:snat

You can find more information on this topic here: <Network_address_translation>

5.2.2.3.2 DHCP-Server

On the LAN side, a DHCP server can be activated to supply the LAN clients with IP addresses. The distribution of the IP addresses can be defined with a reservation list based on the MAC address of the LAN client or via the device name.

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.

The DHCP server offers the following parameters after activation.

IP Range start (end):

The IP addresses for LAN clients are offered in the range specified with these 2 IP addresses.

Lease Time:

The time in seconds after which an IP address must be confirmed again. This renewal is triggered by the LAN client.

DNS IP:

The DHCP server usually also provides the IP address of one or more DNS servers with the IP address. These DNS servers can be defined here. If no information is entered here, the DHCP server retrieves the DNS information from the WLAN interface and transmits it to the LAN clients.

On the LAN side, a DHCP server can be activated that supplies the LAN clients with IP addresses. The distribution of IP addresses can be defined with a reservation list based on the MAC address of the LAN client or via the device name.

Static DHCP Server entries

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

Static
Entry 1

Static
Entry 2

Static
Entry 3

Static
Entry 4

Static
Entry 5

Add

Remove

5.2.2.3.3 Static DHCP Server entries

To ensure that LAN clients are always assigned the same IP address after switching on the MC or the entire system, you can reserve IP addresses from the IP range defined above in this table via the MAC address of the LAN client or via the device name that is sent in the DHCP request.

A maximum of 50 entries can be managed.

Advantages of NAT mode:

1. Almost any number of LAN clients can be connected to an MC.
2. In the WLAN network, the MC appears with all LAN clients only with one IP address.
3. If there are many units working in a project that consist of several LAN clients with one MC, the configuration is the same for all units. Only the IP address of the MC to the WLAN side may need to be set up individually.
4. In some ways, the LAN clients are better protected against unwanted access because the MC only switches through data for the configured ports.

5. local broadcast data packets (on the LAN side of the MC) are not sent over the WLAN.

Disadvantages of NAT mode:

1. Access to the LAN clients via WLAN is only possible on the ports defined in the NAT rules.
2. If the LAN clients offer server services with the same (standard) port numbers (e.g. FTP), you may have to work with different port numbers via WLAN in order to be able to use these services on the different LAN clients.

Important!

Care must be taken that there are no collisions between the port numbers of the LAN clients and the internal interfaces of the MC. The internal interfaces of the MC are e.g.

1 serial port (default port 8888)

2 Printer server (default port 9100)

3 MC Webserver (default port 80 and or 443 (HTTPS), this port can also be changed under Configuration->Admin->Webserver Port)

4 relay

5 Aux-In

6 MCConfig (UDP+TCP Port 17784 + 17785)

See info at: 6.2

If these interfaces are not used, they should be deactivated.

5.2.2.4 Level 2 Pseudo-Bridge Mode

In Level 2 pseudo bridge mode, all LAN clients communicate with their own IP addresses via the WLAN. For this purpose the MAC address of the WLAN card of the MC is used for all LAN clients. **Prerequisite for this mode is that the IP addresses of all LAN clients and also the IP of the MC are in the same network.**

This procedure can lead to problems with some WLAN infrastructures if any WLAN controllers answer ARP requests from the stationary network side using a WLAN client list (ARP caching). If these WLAN controllers only allow one entry MAC <--> IP, access to the LAN clients from the stationary network is not guaranteed, because ARP requests may not be answered.

This problem is usually to be expected in controller-based WLAN infrastructures of CISCO®.

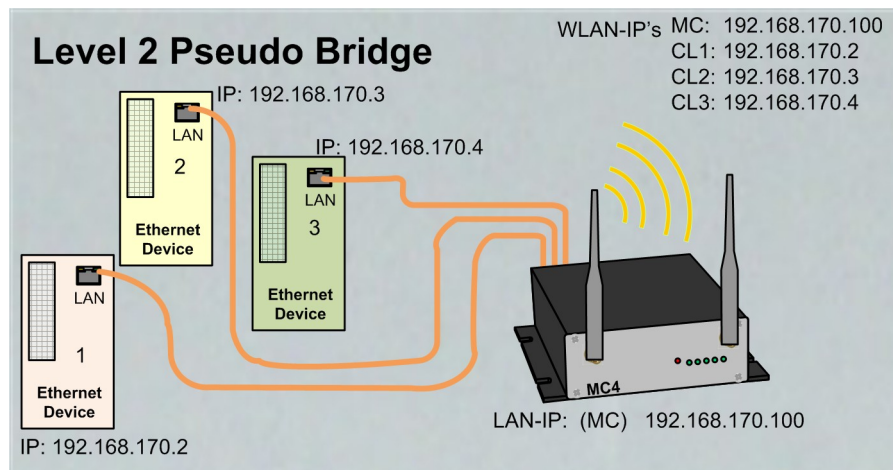


Figure 5.3: Level 2 Bridge (sample configuration)

In this mode, only a few settings have to be made on the MC.

Bridge mode configuration

Bridge active	<input checked="" type="checkbox"/>	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	<div>Level 2 Pseudo-Bridge</div>	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	<input type="checkbox"/>	Delay LAN port link up to support clients that transmit important packets after link up.
Scan LAN Clients	<input checked="" type="checkbox"/>	Check this box to enable automatic scanning of LAN client IPs.
Forward Multicast/Broadcast	<input checked="" type="checkbox"/>	Check this box to enable forwarding of Multicast/Broadcast packets.
Enable DHCP Relay Agent	<input type="checkbox"/>	Check this box to enable relay agent for DHCP requests.
Enable passive client helper	<input checked="" type="checkbox"/>	Check this box to enable a helper function for passive clients.
Helper IP	<div>0.0.0.0</div>	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:

If LAN clients are passive on the MC, i.e. do not send data via Ethernet themselves without a request, this function can be used to cause the MC to regularly scan the network on the LAN side via ARP request. As a result, the MC can quickly registered all connected LAN clients, especially after a restart.

Forward Multicast / Broadcast

This option determines whether broadcast data arriving at the MC via WLAN is forwarded to the LAN side.

Enable DHCP Relay Agent

If the LAN clients on the MC obtain their IP address via DHCP, this option can support this by the MC manipulating the DHCP requests of the LAN client so that the responses arrive correctly at the LAN clients. The need for support depends on the network structure on the WLAN side and the properties of the DHCP server.

Enable passive client helper

If a device is connected to the LAN port that does not communicate via the LAN port on its own but only responds to requests, this function can be used to make the LAN client with its IP better "known" as a station in the WLAN. As soon as the client is recognized by an ARP request, the MC device sends a ping request "in the name" of the LAN client to a specified IP address. This happens only approx. 1x per minute and only if there is no other communication.

Helper IP

An IP to which the ping request is sent can be defined here. If the parameter is 0.0.0.0, the gateway IP is used as the destination.

Advantages:

1. Almost any number of LAN clients can be connected to an MC.
2. good transparency of LAN clients to WLAN without configuration

Disadvantages:

1. The MC and all LAN clients work with their own IP addresses, which must be on the same network.
2. difficulties in some WLAN infrastructures with central controllers (no access to the LAN clients from the WLAN side)

5.2.2.5 MWLC Mode

The MWLC mode removes all restrictions regarding accessibility, IP address assignment and transparency, especially in applications with several LAN clients on the MC. This is achieved by the MC sending all data packets arriving at the LAN port to another MC on the stationary network side via an IP/UDP connection (tunnel) in this mode. This MC restores the received data packets to their original state and sends them to the stationary network. The MC on the WLAN side works in MWLC slave mode and the MC on the stationary network side in MWLC master mode.

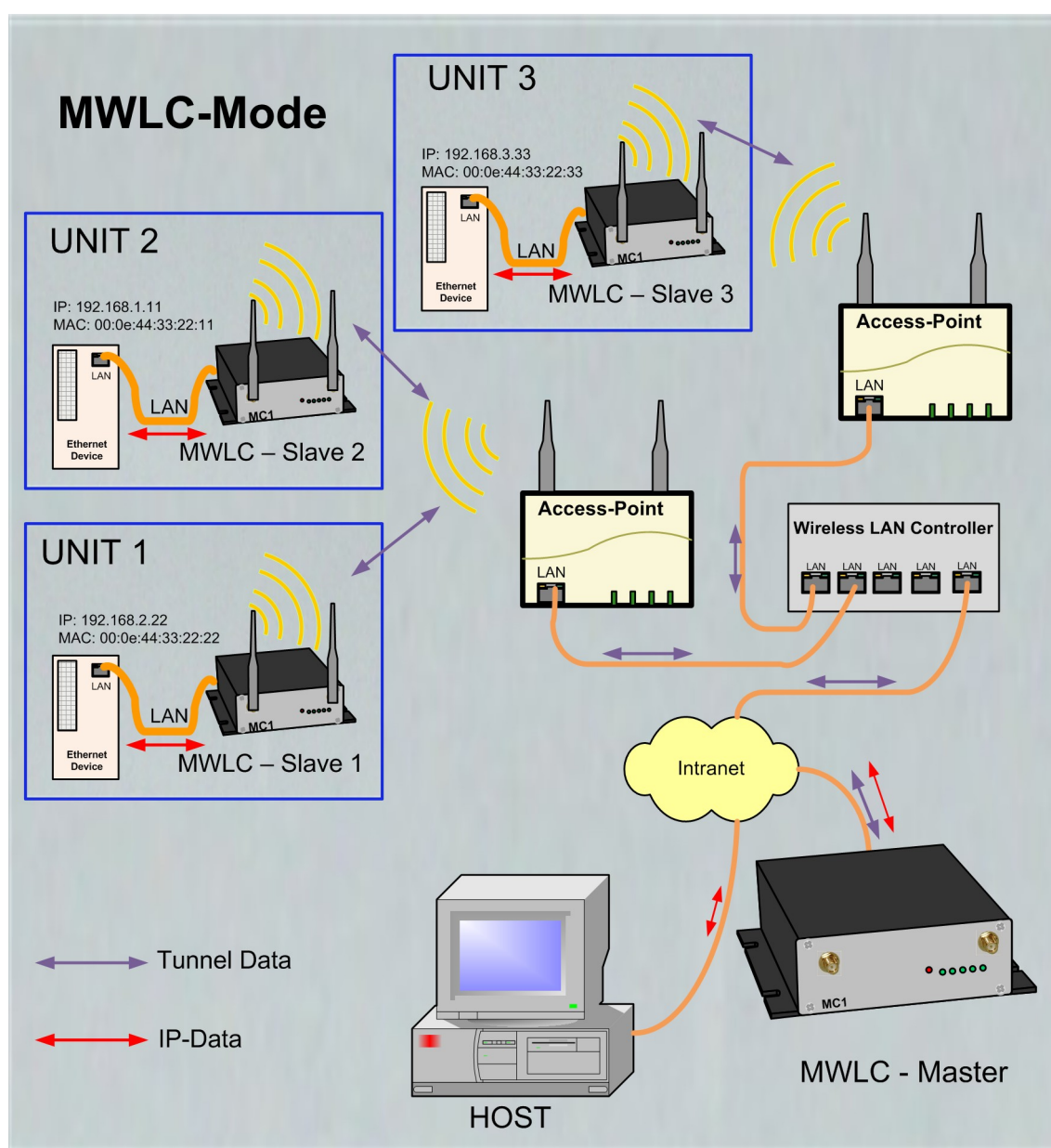


Figure 5.4: MWLC-Mode sample configuration

In this mode it is irrelevant which IP addresses the clients have in relation to the MC, e.g. in level 2 pseudo bridging. The clients are also addressed in the stationary network with their own MAC. Since the MWLC master plays a central role in this constellation and a failure of this device would interrupt the connection of all clients, there is the possibility to install a 2nd MWLC master as backup and to configure the IP address of this backup master in the MWLC slaves.

Advantages of MWLC mode:

1. maximum transparency of LAN client connections to the stationary network via WLAN.
2. no special configuration effort on the MC no matter how many LAN clients are connected.

Disadvantages of the MWLC mode:

1. one or two additional MC adapters are required on the stationary network side.

5.2.2.5.1 MWLC-Master

The screenshot shows a web interface for configuring the MWLC Master. At the top is a navigation bar with links: Home, Device, Configuration, Statistics, Support, and Logout. The main heading is "Bridge mode configuration". Below this, there are three sections: 1. "Bridge active" with a checked checkbox and a note: "Do not disable the bridge except the wireless mode is 'accesspoint'". 2. "Bridge mode" with a dropdown menu set to "MWLC Master" and a detailed note: "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". 3. "High Priority" with an unchecked checkbox and a note: "Enable high priority tunneling data". Below these is the "DHCP Server" section, which states: "DHCP server function is only available when Bridge mode is NAT or Single Client NAT." and has an "Enable DHCP Server" checkbox that is checked, with a note: "Check this box to enable the dhcp server configuration."

The MWLC Master works with WLAN interface switched off.

High Priority:

This means that the data from and to the MWLC slaves is processed with a higher priority than other data.

5.2.2.5.2 MWLC-Slave

Since the master module plays a central role and thus all MWLC slaves would be affected in the event of a failure of this MC device, it is possible to define a second master to which the MWLC slave connects if the first master fails.

Bridge mode configuration

Bridge active

☒

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

Bridge mode

MWLC Slave

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

192.168.170.23

Enter master ip for MWLC-Mode.

Backup Master IP

192.168.170.24

Enter backup master ip for MWLC-Mode.

High Priority

☒

Enable high priority tunneling data.

Master IP:
IP address of the MWLC master

Backup Master IP:
IP address of a 2nd MWLC master that can work as a replacement in the event of a failure of the first.

High Priority:
This means that the data from and to the MWLC slaves is processed with a higher priority than other data.

5.2.3 Bridge not active Mode

If the bridge function of the MC device is switched off, the MC device can be accessed both from the WLAN and via the LAN interface without data being exchanged between the LAN and WLAN.
This mode could be useful, for example, if the MC device is only to be used as an Ethernet to serial adapter.
In this mode, 2 different accesses (LAN + WLAN) to the MC device can be configured.
The IP configuration for the WLAN interface is set as usual under Configuration -> Network -> IP Address. The IP configuration for the LAN side becomes visible as soon as the "Bridge active" option is deactivated.

Home Device Configuration Statistics Support

Admin

Network

Wireless

Serial Ports

IP address

Bridge

Filter

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

Routing Priority:

LAN

Select which interface gateway should be preferred for routing.

LAN side interface IP

Enable LAN DHCP Client

☒

Check this box to enable the dhcp client in LAN side for IP configuration.

Host Name:

MC4-NoBridge

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

☒

Check this box to enable fallback to static IP if the dhcp client fails.

IP:

192.168.1.1

Type the IP address that the device will use on LAN side

Subnetmask:

255.255.255.0

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

Gateway IP

0.0.0.0

This is the IP address of the gateway that the device will use on LAN side.

Nameserver address (DNS):

0.0.0.0

This is the IP address of the nameserver (DNS) that the device will use on LAN side.

Backup DNS 1:

0.0.0.0

This is the IP address of the backup DNS 1 that the device will use on LAN side.

Backup DNS 2:

0.0.0.0

This is the IP address of the backup DNS 2 that the device will use on LAN side.

Routing Priority:

If WLAN and LAN are active, a gateway is usually also defined for both interfaces. If an application on the MC device actively wants to establish a connection, the gateway to be used is defined here.

Enable LAN DHCP Client:

This can be used to activate the DHCP client on the LAN side, which of course only makes sense if a DHCP server is also active in that network.

Host Name:

The DHCP client uses the name entered here to request an IP address from the server.

Enable fallback to static IP:

In the event that the DHCP server does not assign an address, you can also enter IP data in the following, which will then be activated.

In the following area, all IP data of the LAN interface can be statically defined if no DHCP is active.

MC Manual

Version 2.14h

36 / 67

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"/>	At this position you can define different gateways for certain IP address ranges.
--	---

5.2.4 MQTT Client

With this function it is possible to control the MC internal interfaces (relay, AUX-IN, serial) via the MQTT protocol. In addition, you can also make settings on this page that make it possible to send MC status messages via MQTT.

Some of the following parameters can be provided with variables. These variables are currently defined:

%dname	Device name (see Admin)
%wlanmac	MAC address of the WLAN interface
%SN	The serial number of the MC
%FW	Firmware version of the MC

The following parameters can be set:

Parameter	Function	
Broker	Server to which all topics and subscriptions are sent. You can specify an IP address or a host name.	
Port	Tcp port on which the broker expects connections. 1883 is the default port for MQTT. For encrypted data the port 8883.	
TLS Mode	Here you can set whether the data is encrypted.	
	1) unencrypted	Without encryption if necessary with user + password
	2) TLS Accept All	Encrypted without client authentication
	3) Verify by Fingerprint ...	Encrypted: The server certificate is verified against the specified fingerprint.
	4) Configured CA Cert	Encrypted: The uploaded client certificate is used for authentication.
Timeout	Timeout in seconds for the connection to the MQTT server. If the server has no connection to the MQTT client for the specified time period, the server sends the message specified under LWT-Data with the topic LWT-Topic to all subscribers.	
Username / Password	User name and password for authentication with the MQTT server. This information is necessary depending on the configuration of the MQTT server.	
ClientId	Unique identifier for logging in to the MQTT server	
Status Topic Type	1) disabled	Do not send status messages
	2) API/Status Parts	Parts from the API/Status are sent in json format under the topic "Status Topic". The content is determined by the paths defined under "Path 1..x".
	3) Text	The text specified under Status Topic is sent as a status message.
Status Interval	Time interval between status messages	

Path 1... x	<p>If "Status Topic Type = API/Status Parts" is set, parts of the API/Status to be sent are defined here</p> <p>Examples:</p> <p>\$.Device → sends all elements of the query 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 → returns: "</p> <pre> { "Device": { "FirmwareVersion": "2.14h" } } </pre> <p>\$.Wireless.Connection.SNR → returns the current signal strength of the WLAN connection</p> <pre> { "Wireless": { "Connection": { "SNR": 52 } } } </pre> <p>The outputs of the individual paths are combined and then sent.</p>
QoS	Quality of Service (see MQTT protocol)
LWT Topic	<p>" Last Will and Testament":</p> <p>This topic is stored at the broker. The broker sends this topic with the content "LWT Data" if the client does not react within the timeout period (see above).</p>
LWT Data	Last Will Text
Debug	Here you can specify a debug level with which information is written to the debug log file.

5.3 Wireless

In menu "Wireless", all settings are made that define how the WLAN interface of the MC device is to connect to the WLAN infrastructure on site.

There are 4 sub menus with the following parameter groups:

Sub menu	Chapter	Function
Main Parameter	5.3.1	Determination of physical parameters: Frequency band, transmission power, country setting, antenna configuration
SSID Profile 1	5.3.2	Here you define the WLAN network name to which the MC should connect. This includes settings for the encryption used and the possibility of uploading certificates to the MC If desired, you can create several such profiles. The number of these profiles is defined under "Main Parameters".
SCEP	5.3.3	SCEP - Simple Certificate Enrollment Process: This function is only required if certificate-based authentication is defined in an SSID profile and you want the MC to automatically distribute or renew the certificates.
Roaming	5.3.4	Special settings that can support fast switching from one access point to another.

5.3.1 Main Parameter

Home	Device	Configuration	Statistics	Support
------	--------	---------------	------------	---------

Wireless Para

Admin

Network

Wireless

Main Parameter

☒ Enable Wireless Interface

Check this box to enable the wireless interface.

Wireless Mode

Infrastructure

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'

SSID Profiles

1

Number of SSID Profiles.

Phy Mode

2.4+5GHz

Select physical mode - preferred frequencies will be scanned.

Country selection

Germany

Select country.

Enable sleep mode

☐

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.

802.11bg bitrate setting

all bitrates

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.

802.11a bitrate setting

all bitrates

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.

Power selection

Auto (MAX)

Power selection.

Antenna gain

0

Antenna gain setting.

Antenna selection

Ant 1 + Ant 2

Choose Antenna selection

Filter SSID

☐

5.3.1.1 Wireless Mode

To establish a WLAN connection with access points, "Infrastructure" is always set here.

5.3.1.2 SSID-Profiles

Number of different WLAN networks that should be configurable.

5.3.1.3 Phy Mode

Here you define in which frequency band (2.4 or 5 GHz) the access points to which the MC wants to connect operate. You can also use both frequency band at the same time.

5.3.1.4 Country selection

Setting the country in which the MC is to be used. This is important so that the country-specific rules for the use of the frequency bands are observed. Usually, the access points communicate this parameter. In this case, the MC takes over this parameter from the AP.

5.3.1.5 Enable sleep mode

This allows the energy consumption of the MC to be reduced to a limited extent. Activating this function only makes sense for applications that have to work as energy-efficiently as possible.

5.3.1.6 802.11bg bitrate setting

This can be used to control the use of the possible transmit bit rates in the 2.4GHz band.

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

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

The other settings specify the minimum bit rates.

5.3.1.7 802.11a bitrate setting

This controls the use of the minimum transmission bit rates in the 5 GHz band.

5.3.1.8 Power selection

With this parameter the transmitting power of the radio card in the MC can be reduced if necessary. This can be useful if only short distances to the AP's have to be bridged and many other participants work in the frequency band.

5.3.1.9 Antenna gain

This parameter must be used to specify the gain of the connected antenna. This is especially true if, for example, directional antennas are connected whose gain is specified as more than 5 dBi. According to this specification, the WLAN driver reduces the transmission power to comply with the legal requirements depending on the country setting.

5.3.1.10 Antenna selection

If only one antenna connection of the MC is equipped with an antenna, this can be set here. However, you can leave the "Ant 1 + Ant 2" setting as it is, even if only one antenna is connected.

5.3.1.11 Filter SSID

This setting affects the AP list displayed on the "Home" web page. If this option is active, only the AP's are displayed that have a "matching" SSID. Activation makes sense if there are a lot of APs active in the WLAN system that have a different SSID than defined in the profiles.

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 datagrams in seconds.](#)

Destination IP:
[Destination IP address.](#)

Destination port:
[Destination UDP-Port.](#)

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

example:

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

5.3.1.12 Wireless Status Information Service

This option allows the MC to inform the status of the WLAN connection via the devices connected via the **LAN** interface.

Interval

Specifies the time interval in seconds in which the information is sent.

Destination IP

This is the destination address for the status information. A broadcast address can also be specified here so that all devices connected to the LAN can potentially receive this information.

Destination port

Dies ist der UDP-Port auf dem das empfangende Gerät die Daten erwartet.

Format

defines the content of the information to be sent. The following values can currently be queried:

%wlstat	1 = connected	%wlanip	MC IP address to WLAN
%txrate	transmit bit rate	%wlanmac	MC MAC address to WLAN
%ch	Channel	%dname	MC device name
%snr	SNR - value	%SN	MC serial number
%ssid	AP mac	%FW	MC firmware version
%apname	AP name	%Relay	Status of the on board relay

5.3.2 SSID Profile

Starting with firmware 2.09 it is possible to define several WLAN SSID profiles. This allows you to configure the MC so that it can switch between different WLAN areas with different SSIDs without intervention.

Each WLAN profile defines its own parameters for:

- SSID
- Encryption (WPA/WPA2)
- PSK
- 802.1x (EAP parameters incl. user + password)

The 802.1x certificates (server + user) are valid for all profiles.

5.3.2.1 SSID Profile

No.	Parameter	Value	Function
1	SSID	1-32 Zeichen	This is the network name of the WLAN. This is specified by the AP (WLAN system) in 'Infrastructure' mode.
2	Priority	1-10	This value only has a meaning if several SSID profiles are active. The priority determines which profile is preferred to connect to a WLAN. The value 1 means the lowest priority. If only one profile is defined, the value should be set to 1.

You should avoid leaving profiles that are only used for a short time (e.g. during commissioning) active during "normal operation" as well. Otherwise, roaming processes may be unnecessarily prolonged.

5.3.2.2 Profile change action

Here you define what must be done when changing the SSID profile.

No.	Parameter	Value	Function
1	DHCP	Renew Rebind Restart	This setting determines how the MC behaves when switching to this profile in relation to the possibly active DHCP client. With Renew or Rebind it is assumed that the same DHCP server is responsible for both profiles and the IP already assigned can continue to be used. "Restart" restarts the DHCP procedure immediately to obtain a new IP address.


5.3.2.3 Connect Action


This option is only relevant if the DHCP function is active.

Here you can specify what should happen after the MC has connected to an access point.

No.	Parameter	Value	Function
1	DHCP	No action Renew	This setting determines what the DHCP client function of the MC must do when a connection to an access point has been successfully established. This action is then performed each time the access point is changed. A "Renew" may be necessary for appropriately configured WLAN infrastructures that only pass on data if a DHCP action has been performed.

5.3.2.4 Security Parameter

No.	Parameter	Value	Function																								
1	Encryption Mode		Here you define which encryption method is to be used for communication between the MC and the AP. In principle, the AP specifies which method is used on the WLAN network defined with "SSID".																								
			<table><tr><td>1</td><td>no Encryption</td><td></td></tr><tr><td>2</td><td>WEP</td><td>64 oder 128bit Encryption according to the RC4 algorithm</td></tr><tr><td>3</td><td>WPA</td><td>according to 802.11i</td></tr><tr><td>4</td><td>WPA2</td><td>according to 802.11i</td></tr><tr><td>5</td><td>WPA/WPA2</td><td>automatic selection depending on what the AP offers</td></tr><tr><td>6</td><td>WPA3</td><td>Nur WPA3 allowed</td></tr><tr><td>7</td><td>WPA2/WPA3</td><td>WPA 2 oder 3 allowed</td></tr><tr><td>8</td><td>WPA/WPA2/WPA3</td><td>WPA ,WPA2 oder WPA3 encryption allowed</td></tr></table>	1	no Encryption		2	WEP	64 oder 128bit Encryption according to the RC4 algorithm	3	WPA	according to 802.11i	4	WPA2	according to 802.11i	5	WPA/WPA2	automatic selection depending on what the AP offers	6	WPA3	Nur WPA3 allowed	7	WPA2/WPA3	WPA 2 oder 3 allowed	8	WPA/WPA2/WPA3	WPA ,WPA2 oder WPA3 encryption allowed
			1	no Encryption																							
			2	WEP	64 oder 128bit Encryption according to the RC4 algorithm																						
			3	WPA	according to 802.11i																						
			4	WPA2	according to 802.11i																						
			5	WPA/WPA2	automatic selection depending on what the AP offers																						
			6	WPA3	Nur WPA3 allowed																						
			7	WPA2/WPA3	WPA 2 oder 3 allowed																						
			8	WPA/WPA2/WPA3	WPA ,WPA2 oder WPA3 encryption allowed																						
<div> For WPA encryption, we recommend WPA/WPA2(/WPA3) (automatic selection),</div>																											
2	Keying Protocol	only for WPA(2,3)	Here you can set which protocol is selected for key transmission in WPA. Only in exceptional cases should something other than "auto" be selected here																								
			<table><tr><td>1</td><td>TKIP</td><td></td></tr><tr><td>2</td><td>AES</td><td></td></tr><tr><td>3</td><td>Auto</td><td>The MC prefers AES if the AP offers this method.</td></tr><tr><td></td><td></td><td></td></tr></table>	1	TKIP		2	AES		3	Auto	The MC prefers AES if the AP offers this method.															
			1	TKIP																							
			2	AES																							
3	Auto	The MC prefers AES if the AP offers this method.																									
3	Key	with WEP	here the WEP key is specified as a 10 or 26-digit hex value. An example:																								

			If the WEP key consists of the characters "ABCDE", the correct entry is "4142434445".
		with WPA	The "Passphrase" is specified here. This string must be at least 8 - and can be a maximum of 63 characters long. There are applications where the key must be specified as a 32-byte long hex value. If the character string specified here is exactly 64 characters long, a 32-byte hex value is formed and stored as a key.
4	Key Index	only with WEP	Selection of the key index. Usually, "WEP Key 1" is always set.
5	Authentication	only with WEP	Choice between "Open" and "Shared Key" Authentication Usually "Open" is always set
6	Enable 802.11r	only with WPA	With this switch a method can be activated which enables a faster change between the AP's of the WLAN system.  This option may only be activated if the APs support this "Fast Roaming" function according to 802.11r and this option is activated for the specified SSID.

5.3.2.5 EAP

1	Enable EAP		Here, authentication via 802.1x is activated. This deactivates the "Key" parameter under "Security Parameters".																														
2	EAP-Type		<p>There are several EAP methods that can be selected here. Depending on the EAP method, a password must still be specified and certificates may also have to be installed.</p> <table><tr><th></th><th></th><th>User-name</th><th>Password</th><th>Server-Cert.</th><th>Client-Cert + Cert. Password</th></tr><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></table> <p>✓¹ The server certificate does not have to exist. However, in the interests of secure authentication, it is recommended to load a server certificate. ✓² The username does not usually have to be entered with TLS</p>			User-name	Password	Server-Cert.	Client-Cert + Cert. Password	1	TLS	✓ ²	x	✓ ¹	✓	2	TTLS	✓	✓	✓ ¹	✓	3	PEAP	✓	✓	✓ ¹	x	4	LEAP	✓	✓	x	x
		User-name	Password	Server-Cert.	Client-Cert + Cert. Password																												
1	TLS	✓ ²	x	✓ ¹	✓																												
2	TTLS	✓	✓	✓ ¹	✓																												
3	PEAP	✓	✓	✓ ¹	x																												
4	LEAP	✓	✓	x	x																												
3	Inner auth	only with TTLS and PEAP	This defines the protocol used for communication during EAP authentication. MSCHAPV2 is usually the correct setting here.																														
4	EAP Username (public)		EAP user name																														
5	EAP Username (private)		EAP user name for "inner" authentication. Only in exceptional cases does this user name differ from the first specification.																														
6	EAP Password		EAP Password that is assigned in connection with the EAP user name. This password is not required for EAP-Type TLS.																														

5.3.2.6 Certificates

1	Certificate Password		With this password, the MC can access elements of the client certificate.
2	Secure client key		Activating this option prevents the client certificate from being part of the configuration file when it is downloaded from the MC.

In the following, the user has the option of uploading a client certificate and a total of 4 server certificates to the MC. Uploaded certificates can be deleted from the configuration with "Delete".

5.3.3 SCEP

SCEP stands for Simple Certificate Enrollment Protocol. It is an industry standard protocol that enables the automated issuance and management of digital certificates in public key infrastructures (PKI). SCEP was originally developed by Cisco Systems and is now supported by several vendors and PKI implementations.

SCEP simplifies the certificate request process by automating the interaction between endpoints (e.g., devices or users) and the certificate authority (CA). Endpoints can use SCEP to generate certificate signing requests (CSRs) and send them to the CA. The CA then verifies the request and, if approved, issues a digital certificate that can be used by the endpoint for authentication and secure communication.

The SCEP function configurable here is not described in detail in this manual. If you need this function, please contact the manufacturer.

5.3.4 Roaming

In order for the MC to keep up the data connection in a mobile application or an environment with changing reception conditions, the quality of the WLAN connection is continuously checked and, if necessary, a connection is established with other better positioned access points (AP). To do this, the MC must also search for alternative APs on other channels at certain intervals in the specified frequency range. This short-term change of the channel impedes the ongoing data transmission. Therefore, parameters are provided that make this search and the criteria for changing the APs adjustable so that the data connection can be kept as stable as possible, adapted to the operating conditions.

5.3.4.1 Roaming Parameter

The roaming behavior of the MC is determined by the following parameters:

- The set frequency band (2.4 and (or) 5 GHz)
- An SNR threshold that determines whether the MC searches for other APs at short or long intervals.
- Specification of a (long) interval with which the MC scans the channels if the SNR value is **higher** than the specified threshold value.
- Specification of a (short) interval with which the MC scans the channels if the SNR value is **lower** than the specified threshold value.
- The explicit specification of channels to be scanned by the MC.

5.3.4.1.1 AP Density

The SNR threshold is set by setting the "AP Density" parameter.
The following values are (pre)set:

Nr.	AP Density	SNR	Anmerkung
1	autodetect (default)	variabel	This setting activates an algorithm that varies the SNR threshold according to the conditions found. This setting should be preferably configured.
2	high	35	Depending on how "tight" the AP's are mounted in the working area of the MC, a certain threshold value can be set.
3	medium	30	
4	low	25	
5	static client	20	When the MC is used at a fixed location, the threshold can be set relatively low so that no unnecessary scanning is performed.
6	no roaming	0	If scanning should be minimized as much as possible, or if there is only one suitable AP near the MC, you can also set the SNR value to 0 with "no roaming".
7	custom roaming	Para.	This allows the SNR value to be specified individually.

5.3.4.1.2 Channels for Roaming

Especially if the WLAN infrastructure only works in the 2.4 GHz range, it makes sense to define the channels on which the APs are working here. This allows the roaming function of the MC to optimize scanning.
For WLAN infrastructures in the 5GHz range, it only makes sense to specify the channels if only "Non-DFS channels" are used (36, 40, 44, 48).

5.3.4.1.3 Min scan interval

This parameter is used to specify the time interval in seconds at which the MC performs scans if the SNR value of the existing connection is **below** the SNR threshold. 3 seconds is the default value here.

5.3.4.1.4 Max scan interval

This parameter is used to specify the time interval in seconds at which the MC performs scans if the SNR value of the existing connection is **above** the SNR threshold. 60 seconds is the default value here.

5.3.4.1.5 AP Scoring

The decision with which AP the MC establishes a connection is based on an evaluation (scoring) that takes various parameters into account. The parameters that are available also depend on the existing WLAN infrastructure.

The most important value is the signal strength (SNR).
Starting from the SNR value, it can also be taken into account:

- Utilization of the canal
- current transmitting power of the AP's

In addition, statistics are kept on each AP with which a connection has already been established. At the same time, failed attempts are also registered, whereby failed attempts reduce the score.
With this parameter you can switch off the evaluation of the additional parameters and only have the evaluation carried out on the basis of the SNR.

5.3.4.1.6 Blacklist Timer

If the MC changes the AP or the connection to an AP is terminated for some other reason, this AP is initially locked for a certain time. This blocking time can be set with the "Blacklist Timer" parameter. The time is given in seconds. A value of 0 means that the timer never expires and therefore a connection to the AP in the list is only possible after a reset of the MC.

5.3.4.2 Background Scanning

Starting with firmware 2.12r, the MC can use information supplied by the connected access point according to the IEEE 802.11k standard. This 802.11k standard defines how information regarding the existing neighbour APs is provided by the

AP. This information is available if the WLAN system supports this standard and this option is enabled for the corresponding SSID.

The MC can then request a list of suitable neighbor access points from the connected access point, which could potentially be used as new stations in further movement. With this information, the MC can more effectively scan for other matching AP's.

The following options can be selected:

no	option	meaning
1	Include advanced information	The MC uses the current AP list and the 802.11k list to select the channels on which to search for neighboring APs.
2	Only scan channels from neighbor information	The channels to be scanned are selected only from the 802.11k list.
3	Ignore neighbor information	The 802.11k list from the AP is not taken into account.

5.3.4.3 Connection Watchdog

This is an option to monitor the WLAN connection. This is intended to detect a termination of the WLAN connection by registering the received data packets. If no incoming data packets are registered within a certain time, a reassessment of the possible connections is carried out after a scan. This option should only be enabled if the application generates regular traffic over the wireless connection on the LAN clients.

5.3.4.4 Ping-Test

The ping test function is essentially a troubleshooting function. If there are longer interruptions of the WLAN connection during operation and especially after a change of the AP (roaming), this fault can be documented in the debug log with this function. In this case, it is also possible to try to correct the interruption by resetting and restarting the WLAN connection.

The parameters of this function are:

No.	Parameter	Value	Default	Function
1	Ping IP		192.168.170.100	IP address to which pings are sent.
2	Ping-Intervall	1 - 3600	10	Interval in seconds at which the pings are sent
3	Wireless Reconnect		false	This option can be activated to restart the WLAN connection after a certain number of ping responses have failed.
4	Max. missing replies	1-60	10	Maximum number of consecutive failures before restarting the wireless connection.

Enable Ping	<input checked="" type="checkbox"/>
Check this box to enable ping.	
Ping IP:	<input type="text" value="192.168.170.100"/>
IP to use for ping.	
Ping interval	<input type="text" value="10"/>
Ping interval in seconds	
Wireless Reconnect	<input checked="" type="checkbox"/>
Check this box to enable reconnect on ping timeout (Maximum number of missed ping replies reached).	
Max. missing replies	<input type="text" value="10"/>
Missing ping replies that are accepted before reconnect.	

Figure 5.5: Parameters for the ping test function

Since the interruption of the WLAN connection often occurs directly after changing the AP, the ping interval is set to 0.5 seconds for a short time in this situation. As soon as the first response is received correctly, the ping interval returns to the set value. This ensures that such a connection termination is detected quickly and can be corrected promptly with a "Wireless Reconnect" if necessary.

5.3.4.5 Preferred / avoided access points

At this place access points can be defined which are to be either preferred ("Prefer from List") or avoided ("Avoid from List") when roaming the MC device.

This option is only active if the "AP Density" parameter is set to "autodetect".

The AP's are identified by the MAC address of the BSSID.

This function makes sense, for example, if the MC device always moves over a fixed course and is only to use certain APs in an environment with many APs in order to be able to drive this course with as few roaming processes as possible. The "Avoid from List" mode can be useful if AP's are only temporarily well received but are quickly hidden during movement. This can also lead to unnecessary roaming processes.

The "Avoid from List" function does not completely prevent a connection with the listed APs. If no other suitable AP is available, the WLAN driver of the MC will still try to establish a connection.

The 3rd option "strictly avoid" ensures that the MC does not connect to the listed APs even if no other suitable APs are available.

Preferred / avoided access points

Enable AP
(BSSID) List

Prefer from 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	<input type="text" value="00:0E:8E:71:3B:44"/>
BSSID 2	<input type="text"/>
BSSID 3	<input type="text"/>
BSSID 4	<input type="text"/>
BSSID 5	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Remove"/>	

Figure 5.6: Preferred or avoided AP list

5.4 Function of the serial interface

The MC devices in the variants MC1, MC2 and optional MC6C have a serial interface that can be controlled via (W)LAN.

5.4.1 Parameter of the serial interface

The following parameters can be set:

Parameter	Function	Default		
Port active	Activating of the serial port	off		
Device	Port-Address	/dev/ttymxc0		
Baudrate and format	Setting the baud rate, data bits, stop bits and parity handling	9600,8,n,1		
Network configuration	Here you can set the mode in which the serial interface can be controlled via the network. You will find explanations in the next section	TCP-Server, 8888		
Keep alive parameter	Parameters for the TCP server or client mode for monitoring the TCP connection. Please read the explanation below.			
Send trigger configuration	So that not every single received character is sent in its own network packet, 3 criteria for collecting and sending the characters over the network are defined here.			
	1	Byte trigger	maximum number of characters to be buffered.	Default on : 16
	2	Character timeout	Definition of a maximum pause between 2 characters in milliseconds. If this time is exceeded, all characters collected up to that time are sent.	Default on : 100
	3	Frame end trigger	Definition of a character (as HEX value) that leads to the sending of the characters collected so far.	Default off : 0D

Handshake mode	Selection for controlling the handshake lines of the serial interface. Please read the explanation below.

5.4.2 Network-Configuration Parameter

Various modes are available for using the serial interfaces:

1) **TCP/IP-Server-Mode:**

With this setting, the MC opens a socket in the so-called "List" mode. This means that the system waits for a connection to be established on a specific port (local port). The MC only ever holds one connection at a time. In this mode, only the port number is specified as a parameter.

2) **TCP/IP-Client-Mode:**

The MC actively opens a TCP connection on the specified port of another network node. This network node can be another MC or a computer waiting for a connection on the specified port. In addition to the port number (remote port), the IP address of the communication partner must also be specified in this mode (server IP).

3) **UDP/IP-Mode:**

In UDP mode, the MC waits on the "local port" for data to be sent to it via UDP/IP. The received data is sent via UDP/IP to the "Remote-Port" of the remote IP address. If the communication partner is not known, the remote IP address including the remote port can be set to "0.0.0.0" or 0. In this case, the MC takes the sender IP+Port information from the data package that first arrives on the "local port".

The UDP mode should be used in those cases in which e.g. a interruption of the WLAN connection occurs more frequently. However, it must be noted that the UDP protocol does not ensure the complete delivery of the data.

4) **Printerserver-Mode:**

In print server mode, the MC starts a TCP/IP socket in server mode, which is waiting for connections on port 9100. This mode is intended for connecting printers with a serial interface.

5) **COMSERVER-Mode:**

In this mode, the MC can provide virtual COM ports under Windows®. A software product from Wiesemann & Theis (www.wut.de) is used on the PC. The software tool is called COM redirection. The W&T „COM-Umlenkung“ in conjunction with the MC offers the possibility of addressing serial end devices via the network. Simply install the COM redirection driver for Windows® on the PC and enter the IP address and port of the MC.

Please note the license conditions for the use of the „COM-Umlenkung“.

5.4.3 „Keep alive“-Parameter

Once established, a TCP/IP connection remains active until one of the communication partners closes the connection. If the connection between the MC and the network communication partner is interrupted without the TCP/IP connection having been closed beforehand, the MC may not reconnect. The "Keep alive" function sends an "empty" data packet to the other party at the time interval of "keep alive period" seconds. If "keep alive probes" is not received, the MC resets the TCP socket and restarts the connection. Especially if the MC is working in TCP client mode, you should activate the "Keep alive" function by setting the values for "keep alive period" and "keep alive probes" to values > 0.

5.4.4 „Handshake-Mode“ Parameter

In this section you define how the send or receive attendance of the serial communication partners is signalled. The MC signals RTS, DTR indicate attendance for reception. The signals CTS, DSR are input signals via which the connected serial device communicates its attendance to receive, if necessary.

The MC can operate the data flow remotely (remotely) or independently (locally). The user has the following modes to choose from:

- 1) **no Handshake:** the signals CTS/DSR are not evaluated. Only RTS and DTR are set to active if the serial interface is connected via the network.
- 2) **XON / XOFF :** The MC sends and receives the flow control characters XON = 0x11 and XOFF = 0x13. The MC sends an XOFF character to the serial partner when the buffer in the MC is almost full. When the buffer is almost empty, the MC sends an XON character.
- 3) **RTS/CTS:** The MC signals readiness for reception via the RTS signal line and evaluates the CTS signal to determine the readiness for reception of the serial partner.
- 4) **DTR/DSR:** The MC signals readiness for reception via the DTR signal line and evaluates the DSR signal to determine the readiness for reception of the serial partner.

- 5) **Remote:** In this mode, the MC transmits the status of the input signal lines CTS, DSR, DCD and RI to the network communication partner. This is done via a separate socket (port). For this reason, the user must make further specifications for this setting depending on the network mode set.
The states of the signal lines are described as character strings. Certain letters describe the state of a particular signal line. If the letter is capitalized, this means that the signal is active. A lowercase letter means an inactive signal. The assignment is as follows:
- | | |
|------------------|--------------------|
| 'D' = DSR active | ,d' = DSR inactive |
| 'R' = CTS active | ,r' = CTS inactive |
| 'C' = DCD active | ,c' = DCD inactive |
| 'I' = RI aktiv | ,i' = RI inactive |
- To control the RTS and DTR output signal lines, the following characters are sent to the MC via the network:
- | | |
|-----------------------|------------------------|
| 'D' -> DTR set active | ,d' = DTR set inactive |
| 'R' -> RTS set active | ,r' = RTS set inactive |
- 6) **RS422 + RS485:** These are special modes that **must** be set if the serial interface is equipped with an **RS422 / RS485 interface IC**.
With RS485, the RTS line is used to switch between sending and receiving. Therefore it is possible to define the activation of the transmit driver before and after sending data.

5.4.5 Enable dump

If this option is activated, all serially received and transmitted data are recorded in a file in the internal flash memory of the MC. If there are problems with data exchange on the serial interface, an exact error analysis can be carried out in cooperation with the manufacturer. If necessary, ask the manufacturer for the exact procedure.

5.5 Printer server configuration

The print server offers the possibility to connect a printer via the USB interface of the MC.
If a printer is connected and has been recognized by the MC's operating system, the status much follows on the Home page (example).

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

The only parameter of this function is the TCP port on which the MC expects the connections. (TCP server mode)
The default port is number 9100 (RAW port).

5.6 Relay Configuration

Depending on the available connections, the MC has a relay that can be controlled in a certain way. Usually it is used to realize a sleep function e.g. on vehicles with battery operation. The following parameters determine how the relay functions.

Parameter	Function	
Enable	This switches the relay function on or off	
Mode	Type of relay operation:	
	UDP	Control via data received via a UDP/IP socket on a "Local Port".
	TCP	Control via data received via a TCP/IP server socket on a local port.

	internal	Steuerung über das Eingangssignal (AUX-Input)
	SER trigger	Switch on relay if characters for the serial interface were received via (W)LAN.
	WLAN Status	Switch on the relay if there is a WLAN connection, otherwise the relay is switched off.
Relay restore	If the switching position of the relay is to be saved after a restart (reboot by software), mark this option.	
Relay ON	If the switch position of the relay is to be maintained after a restart (rebooting by software), select this option.	
Local Port	Portnumber for the mode UDP oder TCP	
ON Phrase	Character string for switching on the relay in "UDP" or "TCP" mode. If nothing is specified here, every character arriving on the port switches the relay on. Extension from firmware 2.12k: A character string <xx> can be appended to the "ON Phrase" to delay the ON command by xx seconds. Each new ON command with "<xx>" - appendix restarts the switch-on timer.	
OFF Phrase	Character string for switching off the relay in "UDP" or "TCP" mode. Extension from firmware 2.12f: A character string <xx> can be appended to the "OFF Phrase" to delay the OFF command by xx seconds. Each new OFF command with "<xx>" - appendix restarts the switch-off timer.	
Timeout	Time in seconds until the relay is switched off again after switching on. The specification 0 means infinitely long.	

When the correct ON or OFF phrase is received, the MC switches the relay to the corresponding state and responds with a character string corresponding to the current state of the relay.

The response is always 12 characters long (ON or OFF phrase with '\0' characters appended).

To query the status of the relay, you can send any character string to MC and it responds with the current status.

5.6.1 Delayed switching on and off of the relay

As of firmware version 2.12k, it is possible to have the commands for switching the relay on or off executed with a time delay.

For this purpose, directly after the "ON -" or the "OFF Phrase", a time specification set in angle brackets is sent to the corresponding TCP or UDP port of the MC.

e.g.: The ON phrase is set to "ON". Then you can send the string "ON<15>" to the MC, so that the relay switches on delayed by 15 seconds.

When a time delay is active, the MC responds with a character string representing the last command (ON or OFF) followed by the remaining delay in angle brackets.

e.g.: "ON<xx>" where "xx" is the current number of seconds to power on.

5.7 Realtime Clock Configuration

The MC devices have an RTC (Real Time Clock), which is not buffered by a battery. Therefore, once the time has been set, it is lost after the supply voltage has been switched off. After switching on the voltage, the MC starts the RTC with the date 01.01.2000 and the time 00:00:00 o'clock.

Under "Realtime Clock" you can configure a time server that collects current date and time information via the network (WLAN or LAN).

The setting of a time server is required if the SCEP functionality is used.

However, it also has great advantages if system messages from the MC can be provided with a correct time stamp.

Parameter	Funktion
-----------	----------

Enable	Enables the NTP client
NTP-Server	Here you can enter an IP address or a hostname (e.g. ptbtime1.ptb.de) for the time server. The default value is the IP address 192.53.103.108. If a host name is specified, the network connection (WLAN) must be set to a DNS IP (static or via DHCP).
Backup NTP Server	Here you can define a 2nd NTP server
Timezone	The time server supplies a UTC (Coordinated Universal Time) - time. In order to determine the valid local time, the time zone in which the MC is operated must be specified here.
Enable DST/Summertime	In regions with daylight saving time, this option must be activated.

5.8 Input Configuration

The MC is optionally equipped with a digital input. It is possible to transmit the signal status via the network to other network users or to switch the onboard relay via the input. The following parameters are available for configuration:

Parameter	Funktion		
Enable	Enables the digital input		
Mode	1	UDP	sending the state via a UDP socket (Remote IP : Remote Port)
	2	TCP-Client	Sending the signal state to a TCP server socket (TCP-Server-IP : TCP-Server Port)
	3	Relay ON	Switching on the relay when the input signal is active
	4	Relay OFF	Switching off the relay when the input signal is active
	5	Relay toggle	Toggling the relay state when the input signal is activated.
Remote Port Remote IP	IP address and port of the communication partner to which the signal states are sent via UDP/IP.		
TCP-Server Port TCP-Server IP	IP address and port of the communication partner to which the signal states are sent via TCP/IP.		
Relay Timeout (only in Mode „Relay ON“)	If the internal relay is switched via the input signal, you can set a time here that the relay should remain switched on. If this time is set to 0, the time specified in the relay configuration will be used.		
ON Text	Character string that is sent when the signal is active. (above 10V-30V)		
OFF text	Character string that is sent when the signal is inactive. (below 5V)		
Sample Rate	The respective character strings are sent when the input signal changes. Use "Sample Rate" to specify a time interval at which the current state is transmitted even without a signal change.		
Report	With this option a change of the input signal is transmitted to the currently active remote station. For this, either an existing TCP connection must be present, or must be set in UDP mode Remote-IP + Port or a query has already taken place before.		

5.8.1 Input query in UDP mode

In UDP mode it is possible to access the signal status from several stations in the network. If the remote IP is set to "0.0.0.0", the "remote port" - Parameter is used as the local port on which messages are expected from a station in the network. If the MC receives data on this port, it responds with an "ON" or "OFF" message to the requesting station. If the option "Report" is set, signal changes of the input signal are also sent to this last requesting station. If another station requests, the address data of this station <IP:Port> is set as destination for status messages.

5.9 Logging Configuration

The MC offers the following options for recording data and events:

- 1) Store system messages in RAM, FLASH or USB memory and make them available for download under "Statistics -> SystemLog". The download can also be performed with the MC-Config program.
- 2) Send system messages to a syslog server.
- 3) Record the data traffic on the WLAN and (or) LAN interface.
The trace files recorded in this way can be downloaded via the home web page (at the very bottom) or via the MC Config program.

5.9.1 Logging system messages

The options described here for logging system messages or recordings of data traffic are only ever intended to investigate problems that occur and, if necessary, to show how these problems can be remedied. **In normal operation, all settings described here should be reset to the default values.** If log files are still available, you should also use the function: "Statistics -> SystemLog -> Reset System Log".
can be deleted.

The various modules of the MC operating system can generate different "intensive" system messages in the form of formatted text lines. If, for example, there are problems using the serial interface, this part of the program can be specifically forced to record very accurately the events that occur.

It is recommended to configure a time server (NTP) for troubleshooting, so that the debug messages and also the (W)LAN trace recordings can be better assigned to the faults that have occurred.

In general, the system messages are not intended to enable the user to determine the cause of the fault using a defined error list. The DebugLog file should be sent to the manufacturer for verification. The possible system messages are not defined and commented on in detail.

5.9.1.1 Debug Log

Log Destination	The memory in which the file with the messages is stored is set here. Possible targets are:		
	Option	Destination	notation
	RAM	interner RAM Speicher	The messages recorded in this way are lost after a "power down" or a reset.
	Internal FLASH	interner FLASH Speicher	After a "Power Down" or a reset, the following messages are written to the end of any existing debug file. The maximum size of the file is 16 MByte.
	USB	Externer USB-FLASH Speicher	In this mode, a numbered new debug file is created after each reset. So "DebugLog0.dat", "DebugLog1.dat" etc. The size of the file is only limited by the capacity of the USB memory.

5.9.1.2 Debug Information

In addition to the actual message text, you can define which additional information is also specified for each message.

N0.	Information	notation
1	Absolute Timestamp	Time in "day.month Hour:minute:second.microsecond" format If no time has been received via the network (NTP), the time since system startup is shown here.
2	Relative Timestamp	Time specification as acounter of the past milliseconds since the start.
3	Repeat Counter	Counter indicating how often this message has been issued since system startup.
4	Thread	Name or ID of the process that issues this message
5	Source file name	a) name of the program file and b) Number of the program line that generated this message.
6	Class	There are classes: ERROR WARN INFO TRACE that are active according to the debug settings (Default, Detailed, Maximum).

Example of an output line:

5224381 302808 1:27:02.610085 SerPoll SerialUart.c [621] INFO: Ser1: Write 16 bytes to uart

Elements:

2	3	1	4	5a	5b	Class	Message
2934692	158343	0:48:52.921718	SerPoll	SerialUart.c	[621]	INFO:	Ser1: Write 16 bytes to uart

5.9.1.3 Syslog Server

These messages can also be sent to a syslog server. The IP address of this server is defined for this purpose. If "0.0.0.0" is specified, this function is not active.

To use a syslog server, it should be accessible via the LAN port. Sending syslog messages to a server via WLAN is not recommended because they can significantly increase the data traffic via WLAN. In addition, the messages are usually lost in the event of a fault on the WLAN connection.

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.](#)

Figure 5.7: Debug Log Parameter

5.9.1.4 Traffic Dump Configuration

With the "Traffic Dump Configuration" function, data traffic can be recorded on the LAN and (or) WLAN interface. The generated files can be analyzed with known programs such as Wireshark.

Traffic Dump Configuration

Dump Wireless

☒

Check this box to enable dump of wireless packets in monitor mode.

Monitor Dump Destination:

Internal Flash

Select destination for WLAN monitor mode dump.

Filter

Only own traffic

Select method for filtering packets.

Dump Control

Disable Dumper if Flash is full

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:

Internal Flash

Select destination for ethernet monitor dump.

Dump Control

Delete oldest dump files if flash is full

Select desired action if dumping is enabled but flash is full.

Figure 5.8: Traffic Dump Configuration

Parameter	Function
Dump Wireless	This activates the recording of data packets on the WLAN side.
Monitor Dump Destination	Setting the storage location for the WLAN recordings
	1) Internal Flash Internal flash memory (ca. 400MByte)
	2) USB External USB-Memory (depending on capacity of the memory stick)
Filter	In order to record WLAN data over as long a period as possible, you can activate a filter here that only stores the data sent and received by the "own" WLAN wireless card. Alternatively, you can also specify a self-defined filter. To do this, however, you should familiarize yourself with the filter format of the pcap module. The options are: 1) no Filter 2) only own traffic 3) Custom
Dump Control	With "Dump Control" you can set what happens when the memory limit of the internal flash or the USB memory is reached. 1) The recording is stopped 2) The oldest recording is deleted and the recording continues with a new file.
Filesize (is only displayed if "Monitor Dump Destination = USB)	If the recordings are stored in the USB memory, you can set the maximum size of the file here: Small = 8 MByte Medium = 32 MByte (default) Large = 128 MByte
Dump LAN	This activates the recording of data packets on the LAN side.
Monitor Dump Destination	Setting the storage location for the LAN recordings
	1) Internal Flash Internal flash memory (ca. 400MByte)
	2) USB External USB-Memory (depending on capacity of the memory stick)
Dump Control	With "Dump Control" you can set what happens when the memory limit of the internal flash or the USB memory is reached. 1) The recording is stopped 2) The oldest recording is deleted and the recording continues with a new file.
Filesize (is only displayed if "Monitor Dump Destination = USB)	If the recordings are stored in the USB memory, you can set the maximum size of the file here: Small = 8 MByte Medium = 32 MByte (default) Large = 128 MByte

During recording, the current recording file is closed at a size of 32MByte (or 8 or 128MByte) and a new file is opened. The stored file is then compressed and written to the file system as a *.gz file. The original file is then deleted. Depending on the compression rate of the data, the data traffic can be logged over a long period of time.

The compressed files can then be downloaded from the MC's "Home" website. The list of dump files is located at the end of the "Home" page below the list of access points.
The explanation for the composition of the file names is explained here -->58

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)

Figure 5.9: Wireless und Ethernet dump files

As additional information, the number of bytes and data packets stored in the current dump is specified. There is also information about the number of data packets that were rejected (drop count). The file names can be clicked and downloaded.



This way of recording the data traffic on the interfaces places a heavy load on the FLASH memory in particular and **should only be activated for fault diagnosis. In productive use, this function should be deactivated.**

The dump files can be deleted via the function: "Statistics -> SystemLog -> Reset System Log".

5.9.1.4.1 Downloading Debug Files with the MC-Config Program

To download all log files from the MC in one operation, you can select the following command in the MC-Config program via the context menu (right click on MC entry):

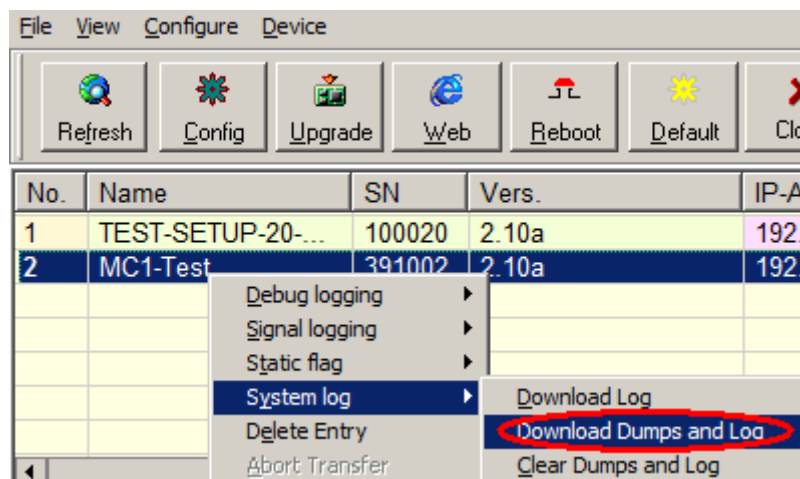


Figure 5.10: Download Dumps and Logs with the MC-Config-Program

A dialog opens for defining the folder in which the files are created. Then a dialog opens in which you can select the log and dump files for downloading. Before opening this dialog all active dump processes are stopped. The remaining pcap files are compressed. This process may take some time. This status is displayed in the "Status" column. The following dialog is then displayed:

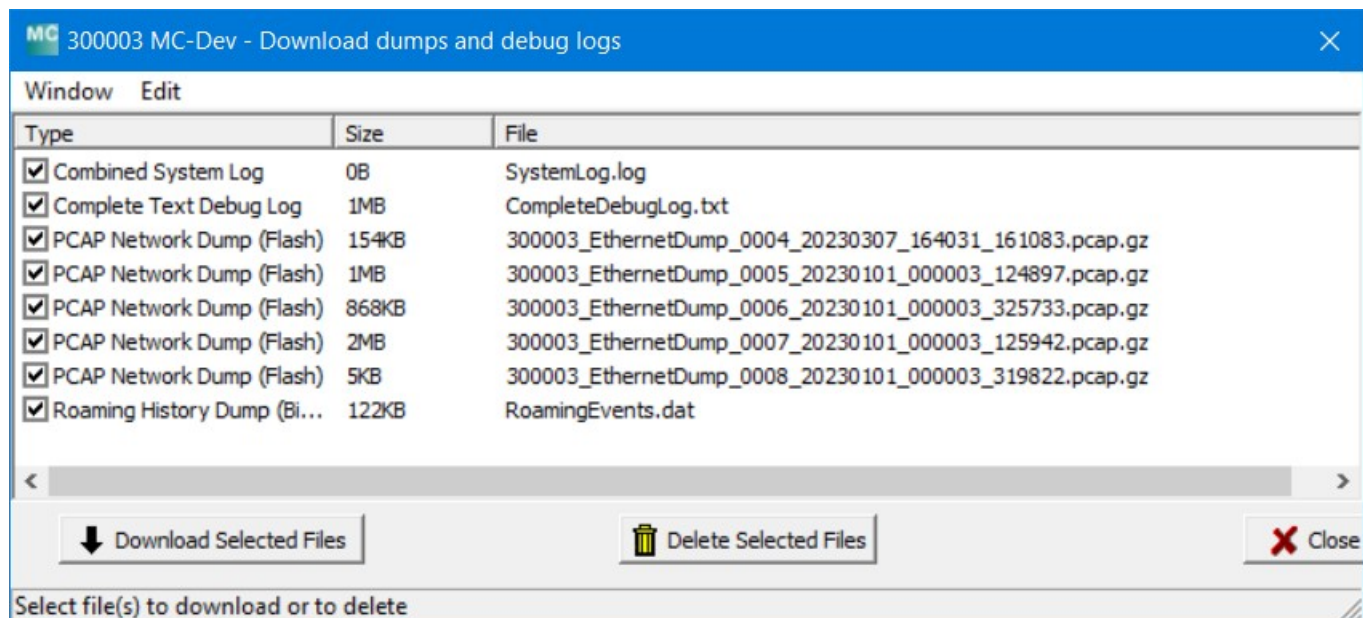


Figure 5.11: File selection for download or deletion

In this selection the file "SystemLog.log" is always listed, which contains a lot of information about the current status of the MC with the last system messages and the current config data.

This file is always important when analyzing error situations.

The "CompleteDebugLog.txt" file contains the system messages that occurred during operation depending on the settings made under "Logging". This file is filled up to a length of 16MByte. When this size is reached, it is renamed to "CompleteOldDebugLog.txt". An existing CompleteOldDebugLog.txt file is deleted beforehand. Further system messages are then written to a newly created " CompleteDebugLog.txt".

The dump files are listed in the order in which they were written. First the LAN dump files then the WLAN dump files. If a time server (--> "Realtime Clock") could be used, the date and time of the start time appears in the file names of the dump files. This is very helpful if you can use it to select exactly the file that could have documented the error that occurred.

Der Dateiname setzt sich wie folgt zusammen:

element	meaning	notice
nnnnn_	Serialnumber of the MC device	
WLAN(Ethernet)Dump		
xxxx	Numbering of the file	This is important if no time server is set up and the MC restarts in between.
YYYYMMDD	Date of recording	Without realtime clock the MC starts with the date 01.01.2000
_hhmmss_uuuuuu	start time	Specification of hour-minute-second-microsecond Without realtime clock the time starts at 00.00.00_000000

From this list you can select one or more files and either download or delete them.

Log and dump files are shown in the list, which are stored in the internal flash drive as well as in the possibly inserted USB stick. Files on the USB stick are marked with"(USB)".

5.9.1.5 Debug Configurations

Here you can define the intensity of the system messages for the different program parts. Messages with a specific debug level are embedded in the program.

The following debug levels are defined:

Level	Function
ERROR	Occurrence of an error that prevents a desired function.
WARN	Occurrence of a condition that delays a desired function
INFO	Message documenting an event that occurs
TRACE	Message documenting the flow of a function

Individual debug levels can be set for the following program parts:

Modul	Function
Wireless	Reports processes in connection with the WLAN interface. The focus is on recording access points and roaming processes.
WPA Supplicant	Here, authentication processes can be documented.
DHCP	Messages generated by the DHCP client or server
Serial	Messages generated by the module for controlling the serial interface
Relay	Messages generated by the module to control the relay
Aux-Input	Messages generated by the module for controlling the digital input
Base System	Messages generated by the general operating system
Network Bridge	Messages generated by the bridge module.

The program parts have 4 debug levels:

Level	Messages issued
Default	ERROR
Information	ERROR + WARN
Detailed	ERROR + WARN + INFO
Maximum	ERROR + WARN + INFO + TRACE

The "Maximum" level should really only be activated for the program module for which there is really a problem. This level may generate such a large number of debug messages that the performance of the primary application suffers.

Debug Configurations

Debug Wireless:

Detailed

Select log configuration for wireless.

WPA Supplicant details:

Detailed information

Select detail level of WPA supplicant. Only increase this if connection can't be established (Reboot needed!).

Debug DHCP:

Default

Select log configuration for DHCP.

Debug Serial:

Default

Select log configuration for serial ports.

Debug Relay:

Default

Select log configuration for the relay port

Debug Aux-Input:

Default

Select log configuration for the auxin port

Debug Base System:

Detailed

Select log configuration for base system.

Debug Network Bridge:

Detailed

Select log configuration for network bridge.

Figure 5.12: Debug Configurations

6 Statistics Menu

Under this menu item you will find possibilities to evaluate the activity of the MC with regard to the LAN + WLAN interface and to display and save stored system messages.

6.1 Statistics - System Log

Under this menu item the system messages are displayed which are stored in the MC. Which messages are stored depends on the settings under "Configuration->Logging". There you can adjust the "intensity" of the output for some software modules separately.

The "Download System Log" button has the effect that the last messages and the current configuration are combined in one file and downloaded from the MC.
The "Reset System Log" button deletes all messages and, if necessary, the files that were created during the recording of data traffic on the WLAN or LAN interface.

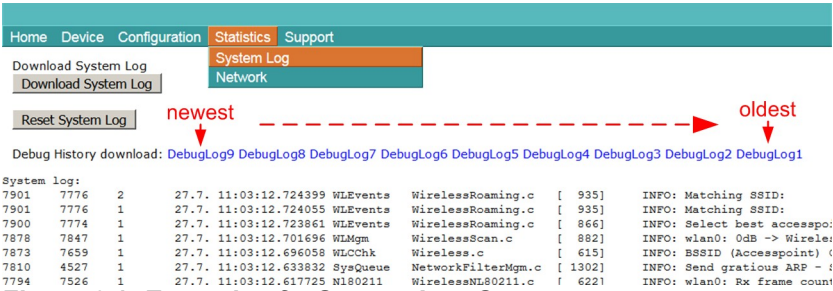


Figure 6.1: Example of a System Log Output

Starting with firmware 2.11p1, a list with links is displayed under "Debug history download". The DebugLog files can be downloaded from the MC device via these links. The first link (newest) points to the current DebugLog.dat file. This is an uncompressed text file. The following links point to older recordings that are stored as compressed files. These files have the following names: DebugLog.dat.xxxxx.old.gz
xxxxx is a numbering that counts down from left to right.

6.2 Statistics - Network

This sub menu shows statistics of the network interfaces. Under "Network Interface eth0" statistical data are given for the LAN interface of the MC. The same for the WLAN interface can be found under "Network Interface wlan0". "Network State Information" shows which ports are open on the MC and which connections currently exist.

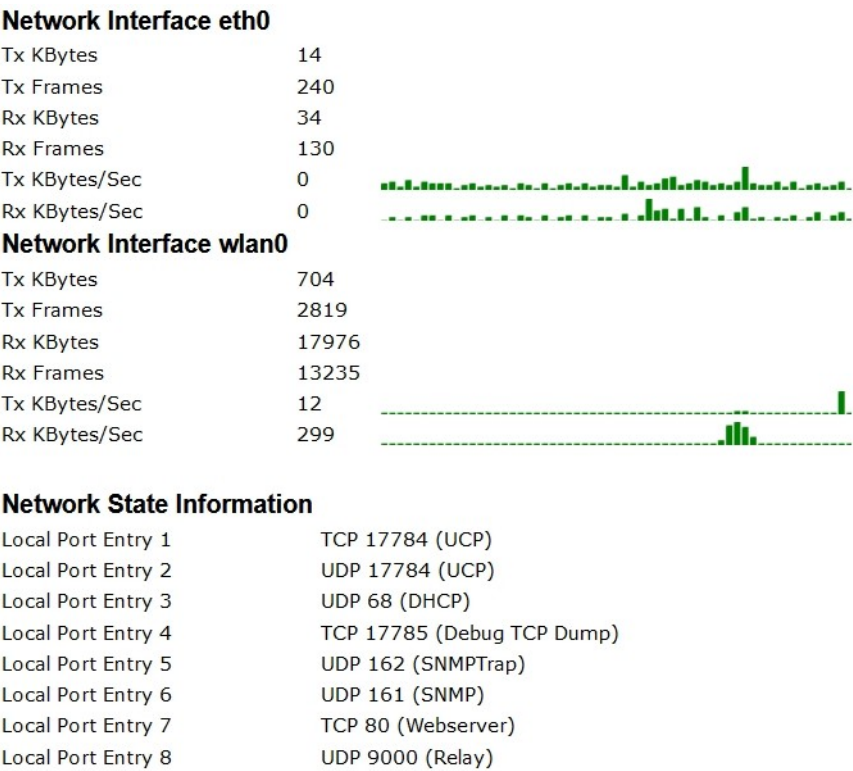


Figure 6.2: Example of an Statistics Network Screen

7 Configuration of MC devices with an USB memory stick

Starting with firmware 2.12a there are 2 possibilities to use a USB stick to configure the MC:

- transfer of a configuration file from the USB stick to the MC device during a "default reset" initiated by the reset button.
- permanently inserted USB stick on which both the configuration and the firmware for a MC device is stored.

7.1 Transfer of a configuration file during a "default reset"

If a "default reset" is performed via the reset button, the MC checks whether a USB stick is available. If yes, a file "Default.cfg" is searched in the root directory of the USB stick. If this file is available, this configuration is adopted for the MC device after the restart.

7.2 Application for the Config-USB-Stick

The aim is to quickly and easily replace a defective MC device with another MC device by simply inserting the USB Config stick from the defective MC device into the replacement device. The replacement MC checks during the boot process whether there is a firmware file on the stick that differs from the firmware in the replacement MC. If this is the case, the firmware is first transferred from the stick to the replacement MC and flashed. After the reboot, the config file of the USB Config stick is used for further operation. The replacement MC will therefore work with exactly the same firmware and configuration as the original MC.

7.2.1 Initializing a USB memory stick

Initialization of the USB memory stick is done via the MC Config program. This function is enabled by a parameter specified as an argument when the MC Config program is started.

This argument is: InitUsbConfigStick (case sensitive!)

An additional selection "Init USB Config Stick" appears in the context menu.

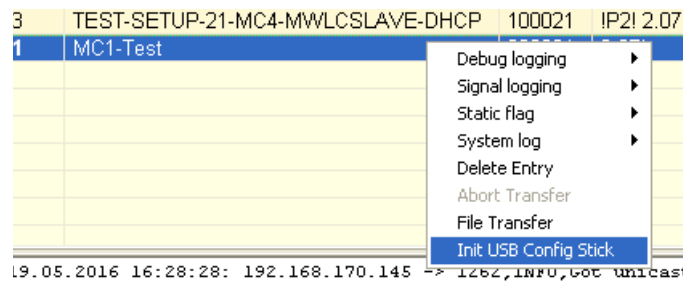


Figure 7.1: Init USB Config Stick



Attention!

When the USB memory stick is initialized, all data on the stick is deleted!

This command reformats the USB memory stick (ext4 format) and creates certain files, which make this special stick recognizable as a config stick. One of these files is the config file currently available on the MC device. After transferring the files, the MC is restarted. During the boot process, this stick is then recognized as a config stick and the config file stored there is used for further operation.

It is designed so that the USB stick always remains plugged into the MC device. This ensures that a change of the configuration takes place in the Config-Stick as well as a change of the MC-firmware is also stored in the USB stick. Thus, another MC device that is started with this Config-Stick will have the same function as the MC device from which the Config-Stick was removed.

If the USB stick is removed, the MC makes a reset very soon. The following boot process is stopped until a Config USB

memory stick is detected. Until then the MC remains blocked. This state is signaled with a blue flicker of the power LED. If you want to run the MC again without Config-USB memory stick, you have to make a "Factory Default Reset" by pushing the reset button continuously (see Cap. 2.2).

8 REST-API

Starting with firmware 2.12p it is possible to perform the following functions via HTTP(S) with GET and POST:

- 1) Download of the config file
- 2) Upload of a config file
- 3) Upload of a firmware
- 4) Status request
- 5) Certificate upload
- 6) Download of the WLAN + LAN - recordings ((W)LAN dump files)
- 7) Download of the system log file
- 8) Download of the CA certificate from the OpenVPN server
- 9) Download of a configuration file for an OpenVPN client

Funktion	URL	Methode	Ergebnis
Download the active config file	http(s)://<MC_IP>/API/Cfg/GetRunning	GET	Text
Download the default config file	http(s)://<MC_IP>/API/Cfg/GetDefault	GET	Text
Upload of a config file	http(s)://<MC_IP>/API/Cfg/Set	POST	
Upload of a firmware file	http(s)://<MC_IP>/API/Firmware/Upgrade	POST	
Status request	http(s)://<MC_IP>/API/Status	GET	JSON
Upload a certificate	http(s)://<MC_IP>/API/Cfg/ImportCertificate	POST	
Download the file list of the existing WLAN+LAN+recordings	http(s)://<MC_IP>/API/Debug/CaptureFiles	GET	JSON
Download a file	http(s)://<MC_IP>/API/Debug/CaptureFile/<FileName>	GET	Binär
Download the systemlog file	http(s)://<MC_IP>/API/Debug/Get/SystemLog	GET	TEXT
Download the CA certificate from the 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

With the command line tool "curl" you can execute the functions of the REST-API via script automatically or via command line. "curl" also processes the transfer of any user/password information.

This is how the command lines for the various functions would look like:

Function	Command
Cfg/GetRunning	curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Cfg/GetRunning"
Cfg/GetDefault	curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Cfg/GetDefault"
Cfg/Set	curl -N -u user:password -k -X POST -F "image=@<config file>" "https://<MC_IP>/API/Cfg/Set"
Firmware/Upgrade	curl -N -u user:password -k -X POST -F "image=@<firmware file>" "https://<MC_IP>/API/Firmware/Upgrade"
Status	curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Status"
ImportCertificate	curl -N -u x:yy -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"
Debug/CaptureFiles	curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Debug/CaptureFiles"
Debug/CaptureFile	curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Debug/CaptureFile/<FileName>"
Debug/Get/SystemLog	curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/Debug/Get/SystemLog"
VPNServer / GetCACert	curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/OpenVPNServer/GetCACert"

VPNServer / `curl -N -u user:password -k --output <destination file> "https://<MC_IP>/API/OpenVPNServer/GetClientConfig`
GetClientConfig

with the "Cfg/Set" function you can also transfer config files with only single parameters.
If, for example, a file with the content:

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

is transmitted, the MC switches off the WLAN interface.

A file with the contents:

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

switches the WLAN interface on again.

Further information about the curl tool can be found at: <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 right holders 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>

10 Statements and instructions according to FCC and Industry Canada Rules

10.1 Information for host integrators of the radio module

CAUTION:

Host integrator is still responsible for testing their end product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral etc.). In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances the host integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

10.1.1 Labeling instructions for host devices

The FCC and IC ID are permanently fixed on a label on the module, and, if the identification numbers are not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. This exterior label can use wording such as the following:

“Contains Transmitter Module FCC ID: RYK-WPEA-121N“

“Contains Transmitter Module IC: 6158A-WPEA121NW“

Any similar wording that expresses the same meaning may be used

Additionally the two part statement must be fixed on the host device:

“This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.”

10.1.2 RF Exposure / collocation requirements

The fixed external antennas used for this mobile transmitter must provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.”

10.1.3 Information to end user

End users may not be provided with the module installation instructions. For information to users, all relevant instructions that pertain to all components of a composite device are required. For example, Class A or Class B statements in Section 15.105; all warning statements and special instructions as required by Sections 15.21 and 15.27; and all Part 18 applicable instructions / attestations must be clearly stated. However, realistic variations in editing to clarify the language and structure are permitted as long as all the relevant points applicable to all of the components are represented.

10.2 FCC and Industry Canada warning statements and special instructions

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

If the device is going to operated in 5.15 – 5.25 GHz frequency range, then is restricted in indoor environment only.

Note: High power radars are allocated as primary users of the bands 5.25 – 5.35 and 5.65 – 5.85 MHz and these radars could cause interference and/or damage to Wireless - LAN devices.