

WLAN Radio Modem 802.11 a/b/g/n

# HG G-76343/4/5

Top Hat Rail or Flange Casing

Variants HG G-76343-A / HG G-76344-A (including version for 4G(LTE)/5G) / HG G-76345-A and version with 802.11 ac

English, Revision 09

Date: 24.01.2024

Dev. by: TC

Author(s): RAD



**GÖTTING**

**Basic characteristics of the radio modems HG G-76343-A / HG G-76344-A / HG G-76345-A**

- ♦ WLAN client for 802.11 a/b/g/n via 2.4 + 5 GHz WLAN, data rates up to 300 MBit/s, variant ac additionally with 802.11 ac and data rates up to 866 MBit/s
- ♦ Integrated OpenVPN client
- ♦ Different Bridge modes for connecting the LAN clients: NAT / Single Client NAT / Single Client Cloning / Level 2 Bridge / MWLC Mode (transparent tunnel mode)
- ♦ WEP, 802.11i WPA-WPA2-WPA3-AES-TKIP-PSK
- ♦ WPA Enterprise 802.1x PEAP LEAP TLS TTLS
- ♦ Certificate management for the authentication via 802.1x
- ♦ SCEP (Simple Certificate Enrollment Protocol)
- ♦ Fast-Roaming 802.11r
- ♦ 2x antenna connectors for diversity
- ♦ 1-4x Gigabit LAN interfaces
- ♦ 1x serial interface (not in HG G-76345): RS232, RS485 or RS422, Serial-Client via TCP or UDP
- ♦ 1x USB 2.0 interface, also for additional interfaces
- ♦ 1x switching relay
- ♦ 1x AUX input (optional)
- ♦ Voltage supply 10-60V or via PoE (LAN)
- ♦ Robust aluminum casing with different mounting
- ♦ Configuration via the internal web server, REST-API or with the help of the dedicated MC-Config program
- ♦ Variant with LTE/4G (Public LTE or Private LTE) or 5G

---

© 2024 Götting KG, errors and modifications reserved.

The Götting KG in D-31275 Lehrte has a certified quality management system according to ISO 9001.



# Contents

<b>1</b>	<b>About this Document.....</b>	<b>7</b>
1.1	Presentation of Information .....	7
1.1.1	Warning Notices.....	7
1.1.2	Symbols.....	8
1.2	Declaration of Conformity .....	8
<b>2</b>	<b>Introduction.....</b>	<b>9</b>
2.1	Versions / Variants.....	10
2.2	Interfaces.....	10
2.3	Indicators and Connectors.....	11
2.3.1	All Variants.....	11
2.3.2	Connectors HG G-76343-A .....	11
2.3.3	Connectors HG G-76344-A .....	12
2.3.4	Connectors HG G-76345-A .....	12
2.4	Pin Assignments.....	12
2.4.1	5 pin M12 Socket Power & Relay.....	12
2.4.2	9 pin Sub-D Socket Serial .....	13
2.5	LEDs.....	13
<b>3</b>	<b>Commissioning .....</b>	<b>15</b>
3.1	Mounting .....	15
3.1.1	Casing Type XA with Top Hat Rail Mounting on narrow Side (all Variants) .....	15
3.1.2	Casing Type YA with Top Hat Rail Mounting on broad Side.....	15
3.1.3	Casing Type ZA with Flange Casing.....	16
3.2	Initial Startup via LAN.....	16
3.3	The MC-Config Program .....	17
3.4	Commissioning via the Web Interface.....	17
3.5	Reset to Factory Settings.....	17
<b>4</b>	<b>MC-Config Program .....</b>	<b>18</b>
4.1	Functional Description.....	18
4.2	IP Protocols and Ports Used .....	18
4.3	Encrypted Transmission .....	18
4.4	Initial Startup.....	19
4.5	Operation.....	20
4.5.1	Operating Elements.....	20
4.5.2	Information Shown by the List View Items.....	21
4.5.3	Arrangement of Columns.....	23
4.5.4	Settings for the Logging of Messages .....	24
4.5.5	Context Menu of the List Items.....	25
4.6	Menus .....	26
4.6.1	File .....	26
4.6.2	View .....	27
4.6.3	Configure.....	27
4.6.4	Device .....	31
4.7	The Config Function .....	32
4.7.1	Variable number of input fields.....	33
4.8	Access Protection with Username and Password.....	33
4.9	Firmware-Updates.....	34
4.10	Downloading the Config from Multiple Devices.....	34
4.11	Search WLAN Clients.....	34
4.11.1	IP Ranges.....	34
4.12	Logging System Messages .....	36
4.12.1	Configuration of the Logging Parameters.....	36

4.12.2	Recording Debug Messages.....	37
4.12.3	Download of Debug Messages and (W)LAN Logs.....	37
<b>5</b>	<b>Parameter Setting via the Web Interface.....</b>	<b>38</b>
5.1	Information Site / Home.....	38
5.1.1	System Information.....	38
5.1.2	Wireless Status Information.....	39
5.1.3	Wired LAN Status Information.....	42
5.1.4	Relay Status Information / IO-Info (Optional).....	42
5.1.5	Serial1.....	43
5.1.6	Network Information .....	44
5.1.7	Access Point Information .....	44
5.1.8	HTTPS Webinterface.....	45
5.1.9	Storage Status Information .....	45
5.1.10	WLAN and LAN Dump Files.....	46
5.2	Device Menu (Firmware and Configuration Management) .....	46
5.2.1	Firmware.....	46
5.2.2	Configuration Management.....	47
5.2.3	Network Test.....	48
5.3	Configuration (of the Operating Parameters).....	49
5.3.1	Admin Menu.....	50
5.3.2	Network Menu.....	52
5.3.2.1	IP Address.....	52
5.3.2.2	IPV6 Settings (experimental) .....	52
5.3.2.3	mDNS Settings.....	53
5.3.2.4	Bridge .....	53
5.3.2.5	MQTT Client.....	53
5.3.3	Wireless / Parameters of WLAN Interface.....	53
5.3.4	Serial Port .....	53
5.3.5	Printer Server .....	53
5.3.6	Relay .....	54
5.3.6.1	Relay Parameter .....	54
5.3.6.2	Delayed switching on and off of the relay.....	55
5.3.7	Realtime Clock .....	55
5.3.8	Input (optional) .....	56
5.3.9	Logging (Debug) .....	56
5.4	Statistics.....	56
5.4.1	Statistics – System Log.....	56
5.4.2	Statistics - Network.....	57
5.5	Support .....	57
<b>6</b>	<b>Bridge Modes.....</b>	<b>58</b>
6.1	Bridge not active Mode .....	58
6.2	LAN Client Cloning.....	59
6.3	NAT and Single Client NAT Mode.....	62
6.3.1	Forwarding rules for NAT .....	64
6.3.2	DHCP Server Settings.....	65
6.3.3	Static DHCP Server entries.....	65
6.4	Level 2 Pseudo Bridge Mode.....	67
6.5	MWLC Mode .....	69
6.5.1	MWLC Master.....	70
6.5.2	MWLC Slave.....	70
<b>7</b>	<b>MQTT Client .....</b>	<b>71</b>
<b>8</b>	<b>Wireless (WLAN Interface) .....</b>	<b>73</b>
8.1	Main Parameter .....	74
8.2	Wireless Status Information Service.....	75
8.3	Wireless SSID Profile.....	76
8.3.1	SSID Profile.....	76
8.3.2	Profile Change Action .....	76
8.3.3	Connect Action.....	77

8.3.4	Security Parameters .....	78
8.3.4.1	EAP .....	79
8.3.4.2	Certificates .....	80
8.4	SCEP .....	80
8.5	Wireless Roaming .....	80
8.5.1	Roaming Parameter .....	80
8.5.1.1	AP Density .....	81
8.5.1.2	Channels for Roaming .....	81
8.5.1.3	Min scan interval .....	81
8.5.1.4	Max scan interval .....	81
8.5.1.5	AP Scoring .....	81
8.5.1.6	Blacklist Timer .....	82
8.5.2	Background Scanning .....	82
8.5.3	Connection Watchdog .....	82
8.5.4	Ping Test .....	82
8.5.5	Preferred / avoided access points .....	83
<b>9</b>	<b>Serial Interface .....</b>	<b>84</b>
9.1	Parameters of the Serial Interface .....	84
9.2	Network-Configuration Modes .....	85
9.3	Keep Alive Settings .....	85
9.4	Handshake Mode Settings .....	85
9.5	Enable Dump .....	86
<b>10</b>	<b>Debug / Logging .....</b>	<b>87</b>
10.1	Record System Messages .....	87
10.1.1	Setting the Debug File Destination .....	88
10.1.2	Set Additional Debug Information .....	88
10.1.3	Syslog Server .....	89
10.2	Traffic Dump Configuration (Recording of Data Traffic from the LAN or WLAN Interface) .....	90
10.3	Downloading Debug Files with the MC-Config Program .....	92
10.4	Debug Configurations .....	93
<b>11</b>	<b>Configuration with USB Memory Stick .....</b>	<b>96</b>
11.1	Transfer of a configuration file during a default reset .....	96
11.2	Application for the Config-USB-Stick .....	96
11.2.1	Initializing a Config-USB-Stick .....	96
<b>12</b>	<b>REST-API .....</b>	<b>98</b>
12.1	Functions and Command Lines .....	98
12.2	Outputs for the Status Function .....	99
12.3	REST API Queries with curl .....	102
<b>13</b>	<b>Technical Data .....</b>	<b>103</b>
13.1	Hardware .....	103
13.2	WLAN Interface .....	104
13.3	Output Power & Sensitivity .....	104
<b>14</b>	<b>HG G-76343/4/5-A ac (802.11ac) .....</b>	<b>106</b>
14.1	Technical Data HG G-76342/4/5-A ac .....	107
14.1.1	WLAN Interface .....	107
14.1.2	Output Power and Sensitivity .....	107
<b>15</b>	<b>HG G-76344XA/ZA 4G LTE 5G .....</b>	<b>108</b>
15.1	Variants HG G-76344-A LTE .....	108
15.2	Connectors .....	109
15.3	Mobile Radio Interface .....	109
15.4	Use as an LTE Router .....	109
15.5	How to Insert the SIM Card .....	110
15.6	LTE LED .....	111
15.7	Additional outputs in the web interface .....	112
15.7.1	Mobile Radio Status .....	112

15.7.2	Network Information .....	113
15.8	Input of the Parameters for the Cellular Connection .....	113
15.9	REST-API .....	114
15.10	Technical Data .....	115
<b>16</b>	<b>Open Source Compliance Information.....</b>	<b>116</b>
<b>17</b>	<b>Statements and instructions according to FCC and Industry Canada Rules .....</b>	<b>117</b>
17.1	Information for host integrators of the radio module .....	117
17.1.1	Labelling instructions for host devices .....	117
17.1.2	RF Exposure / collocation requirements .....	117
17.1.3	Information to end user .....	117
17.2	FCC and Industry Canada warning statements and special instructions .....	117
<b>18</b>	<b>List of Figures .....</b>	<b>119</b>
<b>19</b>	<b>List of Tables .....</b>	<b>122</b>
<b>20</b>	<b>Index .....</b>	<b>124</b>
<b>21</b>	<b>Document Changelog .....</b>	<b>128</b>
<b>22</b>	<b>Copyright and Terms of Liability.....</b>	<b>129</b>
22.1	Copyright .....	129
22.2	Exclusion of Liability .....	129
22.3	Trade Marks and Company Names .....	129

## 1

# About this Document

## 1.1 Presentation of Information

For you to be able to use your product simply and safely this device description uses consistent warning notices, symbols, terms and abbreviations. Those are described in the following sections.

### 1.1.1 Warning Notices

In this device description warning notices appear before sequences of actions that may lead to damage to persons or property. The listed actions for the danger prevention have to be observed.




Warning notices have the following structure:

 <b>SIGNAL WORD</b>
<b>Kind or source of the danger</b>
Consequences
► Danger prevention

- ♦ The **warning symbol** (warning triangle) indicates danger to life or risk of injury.
- ♦ The **signal word** indicates the severity of the danger.
- ♦ The paragraph **kind or source of the danger** names the kind or source of the danger.
- ♦ The paragraph **consequences** describes the consequences of not observing the warning notice.
- ♦ The paragraphs for **danger prevention** explain, how to avoid the danger.

The signal words have the following meanings:

**Table 1** Hazard classification according to ANSI Z535.6-2006

Warning Symbol, Signal Word	Meaning
 <b>DANGER</b>	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
 <b>CAUTION</b>	CAUTION indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.
<b>NOTICE</b>	NOTICE indicates property damage: The product or the environment could be damaged.

### 1.1.2 Symbols

In this device description the following symbols and formatting are used:



If this information is ignored the product may not be operated in an optimal way.



Indicates one or more links to the Internet.

– [www.goetting.de/xxx](http://www.goetting.de/xxx)

– [www.goetting.de/yyy](http://www.goetting.de/yyy)



Indicates tips for easier operation of the product.

- ✓ The check mark lists a requirement.
- ▶ The arrow shows an action step.  
The indentation shows the result of an action or an action sequence.
- ♦ Program texts and variables are indicated through the use of a `fixed width font`.
- ♦ Menu items and parameters are shown in *cursive characters*.
- ♦ Whenever the pressing of letter keys is required for program entries, the required **L**etter **K**eys are indicated as such (for any programs of Götting KG small and capital letters are equally working).

## 1.2 Declaration of Conformity



This product complies with the relevant harmonization legislation of the European Union. The relevant harmonized European standards and directives mentioned in the Declaration of Conformity were used to assess conformity.



You can request the EU declaration of conformity from Götting KG or download it under the following link

<https://www.goetting-agv.com/components/76343>





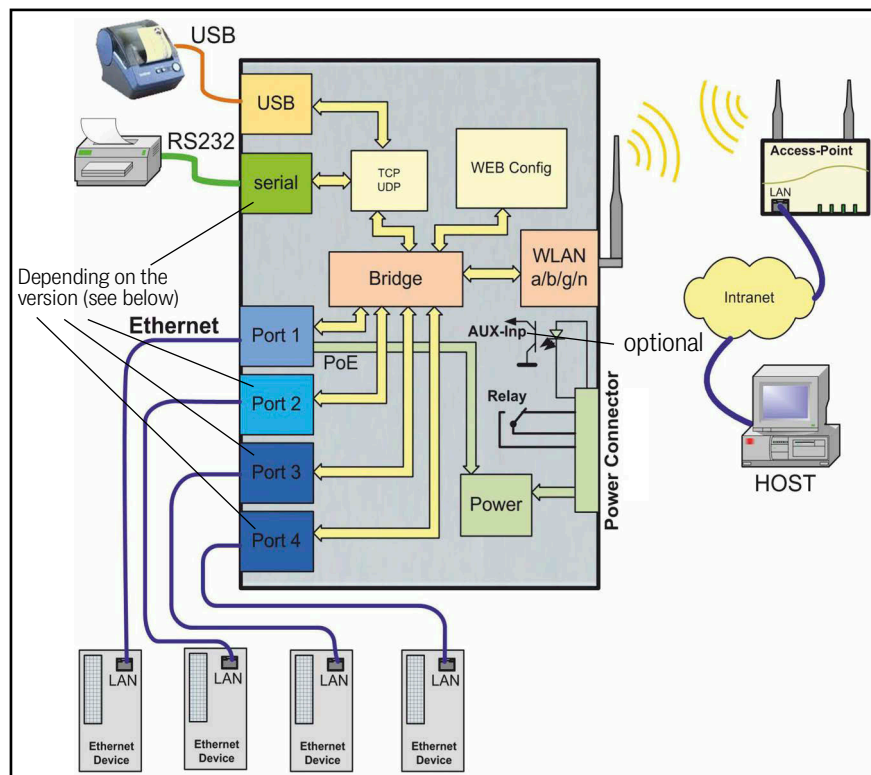
## 2

## Introduction

The Client Adapter HG G-76343/4/5 is a wireless LAN adapter (in Götting documents the terms radio modem respectively WLAN client are used synonymously) that connects devices via Ethernet, USB or serial port to wireless networks conforming to the 802.11 a/b/g/n standard. The HG G-76343/4/5 connects all devices that are connected to its LAN interface to a network reachable via WLAN.

Via a serial interface the HG G-76343/4/5 can receive and transmit data that is sent or received by a communication partner connected to the network (WLAN or LAN). This communication partner can also be a HG G-76343/4/5 or a computer that sends resp. receives via a matching application. The USB port makes it possible to connect extensions like e.g. additional serial interfaces or I/O interfaces.

**Figure 1** Complete system (example)



## 2.1 Versions / Variants

The device is available in different versions that offer different interfaces and mounting possibilities:

**Table 2** *Variants of the radio modem*

Variant / Order Number		Mounting (see section 3.1 on page 15)	Interfaces				
			Serial	ETH 1	ETH 2	ETH 3	ETH 4
HG G-76343	XA	Top hat rail narrow side Top hat rail long side Flange casing	✓	✓	–	–	–
	YA						
	ZA						
HG G-76344 (Variant w. LTE, 5G, see below)	XA	Top hat rail narrow side Top hat rail long side Flange casing	✓	✓	✓	–	–
	YA						
	ZA						
HG G-76345	XA	Top hat rail narrow side Top hat rail long side Flange casing	–	✓	✓	✓	✓
	YA						
	ZA						



There is also a variant **ac** with **802.11 ac**. That version is described in chapter 14 on page 106.



There is also a variant of the HG G-76344-A with **LTE** (4G), **Private LTE** or **5G**. That version is described in chapter 15 on page 108.

All variants operate with the same firmware and can be configured with the same program. You can download them from the following address:



<http://www.goetting-agv.com/components/76343>

## 2.2 Interfaces

The following interfaces are available (depending on the variant):

- 1 - 4 x Ethernet interfaces 10/100/1000 MBit/s + Auto-MDIX (auto crossover function), port 1 has PoE (Power over Ethernet).
- 1 x serial interface with 6 control wires.
- 1 x USB 2.0 interface e.g. for label printers or for the logging of system status messages on USB memory sticks.
- 1 x relay switching contact.
- Only on request: Input with optocoupler.

The Ethernet connection is connected via an RJ45 connector. LAN port 1 has a PoE function (IEEE 802.3af) so that the HG G-76343/4/5 can be powered by this port.

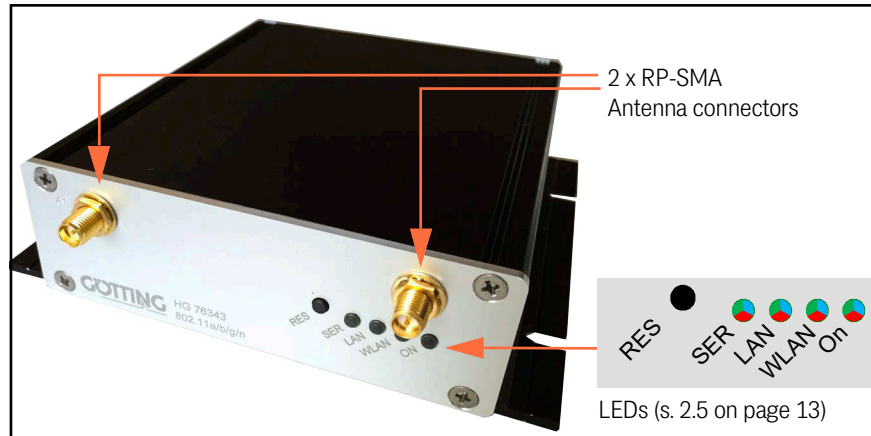
The serial port is connected by a 9 pin D-SUB plug. The assignment is selected in a way that a 1:1 serial cable can be used for the connection to a serial COM-Port of a PC. The exact assignment can be seen in Table 3 on page 13.

The power supply for the HG G-76343/4/5 needs a voltage source of 10 to 60 V. The usual power consumption is around 3 to 4 Watt (WLAN + LAN-Port active).

## 2.3 Indicators and Connectors

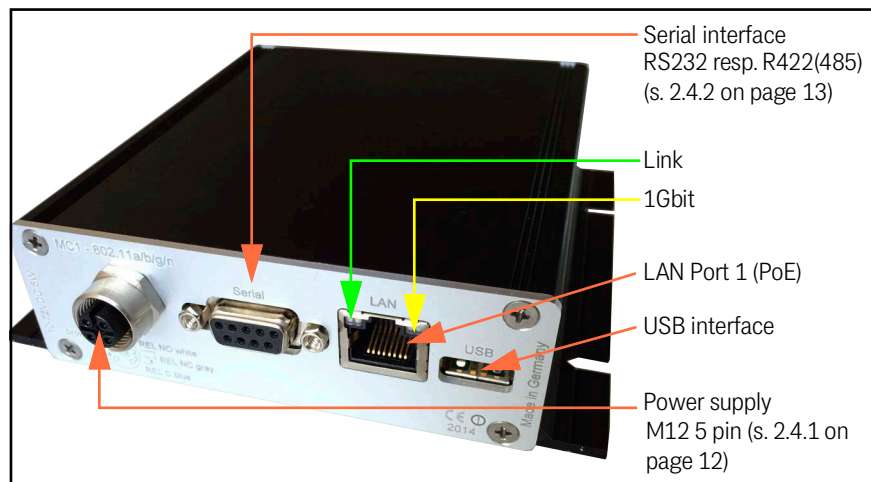
### 2.3.1 All Variants

**Figure 2** All variants: Connectors and indicators on the front panel



### 2.3.2 Connectors HG G-76343-A

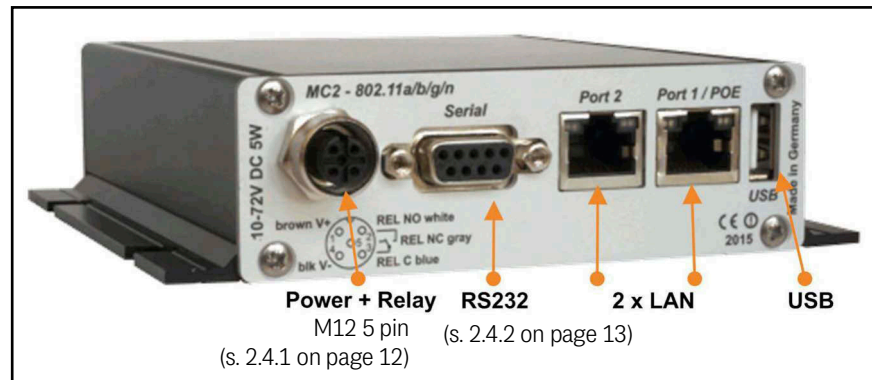
**Figure 3** Connectors HG G-76343ZA



The photo shows the HG G-76343-A with default configuration with 1 serial interface and a 5 pin connector for the power supply and the relay switching contact.

### 2.3.3 Connectors HG G-76344-A

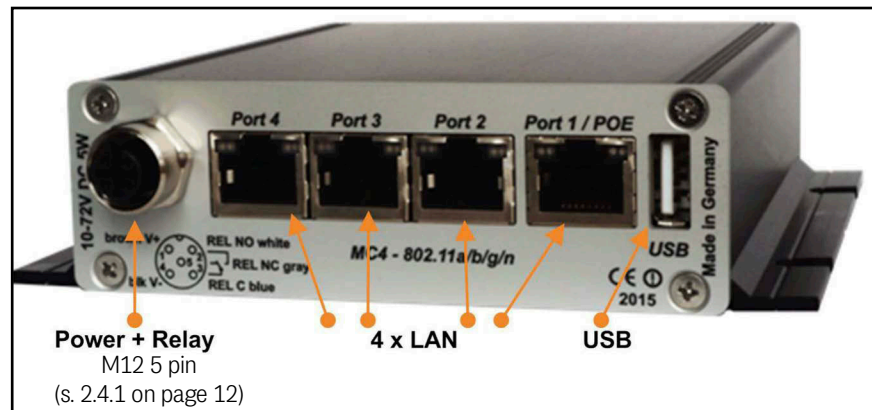
**Figure 4** Connectors HG G-76344ZA



The photo shows the HG G-76344-A with default configuration with 1 serial interface and a 5 pin connector for the power supply and the relay switching contact.

### 2.3.4 Connectors HG G-76345-A

**Figure 5** Connectors HG G-76345ZA

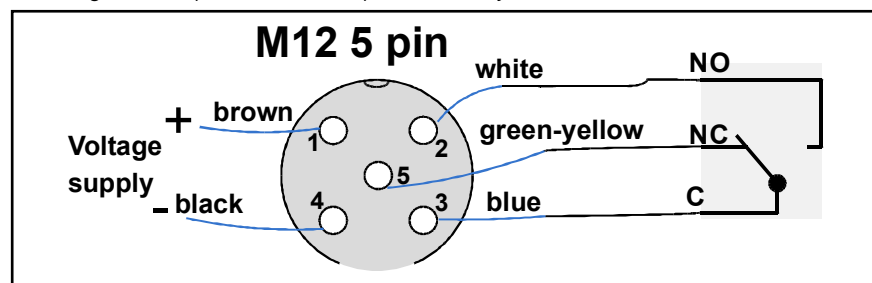


The photo shows the HG G-76345-A with default configuration with a 5 pin connector for the power supply and the relay switching contact.

## 2.4 Pin Assignments

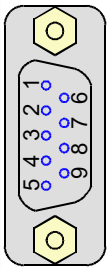
### 2.4.1 5 pin M12 Socket Power & Relay

**Figure 6** Pin assignment 5 pin. M12 socket power & relay



## 2.4.2 9 pin Sub-D Socket Serial

**Table 3** Pin assignment 9 pin Sub-D socket

	Pin	RS 232		RS 422(485)	
		Function	Direction	Function	Direction
	1	DCD	IN	NC	
	2	TxD	OUT	Tx+	OUT
	3	RxD	IN	Rx-	IN
	4	DSR	IN	NC	
	5	GND		GND	
	6	DTR	OUT	NC	
	7	CTS	IN	Rx+	IN
	8	RTS	OUT	Tx-	OUT
	9	RI	IN	NC	

## 2.5 LEDs

**Figure 7** LEDs

The 4 LEDs on the front represent the operating state of the radio modem. 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 flash white when the device is turned on or after a reset. If the LEDs WLAN + LAN + SER blink blue either a new firmware is currently in the flashing process or a new configuration is activated.

**Table 4** Functions of the LEDs (part 1 of 2)

LED	Function
On	<ul style="list-style-type: none"> <li>– <i>off</i>: No or not enough power</li> <li>– <i>green</i>: Sufficient voltage connected</li> <li>– <i>green + orange blinking</i>: <b>Standard mode</b>, radio modem ready</li> <li>– <i>light blue flickering</i>: The radio modem has been operated with a USB stick (s. chapter 11 on page 96) and waits for the stick to be re-inserted.</li> </ul>
WLAN	<ul style="list-style-type: none"> <li>– <i>off</i>: WLAN option off</li> <li>– <i>red blinking</i>: Radio modem is looking for suitable APs or is currently authenticating.</li> <li>– <i>green</i>: WLAN connection working OK.</li> <li>– <i>short red blinking</i>: Shows activity on the interface (sending or receiving of data).</li> </ul>
LAN	<ul style="list-style-type: none"> <li>– <i>off</i>: No device connected to the LAN-Port</li> <li>– <i>green</i>: Device connected to a LAN-Port and switched on.</li> <li>– <i>short orange blinking</i>: Shows activity on the interface (sending or receiving of data).</li> </ul>

Table 4 Functions of the LEDs (part 2 of 2)

LED	Function
SER (Serial) TCP Mode	<ul style="list-style-type: none"> <li>– <i>off</i>: The interface is inactive</li> <li>– <i>green</i>: A partner-device is connected to the interface.</li> <li>– <i>short orange blinking</i>: Shows activity on the interface (sending or receiving of data).</li> <li>– <i>green blinking</i>: The interface is active in the TCP-Server Mode and awaits a connection.</li> <li>– <i>red blinking</i>: The interface is active in the TCP-Client Mode and waits for a connection to the server to be established.</li> </ul>
SER (Serial) UDP Mode	<ul style="list-style-type: none"> <li>– <i>off</i>: The interface is inactive</li> <li>– <i>green</i>: The interface is initialized and ready to receive or transmit data.</li> <li>– <i>green + white blinking</i>: White blinking shows activity (sending or receiving of data). If data is exchanged continuously, the LED light is permanently white.</li> </ul>
RES (Reset)	No LED but a button, see section 3.5 on page 17.

## 3

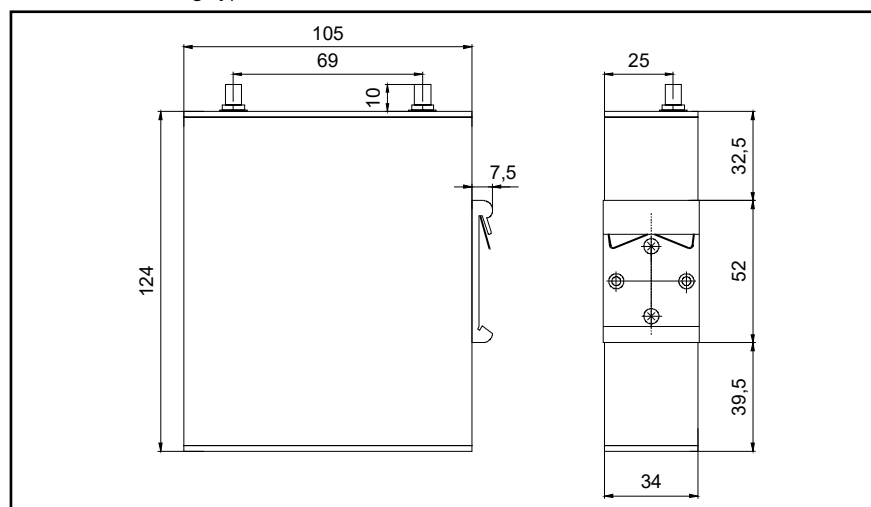
# Commissioning

## 3.1 Mounting

The device is available in three different casing variants: Two versions for top hat rail mounting (narrow and broad side) and one version with a flange casing. Below you can find casing pictures showing the dimensions of the different variants.

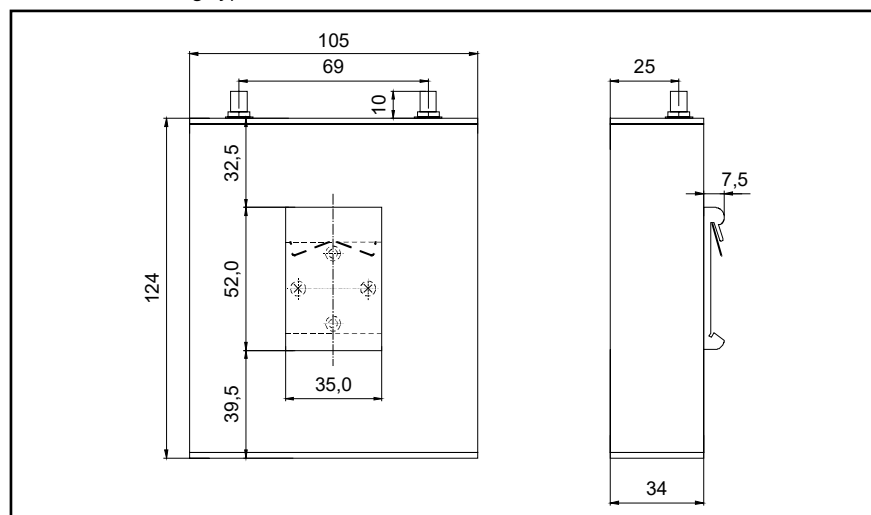
### 3.1.1 Casing Type XA with Top Hat Rail Mounting on narrow Side (all Variants)

**Figure 8** Dimensions casing type XA



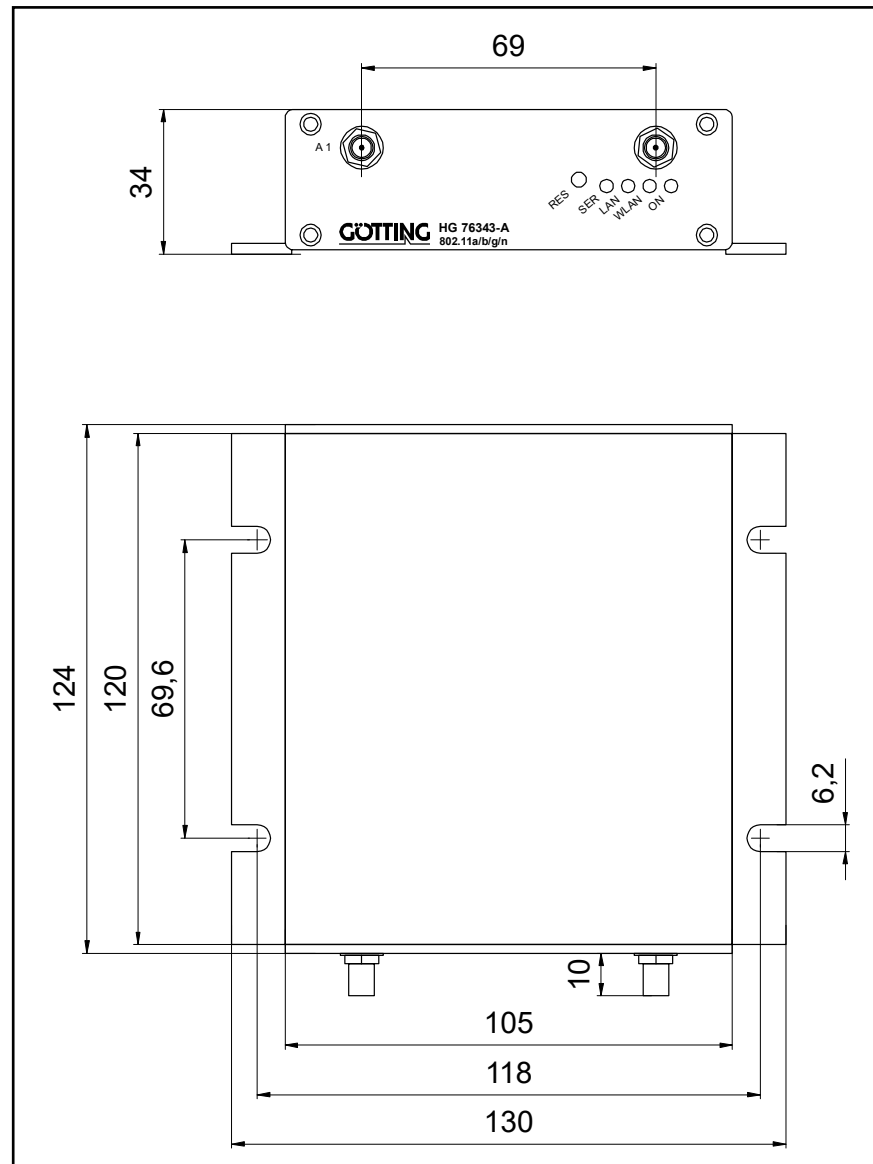
### 3.1.2 Casing Type YA with Top Hat Rail Mounting on broad Side

**Figure 9** Dimensions casing type YA



### 3.1.3 Casing Type ZA with Flange Casing

**Figure 10** Dimensions casing type ZA



## 3.2 Initial Startup via LAN

For the initial startup please connect the HG G-76343/4/5 via the Ethernet-Port with a PC using a patch cable. 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. This indicates the boot process. After about 15 seconds the application is ready and the LEDs indicate the modes described in section 2.5 on page 13.



### 3.3 The MC-Config Program

For its initial startup the radio modem is only able to communicate via its LAN-Port because typically there is no wireless network with a suitable SSID. The HG G-76343/4/5 is then connected to a PC via the Ethernet port.



The MC-Config application is described in chapter 4 on page 18 (including the further commissioning steps).

### 3.4 Commissioning via the Web Interface

If you do not want to or cannot use the MC-Config program, the HG G-76343/4/5 can also be commissioned using a WEB browser. For this purpose, the LAN interface of the commissioning computer must be set to a fixed IP address. Suitable would be e.g. the IP 192.168.170.1 with the subnet mask 255.255.255.0.

If the HG G-76343/4/5 starts with the default setting (see below), a connection to the radio modem can be established with the WEB browser by specifying the address 192.168.170.100 and the home web page of the radio modem can be displayed (see section 5.1 on page 38). From there the necessary settings can be made.

### 3.5 Reset to Factory Settings

By pressing the *Reset* button for a long time, the HG G-76343/4/5 can be set back to its factory settings. When keeping the reset button pressed, the radio modem 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 → red → green; re-starting with white. 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 HG G-76343/4/5 needs to be restarted by briefly pressing the *Reset* button again.

The HG G-76343/4/5 has the following (important) factory settings (device name according to variant):

```
Device Name: "HG76343"
SSID = "DefaultWLAN"
Encryption mode = no encryption
MODE= 802.11b/g/n
```

```
IP = 192.168.170.100
Netmask = "255.255.255.0"
Gateway = 192.168.170.1
```

```
user = "" (leer)
password = "" (leer)
```

```
SER1:   inaktiv
Relais: inaktiv
Input:  inaktiv
```

## 4

## MC-Config Program

### 4.1 Functional Description

The MC-Config Program can perform the following functions in a system with one or several radio modems HG G-76343/4/5:

- ♦ Locating the WLAN clients in the network (via LAN or WLAN)
- ♦ Configuring the WLAN client parameter including saving and loading of configurations via files
- ♦ Transfer of firmware files to WLAN clients
- ♦ Restart WLAN clients (reboot)
- ♦ Reset of WLAN client parameters to default settings (Factory Default)
- ♦ Display of current connection parameters of the WLAN clients in the network
- ♦ Retrieve system messages and log files from the WLAN clients



The MCCConfig program version 2.0.2.51 and higher expects that in the directory in which the MCCConfig\_xxx.exe file is saved, also the DLLs *libeay32.dll* and *ssleay32.dll* contained in the ZIP file are stored. If these are not present, an error is reported after starting the program.

### 4.2 IP Protocols and Ports Used

The MC-Config program uses the **UDP port 17784** to request status messages from the WLAN clients. Firmware upgrades are also transmitted via UDP if the WLAN client can only be reached via broadcast. If there is a unicast connection to a WLAN client, firmware files are transferred via the **TCP port 17784**. Log files and (W)LAN recordings are downloaded via **TCP port 17785**.

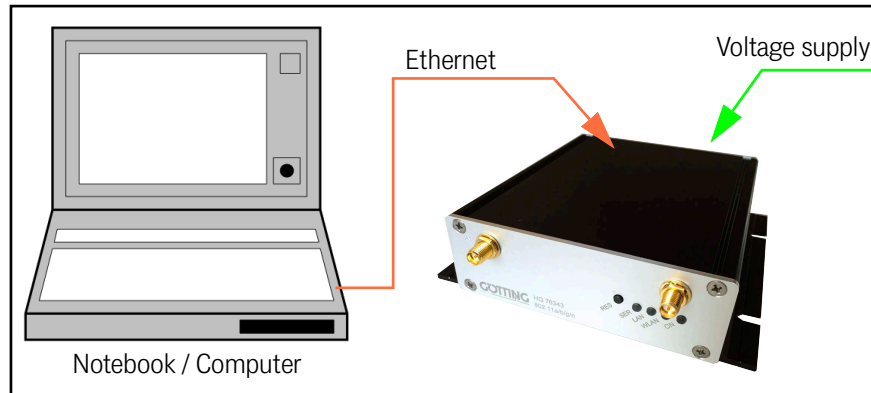
### 4.3 Encrypted Transmission

The MC-Config program encrypts the transfer of config files, the upload during firmware upgrade and the download of debug logs if the WLAN clients support this. This encryption is possible for radio modems with firmware 2.12k and higher.

## 4.4 Initial Startup

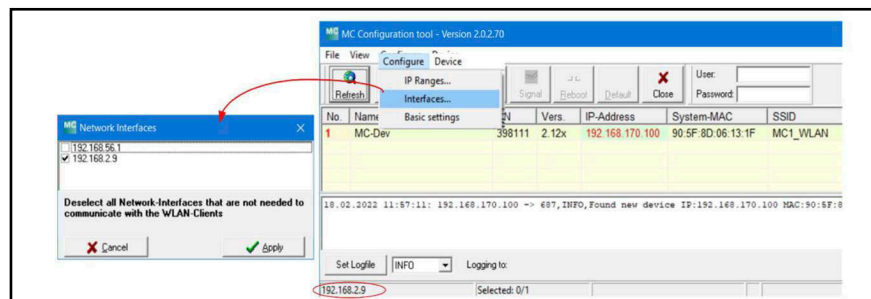
For the initial start-up WLAN clients can communicate only using the LAN connection, because usually there is no wireless network with a matching SSID.

**Figure 11** MC-Config Program: Setup for the initial operation of a WLAN client



The HG G-76343/4/5 is connected to a computer that has an Ethernet port. The MC-Config program is started on the computer.

**Figure 12** Initial commissioning with the MC-Config Program



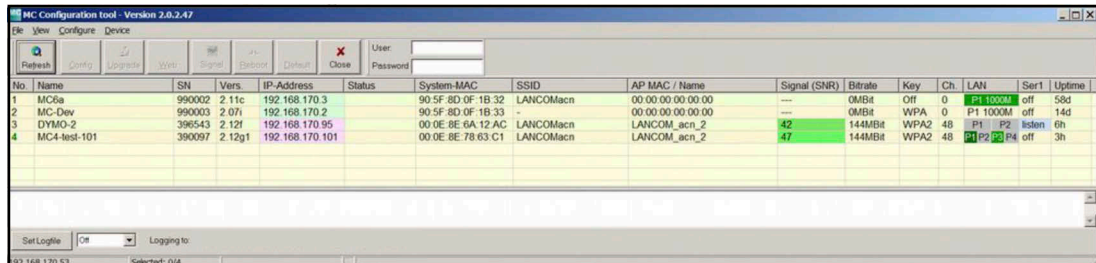
What to pay attention to:

- ✓ The connected computer (notebook) should have a **fixed** IP-address (no DHCP) on the LAN interface.
- ✓ This IP address should appear in the status field at the bottom left of the MC-Config program (see Figure 12 above). If this is not the case, you can check the setting of the LAN interface of the PC by entering the `ipconfig` command in the command line on the PC.
- ✓ If several IP addresses are listed there, you can activate only the relevant interface with *Configure Interfaces* (see Figure 12 above).
- ✓ After changing this configuration, press the Refresh button on the MC-Config program (see Figure 12 above).
- ▶ An active firewall on the computer could prevent the communication with the WLAN client.

## 4.5 Operation

After being started the MC-Config program first detects all network interfaces that are currently active on the computer. Via these interfaces queries are then sent out per Broadcast UDP/IP that will be answered by HG G-76343/4/5 devices. The responding devices are registered and displayed in a list.

Figure 13 MC-Config Program: User Interface



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 are also displayed.

Below the list there is a field for messages from the MC-Config program. Here also debug messages from WLAN clients are displayed, if this function has already been activated on the WLAN client. By double-clicking this field all messages saved so far are opened in a text editor.

### 4.5.1 Operating Elements

Figure 14 MC-Config Program: Operating elements

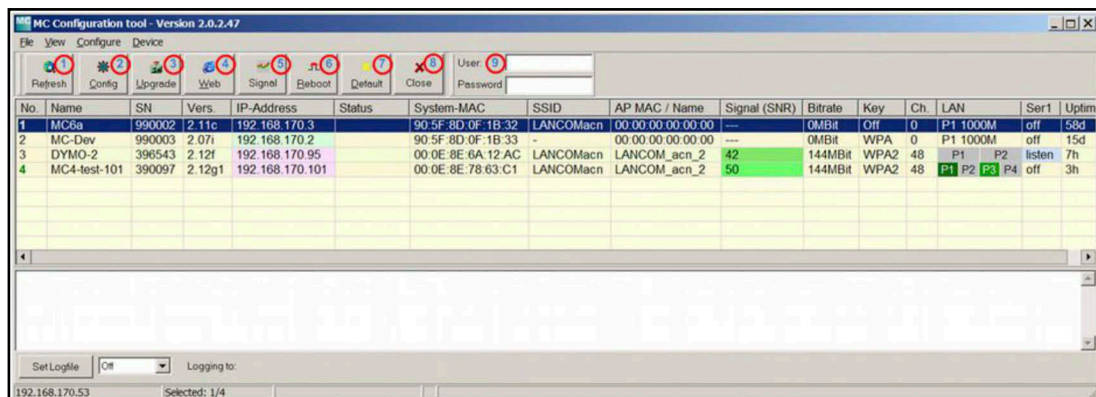


Table 5 MC-Config Program: Operating elements (part 1 of 2)

No	Name	Function
1	Refresh	The existing network interfaces are determined again. If you have changed the settings of the network adapters on the PC or plugged in new LAN cables, you should first update the currently available network interfaces with <i>Refresh</i> . In addition, the scan for existing WLAN clients is restarted. The scan ranges are set under Configure -> IP-Ranges, s. 4.6.3 on page 27.
2	Config	This opens the configuration dialogue for the selected radio modem. For this purpose, the configuration file is first retrieved from the WLAN client. When the configuration has been received completely, a window opens in which the configurable parameters of the WLAN client are displayed. Editing the configuration is described in section 4.7 on page 32.
3	Upgrade	Allows to transfer a firmware file to a WLAN client, see section 4.9 on page 34.

**Table 5** MC-Config Program: Operating elements (part 2 of 2)

No	Name	Function
4	Web	Opens the web-interface of the selected WLAN client in a browser window.
5	Signal	This function opens a window in which statistical data of the WLAN connection of all clients can be displayed.
6	Reboot	Restarts the selected WLAN client.
7	Default	Resets the configuration of the selected WLAN client to the factory default setting. Subsequently, a restart of the device is carried out.
8	Close	Closes the MC-Config program.
9	User/Pass-word	This information must be entered, if the configuration of a WLAN client is protected by the definition of User + Password. If this input is missing or wrong the following status message is shown: <b>Credentials Failed</b>

### 4.5.2 Information Shown by the List View Items

**Figure 15** MC-Config Program: List view items

No	Name	SN	Vers.	IP-Address	System-MAC	SSID	AP MAC / Name	Signal (SNR)	Bitrate	Key	Ch.	Status	LAN	USB	Ser1	Uptime	CPU
2	MC1-Test	307717	2.11p1	192.168.170.108	00:0E:8E:78:64:26	LANCOMacn	LANCOM_acn_2	47	65Mbit	WPA2	48		P1 1000M	off		13m	4%
1	MC2-Dyno	309867	2.11p1	192.168.170.95	00:0E:8E:6A:12:AC	LANCOMacn	LANCOM_acn_2	40	144Mbit	WPA2	48		P1	off		6d	2%
3	MC3-Dev	302222	2.11p1	192.168.170.105	00:0E:8E:6B:CA:C3	LANCOMacn	LANCOM_acn_2	41	65Mbit	WPA2	48		P1 P2	Isden		7m	6%

**Table 6** MC-Config Program: Information in the list view (part 1 of 3)

Column	Name	Function
1	No.	This number is assigned consecutively in the order of registration of the WLAN clients by the MC-Config program.
2	Name	Shows the device name as set in the configuration of the WLAN client.
3	SN	Serial number of the WLAN client
4	Vers.	Firmware version of the WLAN client

Table 6 MC-Config Program: Information in the list view (part 2 of 3)

Column	Name	Function																							
5	IP-Address	<p>IP adress of the WLAN client on the interface (LAN or WLAN) the client is connected by to the MC-Config program.</p> <div><table><tr><td>IP-Address</td><td></td></tr><tr><td>192.168.170.2</td><td></td></tr><tr><td>1) 192.168.170.171</td><td></td></tr><tr><td>3) 192.168.171.14</td><td></td></tr></table></div> <p>Depending on the set bridge mode there might be a different IP address for the LAN and WLAN port. Text color and background color of this field provide information about the type of connection between the MC-Config program and the WLAN client..</p> <p><b>Table 7</b> Color Coding Connection Type IP Address</p> <table><tr><th>Display</th><th></th><th>Function</th></tr><tr><td>green background</td><td></td><td>connection via LAN interface of the WLAN client</td></tr><tr><td>pink background</td><td></td><td>connection via WLAN interface of the WLAN client</td></tr><tr><td>black font</td><td>192.68.170.2 192.168.170.171</td><td>Unicast connection (direct IP connection, connection to website is possible)</td></tr><tr><td>pink font</td><td>192.168.171.14</td><td>Broadcast connection (connection to website is not possible)</td></tr></table> <p><b>Note:</b> A Unicast connection is necessary for the download of the debug and WLAN trace files (see section 10.3 on page 92)</p>	IP-Address		192.168.170.2		1) 192.168.170.171		3) 192.168.171.14		Display		Function	green background		connection via LAN interface of the WLAN client	pink background		connection via WLAN interface of the WLAN client	black font	192.68.170.2 192.168.170.171	Unicast connection (direct IP connection, connection to website is possible)	pink font	192.168.171.14	Broadcast connection (connection to website is not possible)
IP-Address																									
192.168.170.2																									
1) 192.168.170.171																									
3) 192.168.171.14																									
Display		Function																							
green background		connection via LAN interface of the WLAN client																							
pink background		connection via WLAN interface of the WLAN client																							
black font	192.68.170.2 192.168.170.171	Unicast connection (direct IP connection, connection to website is possible)																							
pink font	192.168.171.14	Broadcast connection (connection to website is not possible)																							
6	System-MAC	<p>MAC address of the WLAN client. The LAN interface sends out data using another Mac address than the WLAN interface. If the cursor is positioned over this column, additional information is displayed.</p> <div><p>MAC-Information: Bridge Mode: NAT used MAC on LAN side: 90:5F:8D:05:F3:D1 used MAC on WLAN side: 00:0E:8E:78:63:C1</p></div>																							
7	SSID	<p>Gives the WLAN name (Service Set Identifier, SSID), that the WLAN client wants to connect to. If no connection is established the SSID of the active WLAN profile with the highest priority is shown.</p>																							
8	AP-MAC/Name	<p>When the WLAN client is connected to a WLAN, the Mac address of the connected access point is displayed here. Some access points send out a device name that the WLAN client then shows here instead of the MAC address.</p>																							
9	Signal (SNR)	<p>Strength of the signal received by the access point (AP). The signal-to-noise ratio is given in dBm.</p> <ul style="list-style-type: none"><li>– Signal &gt;= 40 very good connection</li><li>– Signal &gt;= 30 good connection</li><li>– Signal &gt;= 20 sufficient connection, WLAN client starts to search for a better AP</li><li>– Signal &lt; 20 limited connection, the bit rate will be reduced during data transfer</li></ul>																							
10	Bitrate	<p>Bitrate for receiving data from AP. The data rate is given in MBit/s and is in the range of 1 to 300 MBit/s</p>																							
11	Key	<p>When the WLAN client is connected to an AP, here the encryption type used to establish the connection is given.</p>																							

**Table 6** MC-Config Program: Information in the list view (part 3 of 3)

Column	Name	Function
12	Ch.	Channel number for the connection of the WLAN client with the AP. The channel number is defined by the AP. <ul style="list-style-type: none"> <li>Channels 1 - 14 are in the 2.4 GHz band</li> <li>Channels 36 - 165 are in the 5 GHz band</li> </ul>
13	Status	Information on the transfer state of data between the MC-Config program and the WLAN client. This also includes the status of the logging function for recording the LAN and/or WLAN data traffic.
14	LAN	Status of the LAN port(s):
15	USB	If a USB memory stick is plugged in this shows its free capacity (in %). If the USB stick is a Config-Stick (s. chapter 11 on page 96) this is shown as well.
16	Ser1	State of the serial interface. As long as the mouse cursor is positioned above this column additional information is shown in an overlay.
17	Uptime	Run time of the radio modem since power up or last reset.
18	CPU	CPU workload of the radio modem in [%]

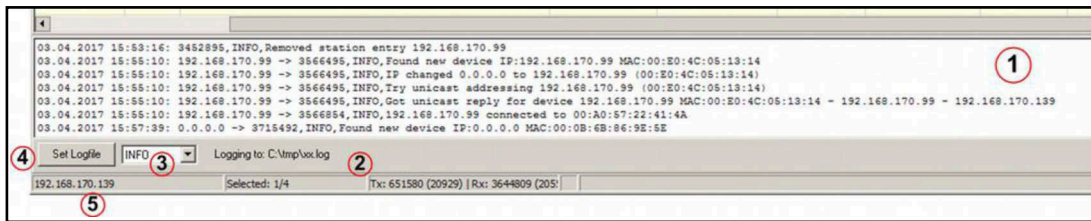
### 4.5.3 Arrangement of Columns

The user can design the position of the columns according to his own requirements. To do this, position the cursor on the column to be moved (in the data area, not at the header). By holding down the CTRL key + the left mouse button, you can move the column to the desired position.



#### 4.5.4 Settings for the Logging of Messages

**Figure 16** MC-Config Program: List view items



**Table 8** MC-Config Program: Logging settings

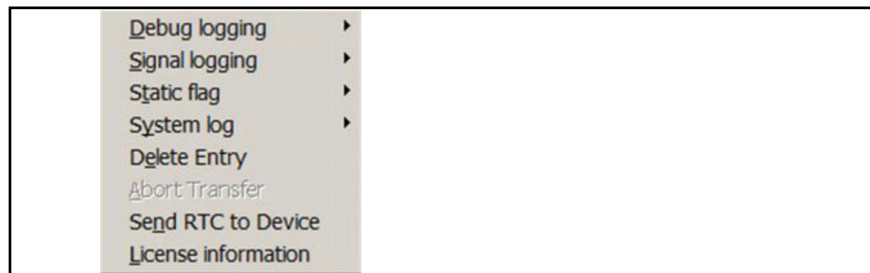
Area	Name	Function
1		This field displays the system messages of the MC-Config program. With the debug-logging-function being switched on at a WLAN client the display changes and shows the messages of the selected WLAN client.
2	Log-Datei	The messages of the MC-Config program are written to the file given here.
3	ERROR INFO DEBUG TRACE	Selection of how detailed the messages should be, that the MC-Config program will output. Here it is sufficient to set the setting to ERROR or INFO, unless you want to analyze an error situation more precisely.
4		This key opens a dialog used to define the log file.
5	IP Interface	Shows the IP address of the interface used for the communication with the radio modem. It is possible that more than one address is shown.



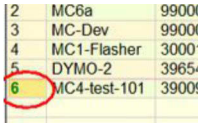
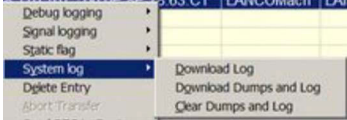
### 4.5.5 Context Menu of the List Items

By performing a right click on a list item the following context menu can be opened:

**Figure 17** MC-Config Program: List context menu items



**Table 9** MC-Config Program: List context menu items (part 1 of 2)

Menu item	Function	Values
Debug logging	De-/activation of the logging of system messages of the selected WLAN client (see section 4.12 on page 36). First, a target file is queried in which the debug messages are to be written.	on off
Signal logging	This function saves the WLAN data (signal strength, connected AP, channel, bit rate) received by the MC-Config program for the WLAN client in a file in the form of text lines.	on off
Static flag	<p>If you want to keep all existing devices in the table in an application, even if they are not currently available, you can set the entries to <i>static</i>. This means that the entries are not deleted from the table, even if the corresponding radio modems are not currently in operation.</p> <p>Entries in the state <i>static</i> are marked yellow in the 1st column:</p> 	
System log	<p>This allows operations to be performed on the log and dump files stored in the radio modem.</p>  <p>There are <i>Log</i> files that store text messages and <i>Dump</i> files that contain recordings from the WLAN or LAN interface of the WLAN client.</p> <ul style="list-style-type: none"> <li>– <i>Download Log</i> transfers the System Log file to the MC-Config program.</li> <li>– <i>Download Dumps and Log</i> leads to a dialog in which all log and dump files for download can be selected and downloaded.</li> <li>– <i>Clear Dumps and Log</i> deletes all relevant files.</li> </ul> <p><b>This deletion should always be carried out before a test, during which a certain function is to be tested and logged.</b></p>	

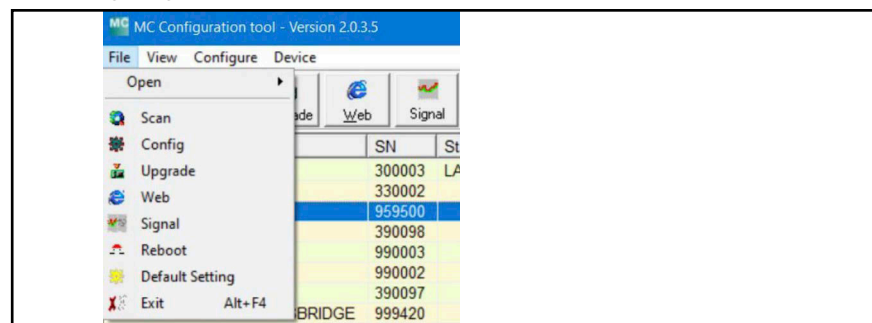
**Table 9** MC-Config Program: List context menu items (part 2 of 2)

Menu item	Function	Values
Delete Entry	This allows the selected entry to be deleted from the list. Deletion only takes place when all file transfers and DebugLog functions have been completed.	
Abort Transfer	With this function a running transfer (e.g. firmware upload) can be aborted.	
Set RTC to Device	This transfers the system time of the PC to the radio modem and applies it there. This allows you to set the radio modem system time to a real value without a time server, e.g. to be able to better identify the time data in log files.	
License Information	Here you will find information on <i>Open Source Compliance</i> for the radio modems.	

## 4.6 Menus

Using the main menu you can initiate actions mentioned above as well as carry out advanced settings for the MC-Config program.

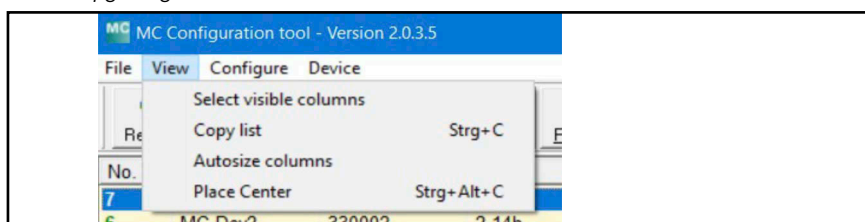
### 4.6.1 File

**Figure 18** MC-Config Program: File Menu

Duplicates the functions of keys above the list (see Table 5 on page 20).

### 4.6.2 View

**Figure 19** MC-Config Program: View Menu



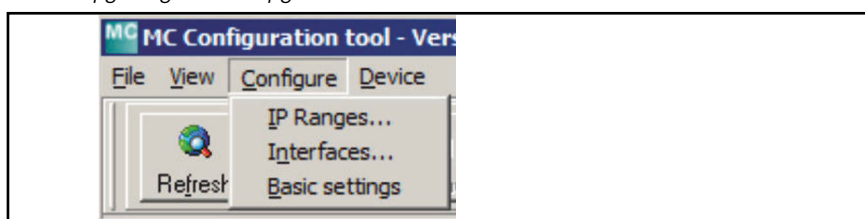
**Table 10** MC-Config Program: Functions of the view menu

Menu item	Function
Select Visible Column	With this function you can set which columns of the list view are visible and which are not.
Copy list	This function is used to copy the text part of the list view including the information of the WLAN clients to the clipboard. With e.g. a text editor this information can be further processed.
Autosize columns	This function sets the width of all visible columns automatically to a certain measure so that all information is visible. This action can also be triggered when you click on the list view and press the keys Ctrl+V.
Place Center	This repositions the main window of the MC-Config program.



### 4.6.3 Configure

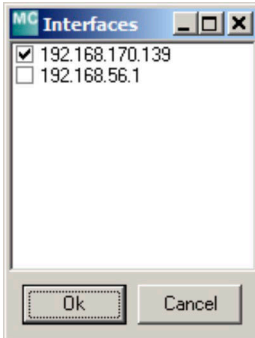

**Figure 20** MC-Config Program: Configure Menu



**Table 11** MC-Config Program: Functions of the configure menu (part 1 of 4)

Menu item	Function
IP ranges	In particular if the MC-Config program is to connect to the WLAN clients via WLAN and the WLAN system does not forward the broadcast UDP packets that the MConfig program sends to search for the WLAN clients, it is necessary to scan specific IP address ranges. This menu item is used to define the parameters for scanning, for further information see 4.11.1 on page 34

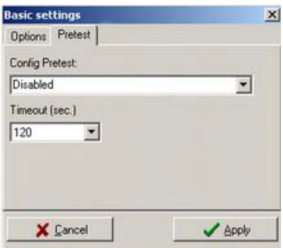
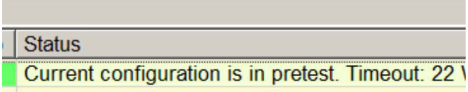
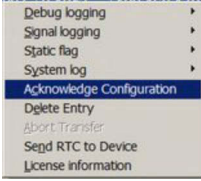
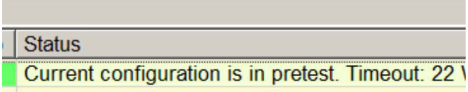
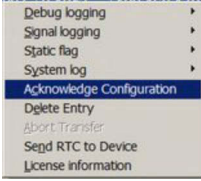
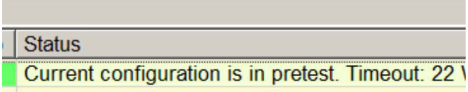
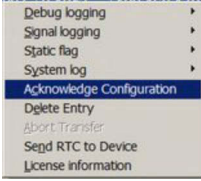
Table 11 MC-Config Program: Functions of the configure menu (part 2 of 4)

Menu item	Function												
Interfaces	<p>If the computer used to run the MC-Config program has several IP network interfaces, via this menu item one can - if necessary - select, which interfaces shall (can) be used for the connection to the WLAN clients. The user should use these settings to selectively activate only the interface that is necessary for communication with the radio modem, so that an unnecessarily large number of broadcast requests are not distributed over the various interfaces.</p> 												
Basic Settings	<p>In this menu item you find settings that influence the functionality of the MC-Config program.</p> 												
Basic Settings	<p><b>Enable Key shortcuts</b></p> <p>This allows to enable Key Shortcuts for the list view. If this option is activated, the list view reacts to the following shortcuts:</p> <p style="text-align: center;"><b>Table 12 MC-Config Program: Key shortcuts</b></p> <table> <tr> <th>Key</th><th>Function</th></tr> <tr> <td>'s'</td><td>Set selected item to <i>static</i></td></tr> <tr> <td>'S'</td><td>Reset <i>static</i> state</td></tr> <tr> <td>ESC</td><td>Cancel data transfer in process</td></tr> <tr> <td>'c'</td><td>Call <i>Config</i> function</td></tr> <tr> <td>'u'</td><td>Call <i>Upgrade</i> function</td></tr> </table>	Key	Function	's'	Set selected item to <i>static</i>	'S'	Reset <i>static</i> state	ESC	Cancel data transfer in process	'c'	Call <i>Config</i> function	'u'	Call <i>Upgrade</i> function
Key	Function												
's'	Set selected item to <i>static</i>												
'S'	Reset <i>static</i> state												
ESC	Cancel data transfer in process												
'c'	Call <i>Config</i> function												
'u'	Call <i>Upgrade</i> function												
Basic Settings	<p><b>Autosend UTC to devices</b></p> <p>With Autosend UTC to devices the MC-Config program can be set so that the current time of the PC is continuously transmitted to the WLAN clients. This makes sense if no time server is available in the network.</p>												

**Table 11** MC-Config Program: Functions of the configure menu (part 3 of 4)

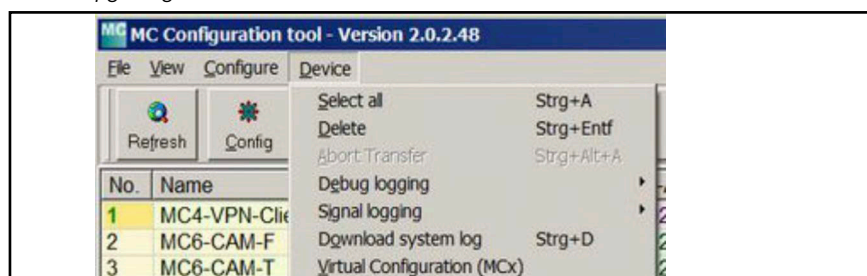
Menu item	Function															
Basic Settings	<b>Device Polling</b> This parameter sets how often the current status of the devices in the list is updated. It also sets how often a <i>Discover</i> is sent to find new devices in the system.  <b>Table 13</b> <i>MC-Config Program: Device Polling</i> <table><tr><th>Option</th><th>Status Request</th><th>Discover</th></tr><tr><td>fast</td><td>5x per second</td><td>1x per 3 seconds</td></tr><tr><td><b>default</b></td><td><b>1x per second</b></td><td><b>1x per 5 seconds</b></td></tr><tr><td>slower</td><td>1x per 3 seconds</td><td>1x per 10 seconds</td></tr><tr><td>extremely slow</td><td>1x per 6 seconds</td><td>1x per 20 seconds</td></tr></table> The setting should be set depending on how many devices are listed in the table, how much (WLAN) data traffic is to be generated by the MC-Config program and how promptly status changes in the devices are to be detected.	Option	Status Request	Discover	fast	5x per second	1x per 3 seconds	<b>default</b>	<b>1x per second</b>	<b>1x per 5 seconds</b>	slower	1x per 3 seconds	1x per 10 seconds	extremely slow	1x per 6 seconds	1x per 20 seconds
	Option	Status Request	Discover													
	fast	5x per second	1x per 3 seconds													
	<b>default</b>	<b>1x per second</b>	<b>1x per 5 seconds</b>													
	slower	1x per 3 seconds	1x per 10 seconds													
extremely slow	1x per 6 seconds	1x per 20 seconds														

Table 11 MC-Config Program: Functions of the configure menu (part 4 of 4)

Menu item	Function								
Basic Settings	<p><b>Pretest</b></p> <p>If this option is activated, a new Config, which has been transferred to a radio modem, is initially accepted and executed <i>for test</i>. If this Config is not confirmed within the time defined by the <i>Timeout</i> parameter, the radio modem activates the previous Config again and restarts it. This prevents a wrong setting in the Config from causing the connection to a radio modem not to be re-established after this Config has been saved. The following settings are possible:</p> <div style="text-align: right;">  </div> <p style="text-align: center;"><b>Table 14 MC-Config Program: Pretest</b></p> <table> <tr> <th>Option</th><th>Function</th></tr> <tr> <td>Disabled</td><td>Pretest not active</td></tr> <tr> <td>Enabled - Need user acknowledge</td><td> <p>The new Config must be confirmed by the user. After the device has been registered with the MC-Config with the new config, the following message appears in the status column: <i>Current configuration is in pretest. Timeout: xx</i></p> <div style="text-align: right;">  </div> <p>The user must confirm the new config before the timeout expires, otherwise the previous config will be reactivated and the device will restart.</p> <p>To confirm, activate the context menu for this device. The new Config is permanently activated via the menu selection <i>Acknowledge Configuration</i>.</p> <div style="text-align: right;">  </div> </td></tr> <tr> <td>Enabled - Auto acknowledge on contact</td><td>The new Config is automatically confirmed when the device is registered again in the list by the MC-Config program after downloading the new Config.</td></tr> </table>	Option	Function	Disabled	Pretest not active	Enabled - Need user acknowledge	<p>The new Config must be confirmed by the user. After the device has been registered with the MC-Config with the new config, the following message appears in the status column: <i>Current configuration is in pretest. Timeout: xx</i></p> <div style="text-align: right;">  </div> <p>The user must confirm the new config before the timeout expires, otherwise the previous config will be reactivated and the device will restart.</p> <p>To confirm, activate the context menu for this device. The new Config is permanently activated via the menu selection <i>Acknowledge Configuration</i>.</p> <div style="text-align: right;">  </div>	Enabled - Auto acknowledge on contact	The new Config is automatically confirmed when the device is registered again in the list by the MC-Config program after downloading the new Config.
Option	Function								
Disabled	Pretest not active								
Enabled - Need user acknowledge	<p>The new Config must be confirmed by the user. After the device has been registered with the MC-Config with the new config, the following message appears in the status column: <i>Current configuration is in pretest. Timeout: xx</i></p> <div style="text-align: right;">  </div> <p>The user must confirm the new config before the timeout expires, otherwise the previous config will be reactivated and the device will restart.</p> <p>To confirm, activate the context menu for this device. The new Config is permanently activated via the menu selection <i>Acknowledge Configuration</i>.</p> <div style="text-align: right;">  </div>								
Enabled - Auto acknowledge on contact	The new Config is automatically confirmed when the device is registered again in the list by the MC-Config program after downloading the new Config.								

#### 4.6.4 Device

**Figure 21** MC-Config Program: Device Menu



**Table 15** MC-Config Program: Functions of the Device menu

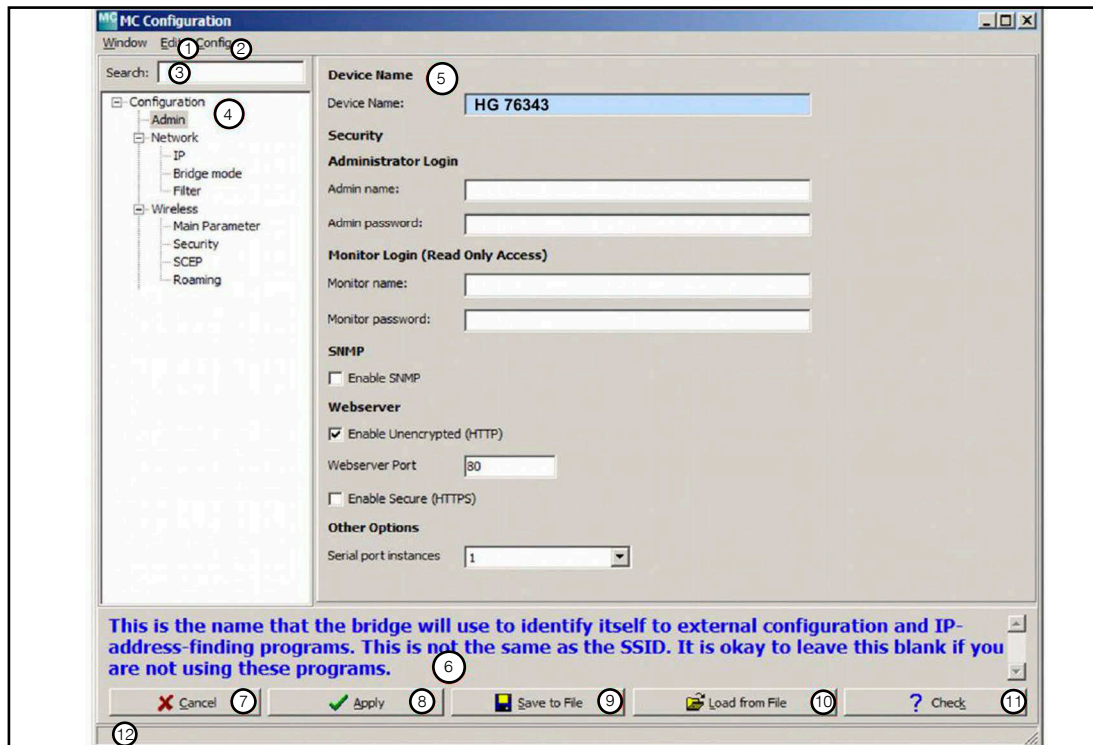
Menu item	Function	Key shortcut
Select all	Select all list items.	Ctrl + A
Delete	Delete selected list items from the table.	Ctrl + Entf
Abort transfer	Abort all currently running data transfers.	Ctrl + Alt + A
Debug logging	Activate or deactivate the logging of debug messages for all selected WLAN clients.	
Signal logging	Activate or deactivate the logging of WLAN connection data for all selected WLAN clients.	
Download system log	Download and save the debug messages of the selected WLAN clients.	Ctrl + D
Virtual Configuration (MCx)	With this function you can view, edit and save an existing Config file without having to use a radio modem.	

## 4.7 The Config Function

By pressing the Config key all data, that define the setting of the selected WLAN client will be transferred to the MC-Config program. All parameters are set dynamically for the config program, and they are solely defined by the firmware of the WLAN client.

When a complete configuration set from the WLAN client is received, the following window opens:

Figure 22 MC-Config Program: Config dialog



The dialog has the following areas:

- ♦ (1 + 2) Main menu
- ♦ (3 + 4) Config structure with search function
- ♦ (5) Parameter definition
- ♦ (6) Field for notes and help regarding the individual parameters
- ♦ (7 – 11) Keys to save, load and apply the configuration data
- ♦ (12) Status messages

In order to show or edit certain parameters the user shall at first select from the config structure the segment where the parameter is defined. By using the search function (3) a parameter can be located in the config structure. Config structure items with a search match are highlighted in blue.

Possible settings for the selected segment are displayed in the parameter field (5). The user can apply changes. Changed parameters are shown in bold. Additionally the changed config structure item gets red. Thus the user can keep an overview about where alterations are done. Using the key combination Ctrl + R you can undo changes. After pressing the key combination Ctrl + D all values are being reset to the delivery state (Factory Default).



After all alterations are done, the configuration is sent back to the WLAN client by pressing the *Apply* button (8). The client will accept the parameters and carry out a reboot depending on the changed parameters. The config dialog is then closed.

The keys of the config dialog have the following functions:

**Table 16** MC-Config Program: Buttons of the Config dialog

Number	Button	Function
7	Break	Closes the Config dialog without transferring the changes to the WLAN client.
8	Apply	Starts the transfer of the parameter set to the WLAN client. The Config dialog is closed.
9	Save to file	Saves the current parameter set in a file.
10	Load from file	Loads a parameter set from a file.
11	Check	Transfer of the parameter set to the WLAN client for verification. The result of the verification is shown in the status bar at the bottom (12).

#### 4.7.1 Variable number of input fields

There are a number of parameters that have multiple instances. For example, under Network → Bridge Mode → NAT there are forwarding rules (NAT Rules). The number of configurable rules can be set by right-clicking on one of the input fields to open a context menu and selecting *Change option count*.

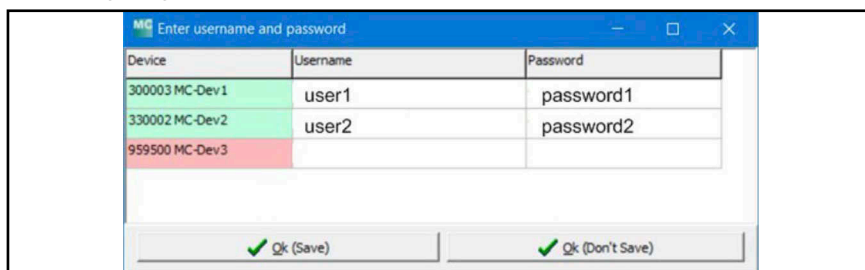
## 4.8 Access Protection with Username and Password

Access to the configuration of a radio modem can be protected by entering Username + Password in the *Config* under *Admin*. If the same values for User + Password are valid for all WLAN clients, one has to only enter these values in the main window once and can then access all devices.

You can also pass the values for user + password when starting the MC-Config programme. With the arguments `MCConfig_2_0_3_5.exe user=.... password=.....` these values are transferred to the two input fields at the start.

However, if the WLAN clients require different user + password details, you can also leave the user + password input fields empty. When accessing protected functions from one or more WLAN clients, a dialog opens in which the information for user name + password can be entered.

**Figure 23** MC-Config Program: Enter username and password



Already during the input, the program checks the correctness of the data and shows the *device* field in green if the username + password input is correct.

These entries can be saved permanently in a file (Save) or temporarily in the memory (don't Save). With don't Save, the entries are deleted when the MC-Config program is closed. With Save, a file <SN>.cred is created in the Credentials directory for each device, which contains the encrypted Username + Password entry.

## 4.9 Firmware-Updates

After pressing the Upgrade button the user is led to a dialog, where a firmware file can be selected. Firmware files for WLAN clients are of the type *bin*. The selected file is subsequently transferred to the WLAN client and stored in its flash memory. The existing configuration of the WLAN client is being taken over and applied to the new firmware.

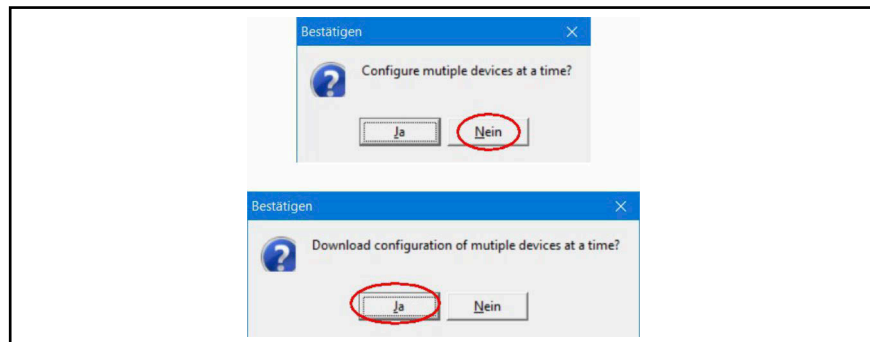
By selecting several units, you can also distribute the firmware to these units simultaneously in one process.

## 4.10 Downloading the Config from Multiple Devices

To download and save the configuration files from several units simultaneously, proceed as follows:

- ▶ In the main window, select the units from which you want to download the Config. This is done by clicking on the device entry while holding down the <Ctrl> key.
- ▶ With several units selected click on the *Config* button. The following dialogs appear, which you answer by clicking on the highlighted button as shown.

**Figure 24** MC-Config Program: Dialogs while downloading the Config from multiple devices



- ▶ Then define the directory in which the Config files are stored.

The Config files stored in the directory have the following file name format:  
Cfg\_<ip-addr>\_<MAC-addr>\_<SN>\_<Device Name>.cfg

## 4.11 Search WLAN Clients

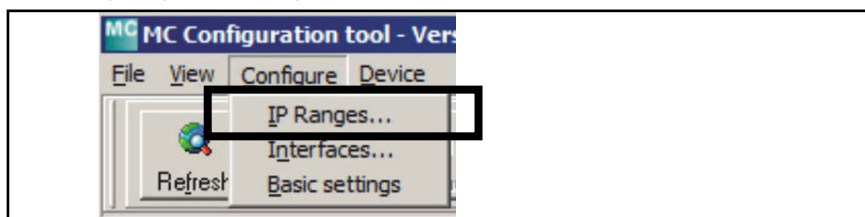
### 4.11.1 IP Ranges

The following conditions might be the reason that the MC-Config program cannot establish a connection to WLAN clients:

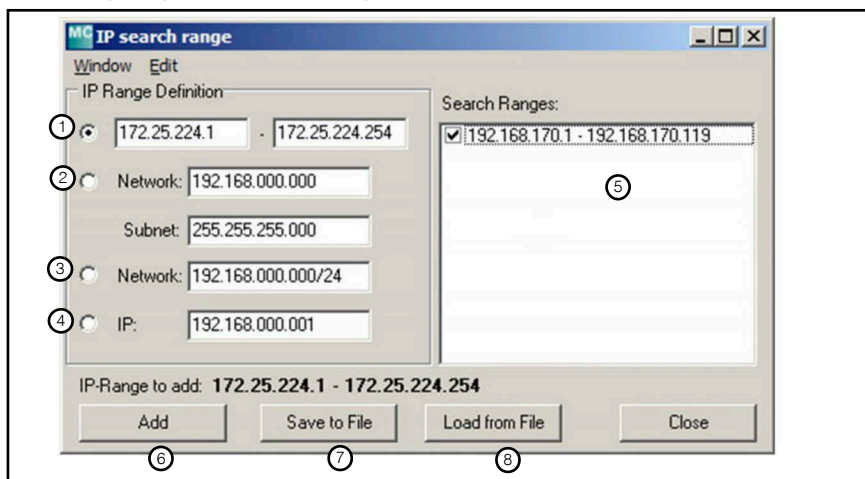
- ♦ The WLAN clients are in a different network.
- ♦ The WLAN clients are connected via a WLAN infrastructure that does not forward the broadcast queries of the MC-Config program.

In order to reach these WLAN clients you can define IP ranges that are scanned with the start of the MC-Config program or after pressing the Refresh button. The dialog for defining the IP ranges can be opened here:

**Figure 25** MC-Config Program: IP Ranges



**Figure 26** MC-Config Program: IP search range



1 - 4 allow to choose different methods for defining a scan range:

1. Freely definable IP range with start and end IP
2. Definition of an IP range with network address and subnet mask
3. Definition of an IP range with network address and bit mask
4. Single IP address entry

Clicking *Add* (6) the selected and edited information will be added to the range (5). With *Save to File* (7) the information can be saved to a file and with *Load from File* (8) loaded from a file. With the delete key a selected IP range item in (5) can be removed. After leaving the dialog with *Close* the defined and activated ranges are scanned.

## 4.12 Logging System Messages

The WLAN clients allow to store events and error situations that occur during operation. What and how this is logged can be set in the configuration of the WLAN clients. In order to be able correlate logged events with the time when they occurred it is advantageous if a time server (NTP server) is configured inside the WLAN client (see section 5.3.7 on page 55).



Logging is described in detail in chapter 10 on page 87. The following only describes the corresponding settings in the MC-Config program.



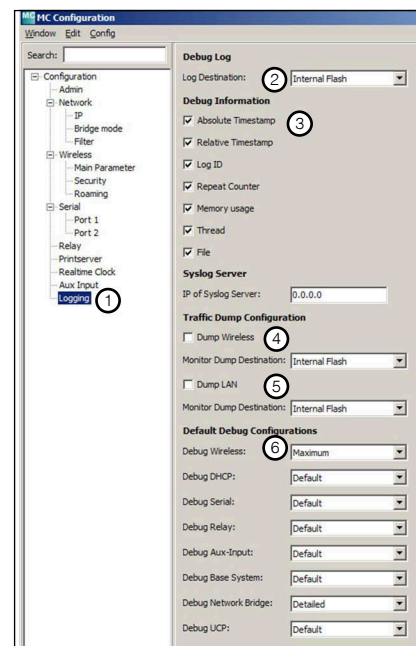
These options for logging system messages or data traffic recordings are only intended to investigate any problems that occur and, if necessary, to show how these problems can be resolved. In normal operation, all settings described here should be reset to the default values.

### 4.12.1 Configuration of the Logging Parameters

Depending on the problem to be investigated you can change the *intensity* of the debug messages for specific parts of the radio modem firmware via Configuration → Logging. Additionally it is possible to make protocol logs for the WLAN and LAN interfaces. The functions of the dialog are described in detail in chapter 10 on page 87.

**Figure 27** MC-Config Program: Configuration of the logging details

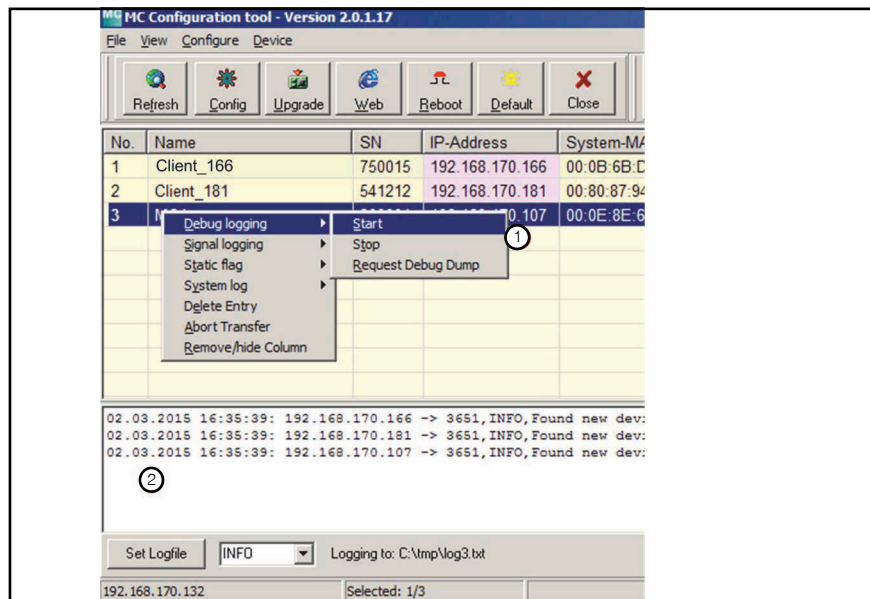
1. Open the Logging parameters
2. Configuration of where to store the logs.
3. Configuration of the information that is put into each line of a debug message.
4. With *Dump Wireless* the WLAN board is put into a special mode that allows to save all sent and received data packets into a file.
5. The same function as (4) but for the LAN interface.
6. Here the intensity of the debug messages is set for the different software modules.



### 4.12.2 Recording Debug Messages

The context menu of MC-Config's list view allows to transfer the debug logs from a WLAN client to the MC-Config program.

**Figure 28** MC-Config Program: Recording debug messages



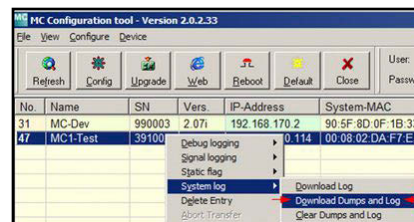
In order to start the logging, right-click the respective entry in the device list and activate *Debug logging* → *Start* (1). A dialog opens that allows to define the log file, then all messages are written to that file and displayed in area (2). By repeating this for other devices it is possible to log debug messages for several WLAN clients at once.

A double click on area (2) opens the logged messages in the default Windows® text editor.

### 4.12.3 Download of Debug Messages and (W)LAN Logs

**Figure 29** MC-Config Program: Download dumps and log

The debug messages and logs stored on a radio modem can be downloaded via the context menu, *System log* → *Download*. Further information on this can be found in section 10.3 on page 92.



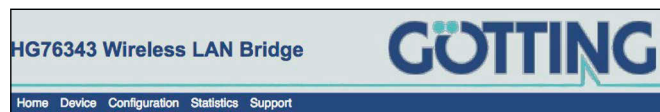
## 5

## Parameter Setting via the Web Interface

Use a web browser to establish a connection with the web server of the HG G-76343/4/5. Then a page with information is shown, displaying the current status of the WLAN client. This site can be accessed without entering the optional *User* and *Password* combination that might be set. If set, user and password will be requested once when opening any of the other available sites.

### 5.1 Information Site / Home

The first site that is visible contains general information regarding the current state of the device and about its firmware. It has the following sections.



#### 5.1.1 System Information

This section contains general information about the device:

**Figure 30** Web interface: System information

System Information	
Device Name	HG76343
Uptime	0 Week(s) 0 Day(s) 00:01:23
Realtime clock (UTC)	17.10.2023 7:02:10
Realtime clock (Local Time)	17.10.2023 8:02:10
Serial number	326550
Firmware Version	2.14p
Kernel Version	Linux version 5.4.256

**Table 17** Web interface: System Information (part 1 of 2)

Entry	Note
Device Name	This information can be edited under → Admin (section 5.2 on page 46) and is being displayed in the MC-Config program as the device's name.
Uptime	Shows the time since the HG G-76343/4/5 was switched on or resetted the last time.
Realtime clock (UTC)	This shows the internal device time. The HG G-76343/4/5 by default sets the internal time to 2000.01.01 00:00:00 when started. If a time server is configured (see section 5.3 on page 49), the HG G-76343/4/5 tries to reach it to receive the current UTC time. If this is successful, the WLAN client changes the internal time accordingly. The internal time is used as a timestamp for debug outputs and for the validation of certificates.

**Table 17** Web interface: System Information (part 2 of 2)

Entry	Note
Serial Number	The serial number assigned by the manufacturer.
Firmware-Version	The currently installed firmware on the device.
Kernel Version	The firmware of the HG G-76343/4/5 is based on Linux. This version-number refers to the Linux kernel version that has been used for the firmware. 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. For more information see chapter 16 on page 116.

### 5.1.2 Wireless Status Information

This section contains information about the Wireless LAN state:

**Figure 31** Web interface: Wireless status information

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 18** Web interface: Wireless Status Information (part 1 of 3)

Entry	Note
Operation Mode	The radio modem can be used as a client in a Wireless LAN Infrastructure or as a device in Adhoc Mode.
AP Mac Address (BSSID)	This is the MAC-Address of the access point (AP) the radio modem is connected to. If the AP transmits a device name, then the name will also be displayed here.
SSID	This is the name of the Wireless LAN network the HG G-76343/4/5 is supposed to or has connected to.

**Table 18** Web interface: Wireless Status Information (part 2 of 3)

Entry	Note																										
Connection state	<p>State of the connection to the AP. The shown status information depends on the authentication method in use:</p> <p><b>Table 19</b> Web interface: Possible messages connection state</p> <table> <tr> <th>State</th><th>Meaning</th></tr> <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>	State	Meaning	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
State	Meaning																										
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	<p><b>Table 20</b> Web interface: Display for active encryption</p> <table> <tr> <th>Encryption</th><th>Output</th></tr> <tr> <td>WEP</td><td>WEP-40 (104)</td></tr> <tr> <td>WPA(2,3)</td><td>WPA(2,3)-PSK</td></tr> <tr> <td>WPA(2,3) Enterprise</td><td>WPA2(3)/IEEE 802.1X/EAP</td></tr> </table>	Encryption	Output	WEP	WEP-40 (104)	WPA(2,3)	WPA(2,3)-PSK	WPA(2,3) Enterprise	WPA2(3)/IEEE 802.1X/EAP																		
Encryption	Output																										
WEP	WEP-40 (104)																										
WPA(2,3)	WPA(2,3)-PSK																										
WPA(2,3) Enterprise	WPA2(3)/IEEE 802.1X/EAP																										
Connection time	Duration of the connection between HG G-76343/4/5 and the current AP																										
Bitrate	Bitrate that is used to send data to the AP																										
Channel/Frequency	Channel number and frequency that is used for the connection to the AP																										



**Table 18** Web interface: Wireless Status Information (part 3 of 3)

Entry	Note												
SNR	<p>Signal quality as measured by the Signal-to-Noise-Ratio) The SNR has the following ranges:</p> <p><b>Table 21</b> Web interface: SNR Quality of the reception signal</p> <table> <tr> <th>SNR</th><th>State</th></tr> <tr> <td>≥ 40</td><td>very good connection</td></tr> <tr> <td>≥ 30</td><td>good connection</td></tr> <tr> <td>≥ 20</td><td>connection just ok, depending on the configuration (→ Roaming, 8.5 on page 80) the radio modem starts looking for „better“ APs by scanning the other channels.</td></tr> <tr> <td>≥ 10</td><td>weak signal! The WLAN client will frequently scan for APs with a stronger signal. The data throughput will be interfered</td></tr> <tr> <td>&lt; 10</td><td>very weak signal. The connection can get lost</td></tr> </table> <p>Additionally static SNr values are shown:</p> <ul style="list-style-type: none"> <li>– Min <b>xx</b> dB Max <b>yy</b> dB, 24h: Min <b>aa</b> dB Max <b>bb</b> dB</li> <li>– xx + yy = minimum and maximum SNR values of the connection to the current AP</li> <li>– aa + bb = minimum and maximum SNR values of the last 24 hours</li> </ul>	SNR	State	≥ 40	very good connection	≥ 30	good connection	≥ 20	connection just ok, depending on the configuration (→ Roaming, 8.5 on page 80) the radio modem starts looking for „better“ APs by scanning the other channels.	≥ 10	weak signal! The WLAN client 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 connection												
≥ 30	good connection												
≥ 20	connection just ok, depending on the configuration (→ Roaming, 8.5 on page 80) the radio modem starts looking for „better“ APs by scanning the other channels.												
≥ 10	weak signal! The WLAN client 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, between -30 to -90 dBm												
Noise	Noise level, usually between -90 to -95 dBm												
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.</p> <ul style="list-style-type: none"> <li>– Green → low utilization</li> <li>– Orange → moderate utilization</li> <li>– Red → high utilization</li> </ul>												

### 5.1.3 Wired LAN Status Information

This section shows the current status of the LAN ports.

**Figure 32** Web interface: Wired LAN Status Information

Wired LAN Status Information	
LAN link state	Link: <b>Up</b> Speed: 100MBit/s Duplex: Full MDI-X: Cross

**Table 22** Web interface: Wired LAN Status Information

Entry	Note
LAN link state	Link <ul style="list-style-type: none"> <li>– <b>Down</b> → no LAN cable with an active Ethernet client connected</li> <li>– <b>Up</b> → LAN cable with an active Ethernet client connected</li> </ul>
	Speed <b>10, 100, 1000</b> MBit/s → transfer rate
	Duplex <b>Half / Full</b> → Simultaneous sending and receiving not possible / possible
	MDI-X <b>Straight, Cross</b> → MDI-X State

### 5.1.4 Relay Status Information / IO-Info (Optional)

This section shows the current state of the optional relay and input, as soon as they are activated.

**Table 23** Web interface: Relay Status Information / IO-Info (Optional)

Entry	Note														
Relay	Operating mode of the relay.														
	<b>Table 24</b> <i>Web interface: Operating modes relay</i>														
	<table><tr><th>Modus</th><th>Function</th></tr><tr><td>Disabled</td><td>Function inactive</td></tr><tr><td>TCP (UDP)</td><td>The relay function opens a TCP (UDP) - Socket and listens on the configured port.</td></tr><tr><td>Internal</td><td>The relay is controlled by the digital input.</td></tr><tr><td>Serial Trigger</td><td>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 device connected to the radio modem. The relay switches off again if no data are sent over the serial interface longer than <i>timeout</i>.</td></tr><tr><td>WLAN Status</td><td>The relay switches on if a WLAN connection is available.</td></tr><tr><td>MQTT Client</td><td>The Relay is controlled via MQTT</td></tr></table>	Modus	Function	Disabled	Function inactive	TCP (UDP)	The relay function opens a TCP (UDP) - Socket and listens 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 device connected to the radio modem. The relay switches off again if no data are sent over the serial interface longer than <i>timeout</i> .	WLAN Status	The relay switches on if a WLAN connection is available.	MQTT Client	The Relay is controlled via MQTT
	Modus	Function													
	Disabled	Function inactive													
	TCP (UDP)	The relay function opens a TCP (UDP) - Socket and listens 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 device connected to the radio modem. The relay switches off again if no data are sent over the serial interface longer than <i>timeout</i> .													
WLAN Status	The relay switches on if a WLAN connection is available.														
MQTT Client	The Relay is controlled via MQTT														
Current State	Current state of the relay, on or off														

### 5.1.5 Serial1

This section shows the current state of the serial Port.

**Figure 33** Web interface: Serial1 Status Information

<b>Serial 1</b>	
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

**Table 25** Web interface: Serial1

Entry	Note
State	Shows whether the serial port is active
Device	This specification refers to the hardware interface of the serial port. The normally used processor internal device is: <code>/dev/ttymx0</code> If a compatible USB <-> serial adapter is connected the following declarations like <code>/dev/ttyUSB0 (1,...)</code> are also possible
Network Connection	The configured port mode is shown here followed by the current state of the connection with IP and port of the connected device, e.g. Mode: 'TCP-Server' IP: 0.0.0.0:0 (Listen Port 8888)
Baudrate Parity Databits	These are the currently configured parameters of the serial interface.
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	These values shown here, inform us how many bytes or data packets via the serial port has been sent or received.

### 5.1.6 Network Information

This section displays information on the active network interfaces. The information displayed depends on the configured bridge mode (see chapter 6 on page 58).

**Table 26** Web interface: Network Information

Bridge Type	Information shown (depending on the configuration of the HG G-76343/4/5 and the connected LAN clients)	
LAN Client Cloning	<b>Bridge</b> Bridge Type LAN Client Cloning Client Detection Detected Client information by DHCP Client IP 192.168.170.63 (Autodetected) Client Netmask 255.255.255.0 (Autodetected) Client Gateway 192.168.170.249 (Autodetected) Client DNS 8.8.8.8 (Autodetected) Client Hostname LAPTOP-BLROHEN0 (From DHCP Request) Client MAC 54:E1:AD:B4:DB:81 (Autodetected) Original WLAN Card MAC 00:0E:8E:B4:F5:22 LAN MAC 90:5F:8D:04:FB:96	
NAT or Single Client NAT	<b>Network Information</b> Interface Wireless (IPv4) IP 192.168.170.79 (DHCP successful) Broadcast 192.168.170.255 Netmask 255.255.255.0 MAC 00:0E:8E:B4:F5:22 default gw 192.168.170.249 Interface LAN (IPv4) IP 192.168.2.100 (Static IP) Broadcast 192.168.2.255 Netmask 255.255.255.0 MAC 90:5F:8D:04:FB:96 Interface lo (IPv4) IP 127.0.0.1 Broadcast 127.0.0.1 Netmask 255.0.0.0 Routing Default gateway 192.168.170.249 on Wireless  <b>Bridge</b> Bridge Type Nat  <b>DHCP Server Status (LAN)</b> Dynamic IP Range 192.168.2.10 - 192.168.2.20  <b>Active clients</b> DHCP Client 1 54:E1:AD:B4:DB:81 192.168.2.10 (LAPTOP-BLROHEN0)	
Level 2 Pseudo-Bridge	<b>Network Information</b> Interface Wireless (IPv4) IP 192.168.170.79 (DHCP successful) Broadcast 192.168.170.255 Netmask 255.255.255.0 MAC 00:0E:8E:B4:F5:22 default gw 192.168.170.249 Interface LAN+ (IPv4) IP 1.1.1.1 Broadcast 1.255.255.255 Netmask 255.255.255.255 MAC 90:5F:8D:04:FB:96 Interface LAN (IPv4) IP 192.168.170.79 Broadcast 192.168.170.255 Netmask 255.255.255.255 MAC 90:5F:8D:04:FB:96 Interface lo (IPv4) IP 127.0.0.1 Broadcast 127.0.0.1 Netmask 255.0.0.0 Routing Default gateway 192.168.170.249 on Wireless  <b>Bridge</b> Bridge Type Level 2 Bridge  <b>Level 2 Bridge Status</b> Bridge Entry 1 LAN1: 54:E1:AD:B4:DB:81 192.168.170.63 (5sec)	

### 5.1.7 Access Point Information

**Figure 34** Web interface: Access point list

Access point list									
BSSID	SSID	Security	SNR	AP Name	Channel/Frequency	Max Bitrate	Last Seen	Extra Information	
00:A0:57:22:41:4A	LANCOMacn	[WPA2-PSK-CCMP]	48dB	LANCOM_acn_2	48: 5240MHz	54.0 + 11n: BW 20MHz	1	DE 4/1% 802.11k (1) Roam 0/2 -95dBm	
00:A0:57:22:41:2A	LANCOMacn	[WPA2-PSK-CCMP]	22dB	LANCOM_acn_1	44: 5220MHz	54.0 + 11n: BW 40MHz	30	DE 1/9% Roam 0/1 -95dBm	
68:86:A7:13:81:1E	RadiusTest	[WPA2-EAP-TKIP+CCMP] [WPA-EAP-TKIP+CCMP]	54dB	CAP-3502E-H	60: 5300MHz	54.0 + 11n: BW 20MHz	158	DE 12/10% 17dBm -95dBm	
0E:A0:57:22:41:4A	LANCOM_WPA3as	[WPA2-PSK-SHA256-CCMP]	50dB	LANCOM_acn_2	48: 5240MHz	54.0 + 11n: BW 20MHz	30	DE 0/1% -95dBm	

on mouse hover

Neighbor (11sec):  
Ch44  
00:A0:57:22:41:2A  
Last Seen Extra 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 APs.

In this section a list of all access points that are registered by the WLAN client is displayed. The list entry of the currently connected AP is highlighted in gray and is always displayed in the first position. This is followed by the APs with the appropriate SSID, which can also be used for a connection. These are displayed in **green font**.

Then APs with other or unknown SSID (hidden) are listed. The information under *Security* shows what authentication methods are expected by these APs.

If an AP offers the SSID matching the HG G-76343/4/5 but the AP's security settings prevent the radio modem from connecting to the AP, the security information is **displayed in red**.

The same applies to the column *Channel/Frequency* if the AP works on a channel that is not included, for example, by specifying a channel list under Configuration → Wireless → Roaming.

The *Extra Information* column contains the following information (if available):

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

### 5.1.8 HTTPS Webinterface

The websites of the radio modem can also be accessed via HTTPS (Hypertext Transfer Protocol Secure). This enables an encrypted data exchange between radio modem and web browser. The HTTPS server on a configurable TCP port (default 443) is activated under *Admin* (see section 5.3.1 on page 50).



For this access, the radio modem uses a self-generated server certificate that must be confirmed in the web browser during the first connection. The browser usually reports an insecure connection or certificate problems. This message usually offers a way to continue to the site nonetheless. The browser's confirmation message varies depending on the browser type, e.g.: Advanced - add exception, continue, load website nonetheless, ...



To avoid this procedure it is also possible to load an own registered server certificate into the radio modem, see section 5.3.1 on page 50.

### 5.1.9 Storage Status Information

**Figure 35** Web interface: USB Storage Status Information

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

A USB memory stick can be connected to the radio modem, which can be used to store debug messages or recordings on the WLAN or LAN interfaces. When such a USB memory stick is plugged in, the status of this memory is displayed at the bottom of the home page.

Before removing the memory stick, the user should disconnect the memory from the system using the *Unmount* function to ensure that the contents remain consistent. In particular, if the USB stick is formatted as a FAT file system, errors in the file system of the USB stick may occur when switching off without first unmounting.

If the USB stick is used to record debug messages and/or (W)LAN recordings (see chapter 10 on page 87), the USB stick should be formatted with the EXT4 file system. This file system is more robust in terms of data consistency when the radio modem is suddenly switched on and off.



All existing files on the USB stick are deleted during formatting!

Therefore, the function *Format as EXT4 Filesystem* is offered here. This formats the currently inserted USB stick with the EXT4 format.

### 5.1.10 WLAN and LAN Dump Files

**Figure 36** Wireless Dump / Ethernet Dump file list

<b>Wireless Dump</b>	
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)
<b>Ethernet Dump</b>	
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)

If the recording of the communication on the WLAN and/or LAN interface is activated, the resulting files are listed here. The files contain the recorded data in compressed form of the type .gz. Only the files that are currently being written are of type .pcap.

For more information, see section 10.2 on page 90.

## 5.2 Device Menu (Firmware and Configuration Management)

In this menu item you can transfer firmware files to the HG G-76343/4/5 or save and restore the currently configured parameters in a file.

### 5.2.1 Firmware

With this dialog a firmware file can be uploaded to the radio modem.

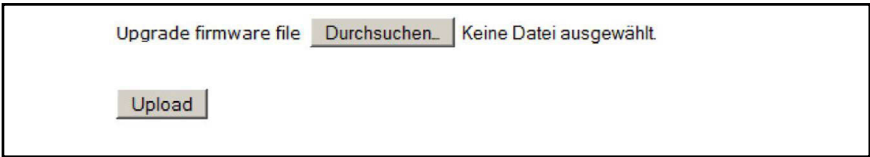
#### NOTICE

##### Incomplete Firmware

If the firmware is incompletely transmitted the device might not work anymore. While uploading a firmware file:

- ▶ Do not interrupt the power supply.
- ▶ Do not press the reset key.

Figure 37 Web interface: Firmware upload dialog



5.2.2 Configuration Management

Figure 38 Web interface: Configuration management

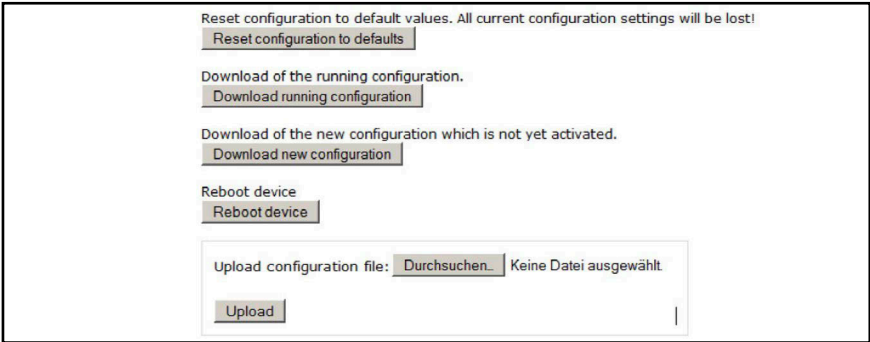


Table 27 Web interface: Configuration Management

Button	Function
Reset configuration to defaults	With this button all parameters can be set to the factory default values. The user can either confirm this setting with the button <i>Save &amp; apply</i> . Alternatively the button declines <i>Cancel changes</i> the changes. <div><div>Unsaved Changes!!</div><div>Save &amp; apply</div><div>Cancel changes</div></div>
Download running configuration	With this button the running configuration can be stored to a file. <i>Running configuration</i> means the configuration that is currently active on the WLAN client <b>without</b> the changes made temporarily within the actual configuration session.
Download new configuration	With this button the new configuration can be stored to a file. <i>New configuration</i> means the configuration that is currently active on the device <b>including</b> the changes made within the actual configuration session.
Reboot device	With this button the device will perform a reboot. <b>Changes made in the actual session will get lost!</b>
Upload configuration file	With this dialog a config file can be selected and <i>uploaded</i> to the HG G-76343/4/5. If parameters of the current configuration are changed with this upload, a dialog box will appear to <i>Save &amp; apply</i> . You can reverse the loading of the parameters via <i>Cancel changes</i> .

### 5.2.3 Network Test



This function is available in firmware version 2.14b and higher.

**Figure 39** *Web Interface: Network Test*

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:

**Table 28** *Web Interface: Network Test*

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 <i>Payload</i> .
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. <i>Clear Results</i> followed by <i>Filter UDP RX</i> 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.



### 5.3 Configuration (of the Operating Parameters)

The Configuration menu has a collection of items to get to the configuration dialogs for all of the WLAN client's functions. Depending on the built-in options of the HG G-76343/4/5 some of this submenu items will not appear. The following table shows all currently available sub menus.

**Table 29** *Web interface: configuration menus*

Menu item	important parameters	requirement
Admin	Device name, user, password	
Network	IP address, Bridge mode	
Wireless	SSID, security	
Serial Ports	Baudrate, mode etc.	Serial interface
Printer Server	USB printer mode	USB port
Relay	Relay mode	Relay switch
Realtime clock	NTP server IP	
LAN-Port	LAN port settings	
Logging	Debug messages on / off	

The menus mentioned are described and explained in more detail in the following sections.

### 5.3.1 Admin Menu

**Figure 40** Web interface: Admin page

**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.

**Security (access protection)**

**Administrator Login:** To protect the configuration of the radio modem from being changed or read out, you can define an *Admin* with *Name* and *Password* here.

**Monitor Login:** For someone who should only see the configuration but not be able to 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 radio modem via a link. The *Community name* is set to *public* by default.

**Webserver:** The web server of the radio modem 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.

The screenshot displays the Admin page of a web interface with the following sections and fields:

- Device Name:** Device Name: LBLWRT400 USB. A note states: "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: HG76343. A note: "This is the admin user name that must be entered to get access to these pages." Admin password: [masked]. A note: "This password must be entered to get access to these pages."
  - Monitor Login (Read Only Access):** Monitor name: [empty]. A note: "This is the monitor user name for read only access to these pages." Monitor password: [empty]. A note: "This is the password of the monitor user for read only access to these pages."
- SNMP:** Enable SNMP: [checkbox]. A note: "Check this box to enable SNMP server. Download MIB here."
- Webserver:**
  - Enable Unencrypted (HTTP): [checked]. A note: "Check this box to enable standard unencrypted webserver."
  - Webserver Port: 80. A note: "Configure a alternative webserver port to avoid a collision with a LAN-Client setup. Default is port 80."
  - Enable Secure (HTTPS): [checkbox]. A note: "Check this box to enable secure webserver over https."
  - Show website state: Show Information without Authentication. A note: "Select to restrict state information on webpage."
- Configuration tool accessibility:**
  - MC-Config Port: WLAN+LAN. A note: "Port selection for MC-Config-Tool accessibility of the device."
  - Enable TLS: [checkbox]. A note: "Check this box to enable secure its connection for dump downloads and firmware upgrades (requires recent configuration tool)."
- Other Options:**
  - Serial port instances: 1. A note: "Number of serial port instances."
- Power Save:**
  - Enable Power Save Interface: [checkbox]. A note: "Enable interface for remote controlled power down periods."
  - Debug Level: Information. A note: "Select debug level for power save function."
- Securing Passwords:**
  - Secure Passwords: [checkbox]. A note: "WARNING: Enable to secure passwords limits exporting passwords an downgrade possibilities."
- Webserver certificate:**
  - Use a custom webserver certificate. If no custom certificate is set the device generates a self signed certificate instead.
  - Certificate Password: [empty]. A note: "Enter certificate password."
  - Webserver certificate info: Information about loaded client certificate.
  - Upload certificate file: [Durchsuchen...] Keine Datei ausgewählt. [Upload]

*URL Authentication:* Access to the REST-API is normally regulated according to the specification of Admin user/password or Read-Only user/password. To avoid having to provide this user/password information to use the Rest API, separate access rules can be defined for certain URLs. For example, if you want to query the status of the WLAN connection without user/password, you can do this as follows.

**Figure 41** Web Interface: Admin → URL Authentication

*Configuration tool accessibility:* With this setting the access for the MC-Config tool can be restricted:

- ♦ WLAN+LAN
- ♦ LAN
- ♦ none

*Other options:* Here you can define how many *Serial port instances* are to be used. The number of serial ports can be extended by connecting suitable adapters to the USB port.

*Power Save:* With this option it is possible to set the radio modem 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. For how to use the power save function please contact the service.

*Securing Passwords:* By activating this option you can define that the passwords and keys (e.g. PSK) stored in the Config are not transferred when downloading the Config file. Thus you can prevent that these data can be read out from the stored Config file of a radio modem.



Once *Securing Passwords* has been activated, it is no longer possible to deactivate this option. This option can only be switched off via a default reset. It is also not possible to downgrade the firmware while *Securing Passwords* is active.

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

### 5.3.2 Network Menu

Allows to change the network settings of the device and to configure the Bridge function.

#### 5.3.2.1 IP Address

**Figure 42** Web interface: Network > IP settings

**Enable DHCP Client:** By activating this option, the radio modem obtains the network settings via DHCP. Usually this will be done over an existing WLAN connection. If this parameter is empty, the *Device Name* from the Admin page is used.

**Enable Fallback to Static IP:** In case no DHCP server can be reached the radio modem uses the static settings.

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

The screenshot shows the 'IP settings' page in the web interface. The navigation bar at the top includes 'Home', 'Device', 'Configuration' (selected), 'Statistics', and 'Support'. Under 'Configuration', there are tabs for 'Admin', 'Network' (selected), and 'IP address'. The main content area is titled 'IP settings' and contains the following fields and options:

- Enable DHCP Client:** A checkbox that is checked. Below it is a note: 'Check this box to enable the dhcp client for IP configuration. (Disabled for LAN-Client-Cloning)'.
- Host Name:** An empty text input field. Below it is a note: 'This information is sent to the DHCP server as the parameter "hostname" during the DHCP process. If this parameter is empty the parameter "Device Name" (see -> Admin) is used'.
- Enable Fallback to Static IP:** A checkbox that is checked. Below it is a note: 'Check this box to enable fallback to static IP if the dhcp client fails'.
- Default IPv4 address:** A text input field containing '192.168.170.105'. Below it is a note: 'Type the IP address of your bridge'.
- Default Subnetmask:** A text input field containing '255.255.255.0'. Below it is a note: 'The subnet mask specifies the network number portion of an IP address. The factory default is 255 255 255 0'.
- Gateway Address:** A text input field containing '192.168.170.249'. Below it is a note: 'This is the IP address of the gateway that connects you to the internet'.
- Nameserver Address (DNS):** A text input field containing '0.0.0.0'. Below it is a note: 'This is the IP address of the nameserver (DNS)'.
- Backup DNS 1:** A text input field containing '0.0.0.0'. Below it is a note: 'This is the IP address of the backup DNS 1'.
- Backup DNS 2:** A text input field containing '0.0.0.0'. Below it is a note: 'This is the IP address of the backup DNS 2'.

**Figure 43** Web interface: Network > Gateway Settings

The screenshot shows the 'Gateway Settings' page. It features a table with the following structure:

Format: <SubnetIP>/<MaskBits>,<GatewayIP>	
Subnet 1	<input type="text"/>
Subnet 2	<input type="text"/>
Subnet 3	<input type="text"/>

Below the table are two buttons: 'Add' and 'Remove'.

With these parameters you can define other gateway IPs for certain networks.

#### 5.3.2.2 IPV6 Settings (experimental)

**Figure 44** Web interface: Network > IPV6 Settings

The screenshot shows the 'IPv6 settings' page. It contains the following fields and options:

- Enable IPv6 Support (experimental):** A checkbox that is checked. Below it is a note: 'Check this box to enable IPv6 support (interface autoconfiguration)'.
- Debug IPv6:** A dropdown menu currently set to 'Detailed'. Below it is a note: 'Select log configuration IPv6'.
- Enable Bridge:** A checkbox that is unchecked. Below it is a note: 'Check this box to enable IPv6 bridge support. Forwarding router advertise with prefix'.

This activates the IPV6 functionality of the radio modem. This function is still in the development stage. So far only the internal web server can be reached via IPV6.

### 5.3.2.3 mDNS Settings

**Figure 45** Web interface: Network > mDNS Settings

**mDNS settings**

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

Debug mDNS:  Select log configuration for mDNS/LLMNR.

Enable LLNMR ☒ 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]mc.dev.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.

**Enable mDNS Support:** 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.

### 5.3.2.4 Bridge

The bridge mode configuration is explained in chapter 6 on page 58.

### 5.3.2.5 MQTT Client

The MQTT client configuration is explained in chapter 7 on page 71.

## 5.3.3 Wireless / Parameters of WLAN Interface

The configuration of the WLAN interface is explained in chapter 8 on page 73.

## 5.3.4 Serial Port

The configuration of the WLAN interface is explained in chapter 9 on page 84.

## 5.3.5 Printer Server

The print server offers the possibility to connect a printer via the USB interface of the HG G-76343/4/5. If a printer is connected and has been recognized by the operating system of the HG G-76343/4/5, the status as shown below is shown on the Home page (example).

**Figure 46** Web interface: Printer server configuration

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 HG G-76343/4/5 expects the connections (TCP server mode). The default port is number 9100 (RAW port).

### 5.3.6 Relay

The HG G-76343/4/5 has a relay that can be activated in different ways. Usually it is used to e.g. realise a sleeping/stand-by mode for vehicles running on battery power. The following parameters set the function of the relay.

#### 5.3.6.1 Relay Parameter

**Table 30** Web interface: Onboard Relay (part 1 of 2)

Parameter	Function																
Enable	This switches the relay function on or off																
Mode	Operational Mode: <div> <b>Table 31</b> Web Interface: Relay Modes <table> <tr> <th>Modus</th><th>Function</th></tr> <tr> <td>UDP</td><td>Control via data received via a UDP/IP socket on a <i>Local Port</i>.</td></tr> <tr> <td>TCP</td><td>Control via data received via a TCP/IP server socket on a local port.</td></tr> <tr> <td>internal</td><td>Control via the input signal (AUX input, not relevant for Götting devices).</td></tr> <tr> <td>SER trigger</td><td>Switch on relay if characters for the serial interface were received via (W)LAN</td></tr> <tr> <td>WLAN Status</td><td>Switch on the relay if there is a WLAN connection, otherwise the relay is switched off.</td></tr> <tr> <td rowspan="3">MQTT</td><td>The relay is controlled via MQTT. Parameters for this mode:</td></tr> <tr> <td>MQTT Ctrl Topic: The MQTT client subscribes to this topic to receive relay control data.</td></tr> <tr> <td>MQTT Status Topic: With this topic the state of the relay is sent. A topic is triggered for each change of state of the relay.</td></tr> </table> </div>	Modus	Function	UDP	Control via data received via a UDP/IP socket on a <i>Local Port</i> .	TCP	Control via data received via a TCP/IP server socket on a local port.	internal	Control via the input signal (AUX input, not relevant for Götting devices).	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.	MQTT	The relay is controlled via MQTT. Parameters for this mode:	MQTT Ctrl Topic: The MQTT client subscribes to this topic to receive relay control data.	MQTT Status Topic: With this topic the state of the relay is sent. A topic is triggered for each change of state of the relay.
Modus	Function																
UDP	Control via data received via a UDP/IP socket on a <i>Local Port</i> .																
TCP	Control via data received via a TCP/IP server socket on a local port.																
internal	Control via the input signal (AUX input, not relevant for Götting devices).																
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.																
MQTT	The relay is controlled via MQTT. Parameters for this mode:																
	MQTT Ctrl Topic: The MQTT client subscribes to this topic to receive relay control data.																
	MQTT Status Topic: With this topic the state of the relay is sent. A topic is triggered for each change of state of the relay.																
Relay restore	With this activated the position of the relay is preserved through a re-start of the device (re-boot of the software).																
Relay ON	If you want the relay to be switched on after the power is turned on, check this option. After the <i>timeout</i> period has elapsed, the relay will switch back to the idle state.																
Local Port	Port number for the operational modes UDP or TCP																

**Table 30** Web interface: Onboard Relay (part 2 of 2)

Parameter	Function
ON Phrase	Character string to switch on the relay in UDP or TCP mode. If nothing is specified here, every character arriving on the port switches the relay on. Starting with version 2.12k, the firmware offers an extension for delayed relay switch-on, see section 5.3.6.2 below.
OFF Phrase	Character string to switch off the relay in UDP or TCP mode. Starting with version 2.12f, the firmware offers an extension for delayed relay switch-off, see section 5.3.6.2 below.
Timeout	Time in seconds until the relay is switched off again after switching on. The value 0 means infinitely long.

When the radio modem receives the correct ON or OFF phrase it switches the relay to the appropriate state and responds with a character string corresponding to the then 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 string of characters to the radio modem and it will respond with the current status.

#### 5.3.6.2 Delayed switching on and off of the relay

Starting with firmware versions 2.12f/2.12k, it is possible to have the commands for switching the relay on or off executed with a time delay. For this purpose, a time specification in angle brackets is sent to the corresponding TCP or UDP port of the radio modem directly after the ON phrase or the OFF phrase.

**Example:** The ON phrase is set to ON. Then you can send the string ON<15> to the radio modem so that the relay switches on delayed by 15 seconds.

If a time delay is active, the radio modem responds with a character string that reflects the last command (ON or OFF) followed by the remaining delay in angle brackets.

**Example:** ON<xx> where xx is the current number of seconds to switch on.

### 5.3.7 Realtime Clock

The HG G-76343/4/5 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 HG G-76343/4/5 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) using NTP. The setting of a time server is absolutely necessary if the SCEP functionality is used. However, there are also great advantages if system messages of the HG G-76343/4/5 can be provided with a correct time stamp.



Table 32 Web interface: Realtime Clock

Parameter	Function
Enable	Enables the NTP client
NTP-Server	Here an IP address or host name of a time server (e.g. <code>ptbtime1.ptb.de</code> ) can be entered. The default value is <code>192.53.103.108</code> . If a host name is entered the network connection (WLAN) must have a DNS IP defined (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 radio modem is operated must be specified here.
Enable DST/Summertime	In regions with daylight saving time, this option must be activated.

### 5.3.8 Input (optional)



The radio modem can optionally be equipped with a digital input signal on demand (when ordering). With the input the connectors on the back plane change (s. Figure 3 on page 11). The software allows to configure the input even if the hardware is not present. For Götting devices this AUX option is not relevant.

### 5.3.9 Logging (Debug)

The Logging of system messages for the diagnosis of problems is described in chapter 10 on page 87.

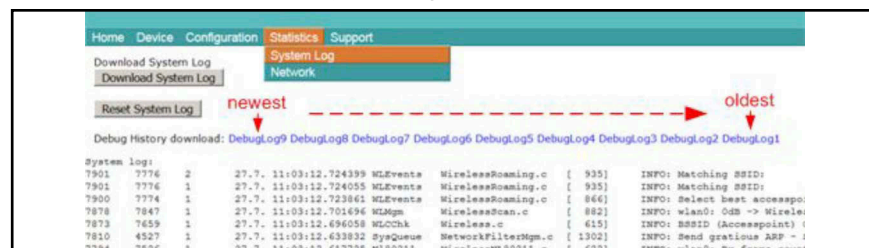
## 5.4 Statistics

The Statistics menu gives you access to information regarding the activity on the LAN + WLAN interfaces and watch and download system stored messages.

### 5.4.1 Statistics – System Log

Here the messages are shown, that are stored on the HG G-76343/4/5. Which messages are logged depends on the settings in Configuration → Logging ab (s. chapter 10 on page 87). There you can adjust the logging *intensity* for the different firmware modules.

Figure 47 Web interface: Example for a System Log output



The button *Download System Log* has the effect, that the last messages and the current configuration are combined into a single file that is downloaded from the WLAN client. The button *Reset System Log* deletes all messages and all files that have been created during the logging of the communication via the WLAN or LAN interfaces.



Starting with firmware 2.11p, a list with links is displayed under *Debug history download*. The DebugLog files can be downloaded from the radio modem 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:

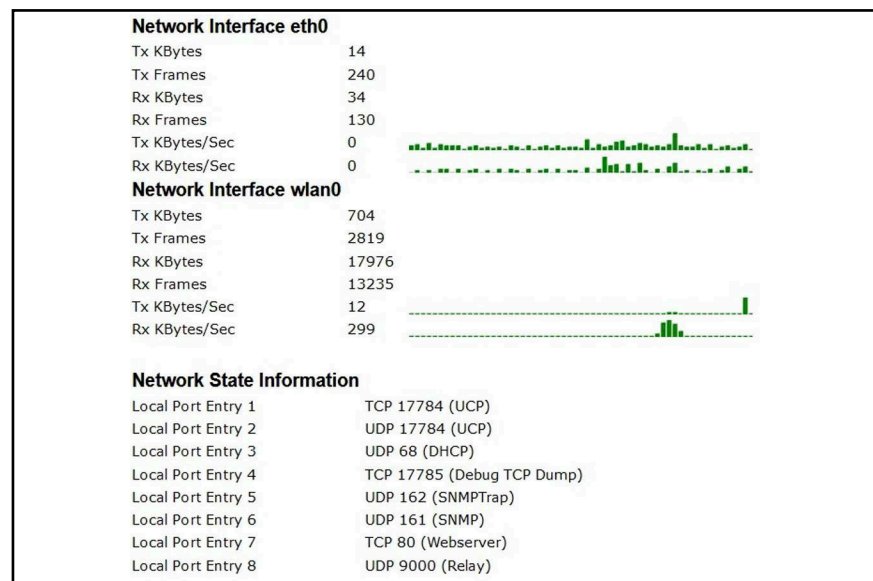
DebugLog.dat.xxxxx.old.gz

xxxxx is a numbering that counts down from left to right.

### 5.4.2 Statistics - Network

This sub menu shows statistics of the network interfaces. The section *Network Interface eth0* shows them for the LAN interface, the section *Network Interface wlan0* for the WLAN interface. *Network State Information* shows, which ports are opened on the radio modem and which connections currently exist.

**Figure 48** Web interface: Example for a Statistics Network output



## 5.5 Support

An *About* menu gives information about the components in use:

- ♦ Linux version
- ♦ Libraries used for the Web Interface
- ♦ OpenSSL Version



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. For more information see chapter 16 on page 116.

## 6

## Bridge Modes

The HG G-76343/4/5 supports 5 different Bridge Modes, that are explained in this chapter. The modes differ in how transparent the LAN clients connected to the HG G-76343/4/5 are connected to the WLAN, which MAC address the LAN clients operate in the WLAN and whether the LAN clients have an IP address of their own in the WLAN.

**Table 33** Bridge Modes

Bridge-Mode	LAN clients	IP's in WLAN	Transparency	Note
OFF	any number	1 (Radio Modem IP)	Disconnected	If the bridge function is disabled, the LAN clients cannot communicate with other devices via the radio modem's WLAN interface.
LAN Client Cloning	1	1 (LAN Client IP)	all Ports	IP- and MAC-address of the LAN-Client is registered in the WLAN.
Single Client NAT	1 + x	1 (Radio Modem IP)	all Ports	IP- and WLAN-MAC-address of the radio modem is registered in the WLAN. Only 1 LAN-Client can be reached via WLAN. All other LAN-Clients can communicate with each other and with the WLAN.
NAT	any number	1 (Radio Modem IP)	Ports def. per Config	IP- and WLAN-MAC-address of the HG G-76343/4/5 is registered in the WLAN.
Level 2 Bridge	any number	n LAN-Clients + 1	all Ports	All LAN-Client-IPs and the IP of the HG G-76343/4/5 are registered with the WLAN-MAC-address of the HG G-76343/4/5.
MWLC-Mode	any number	1 (Radio Modem IP)	all Ports	Only the IP- and the WLAN-MAC-address of the HG G-76343/4/5 is registered in the WLAN.

### 6.1 Bridge not active Mode

If the bridge function of the radio modem is switched off, the radio modem can be accessed both from the WLAN and via the LAN interface without data being exchanged between the LAN and WLAN.

In this mode, 2 different IP addresses (LAN + WLAN) can be configured for the radio modem via which the MC internal functions such as relay, serial interface, web interface etc. can be accessed. This mode should be selected if:

- ♦ the WLAN interface is switched off.
- ♦ the radio modem should only be used as Ethernet-to-serial adapter. This way you can ensure that the radio modem's LAN port cannot be used to access the WLAN.

The IP configuration for the WLAN interface is set as usual under Configuration -> Network -> IP Address (see 5.3.2.1 on page 52). The IP configuration for the LAN side becomes visible as soon as the *Bridge active* option is deactivated.

**Figure 49** Bridge Modes: Bridge OFF

**Routing Priority:** If WLAN and LAN are active, a gateway is usually also defined for both interfaces. If an application on the radio modem 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.

**Figure 50** Bridge Modes: Bridge OFF > Gateway Settings

With these parameters you can define other gateway IPs for certain networks.

## 6.2 LAN Client Cloning

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

If the radio modem 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.



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

**Figure 51** Bridge Modes: LAN Client Cloning parameters 1

**LAN Port Delay:** If the wireless modem is switched on together with the LAN client, it is possible that the LAN client is ready faster than the wireless modem. In this case, the LAN client could, for example, start DHCP attempts at a time when the radio modem is not yet able to forward data via WLAN. If *LAN Port Delay* is activated, the LAN port on the radio modem is switched on with a delay so that the LAN client only starts its communication later.

**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 radio modem 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 radio modem 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 radio modem. Thus, the WLAN client and the LAN client can be reached via WLAN with this IP address.

The screenshot shows the 'Bridge mode configuration' window. It includes the following settings:

- Bridge active:** Checked (checkbox).
- Bridge mode:** Set to 'LAN Client Cloning' (dropdown menu).
- LAN Port Delay:** Unchecked (checkbox).
- LAN client Type:** Set to 'Autodetect' (dropdown menu).
- LAN Client IP:** Set to '0.0.0.0' (text input).
- Subnet mask:** Set to '255.255.255.0' (text input).
- Gateway IP:** Set to '0.0.0.0' (text input).

Each input field has a small blue tooltip explaining its function. For example, the 'LAN Client IP' tooltip states: 'Type the IP address the LAN client to speed up detection. If detection by DHCP is enabled DHCP-Replies will be used for detection.'

**Figure 52** Bridge Modes: LAN Client Cloning parameters 2

**DNS1 + 2:** If the radio modem 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 radio modem via the LAN side via an IP address other than the gateway IP, you can define it here.

**IP Timeout:** The radio modem constantly checks whether the cloned IP is still accessible. If no response is received after IP Timeout seconds, the WLAN interface of the radio modem is switched off and only switched on again when a new response is registered by the LAN Client IP.

**Stay connected:** Sometimes it is necessary that the WLAN interface of the radio modem remains active even if the LAN client is switched off. E.g. in the case that the relay is used to switch off the LAN client. Then with *Stay connected* active the WLAN connection is held, so that the relay reacts to a switch-on request.

**Forward Wake on LAN:** If this option is active, Wake on LAN packets received via WLAN (udp port 9) are forwarded as a broadcast via the LAN connections of the wireless modem.

**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.

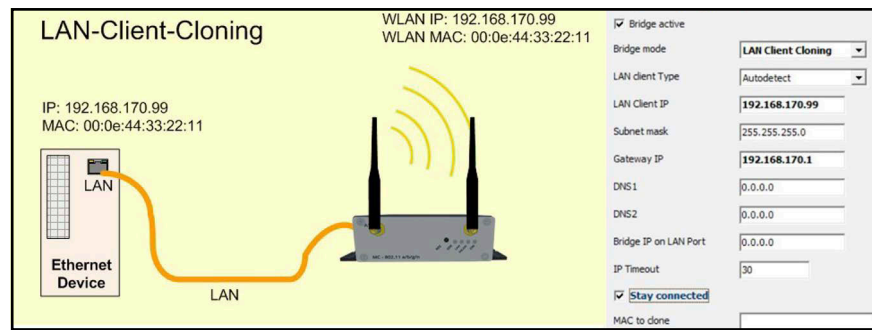
**Preconnect:** Normally, the radio modem in cloning mode only switches the WLAN on when a packet has been received from the LAN client via the LAN port. However, if the LAN client is switched on with the radio modem's relay, for example, the radio modem must activate the WLAN in any case.

**MAC for Preconnect:** The *MAC for Preconnect* parameter is automatically set to the detected client MAC after a start and remains set there. The value can be left blank for the initial setup. In this case, the MAC of the WLAN card is used for the first WLAN connection.

The screenshot shows a configuration page for Bridge Modes: LAN Client Cloning parameters 2. It includes the following fields and options:

- DNS1:** Input field with value 0.0.0.0. Description: DNS Server 1 if not determined by DHCP. This DNS server IP can be used by the MC.
- DNS2:** Input field with value 0.0.0.0. Description: DNS Server 2 if not determined by DHCP. This DNS server IP can be used by the MC.
- Bridge IP on LAN Port:** Input field with value 0.0.0.0. Description: 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:** Input field with value 30. Description: Timeout after detected ip configuration will time out (0 = disable timeout).
- Stay connected:** Checkmark is checked. Description: If enabled, the wireless connection will not go down even when the LAN link is disconnected.
- Forward Wake on LAN:** Checkmark is checked. Description: If enabled, wake on lan packets are forwarded (UDP port 9) and resent on LAN as broadcast packets.
- MAC to clone:** Input field. Description: Define here the MAC address that will be cloned. This is useful when more than one MAC can be detected at LAN port 1.
- Preconnect:** Checkmark is checked. Description: If enabled, the wireless connection will come up using the following mac before the client is found. The following mac is learned back to the configuration in this mode.
- MAC for Preconnect:** Input field. Description: Define here the MAC address that will be used for preconnect. If it is empty the mac wireless card is used initially.

Figure 53 Bridge Modes: Example for LAN Client Cloning



The LAN client's IP address is used to operate the radio modem's internal interfaces (website, serial, relay, USB). In order to avoid collisions with port numbers used on the LAN client the radio modem's port numbers have to be adjusted. If the LAN client also has running a web server on port 80 the radio modem's web server port can be changed at *Configuration → Admin → Webserver Port*.

Advantages of the LAN Client Cloning mode:

1. In the WLAN network, the HG G-76343/4/5 will appear along with the LAN client with only one IP address.

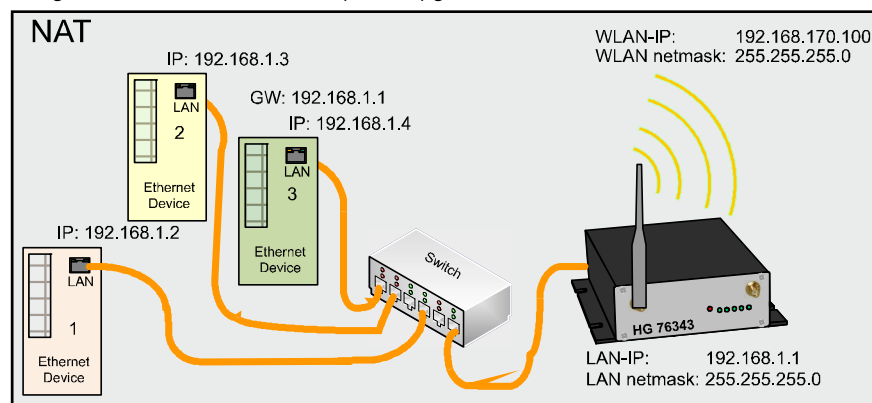
Disadvantage of the LAN Client Cloning mode:

1. Only one LAN client can be connected to the HG G-76343/4/5.

### 6.3 NAT and Single Client NAT Mode

In NAT mode, the HG G-76343/4/5 works with different networks on the LAN and WLAN side. In WLAN the HG G-76343/4/5 communicates with the IP settings as described in 5.3.2.1 on page 52. 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 54 Bridge Modes: NAT mode (example 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*.

**Figure 55** Bridge Modes: Single Client NAT Mode

**Autodetect LAN client:** (Single Client NAT only) 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 only) All connection requests from the WLAN side are forwarded to this IP specified here.

**Local IP address:** With this IP address the radio modem communicates on the LAN side. LAN clients connected to the HG G-76343/4/5 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 page. This eliminates the need to configure a special DNS server on the LAN clients. In this case, only the local IP of the HG G-76343/4/5 must be entered.

**MAC Authentication:** (NAT mode only) To prevent any device plugged into the LAN port of the radio modem from connecting to the WLAN, it is now possible to register the MAC address of the allowed devices. To do this, the permitted radio modem 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 Auth.

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.

The screenshot shows the 'Bridge mode configuration' page. At the top, there is a navigation bar with links: Home, Device, Configuration, Statistics, Support, and Logout. The page title is 'Bridge mode configuration'. Below the title, there are several configuration options:

- Bridge active:** A checkbox that is checked. Below it, a note says 'Do not disable the bridge except the wireless mode is 'accesspoint'.'
- Bridge mode:** A dropdown menu set to 'Single Client NAT'. Below it, a note explains: '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:** A checkbox that is unchecked. Below it, a note says: '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:** A text input field containing '192.168.1.10'. Below it, a note says: 'Define the LAN Client IP address or 0.0.0.0 to autodetect the IP.'
- Local IP address:** A text input field containing '192.168.1.1'. Below it, a note says: 'Type the IP address of your bridge that will be used to the LAN site.'
- Subnetmask:** A text input field containing '255.255.255.0'. Below it, a note says: 'The subnet mask specifies the network number portion of an IP address. The default is 255.255.255.0.'
- Forward DNS requests:** A checkbox that is unchecked. Below it, a note says: 'Check this box to enable forwarding of DNS requests that are send to our local IP address.'
- Enable MAC Authentication:** A checkbox that is checked. Below it, a note says: 'Check this box to enable port authentication via LAN-Client MAC by using configured radius server.'
- Radius server IPv4 address:** A text input field containing '192.168.170.249'. Below it, a note says: 'Type the IP address of the radius server.'
- Radius server port:** A text input field containing '1812'. Below it, a note says: 'Port for radius server.'
- Radius shared secret:** A text input field. Below it, a note says: 'Shared secret for radius server.'
- Authentication Timeout:** A text input field containing '3600'. Below it, a note says: 'Timeout for authentication until reauthentication is required.'
- Radius Debug Level:** A dropdown menu set to 'Default'. Below it, a note says: 'Select log configuration for radius.'



### 6.3.1 Forwarding rules for NAT

**Figure 56** Bridge Modes: 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 is either TCP or UDP):

```
< Protocol > :
< Port definition > :
< Client IP > : Option
```

Protocol is either TCP or UDP.

**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: TCP:8020:192.168.1.10

NAT Rule 2:

NAT Rule 3:

NAT Rule 4:

NAT Rule 5:

Add Remove

DMZ IP: 0.0.0.0

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

Enable NAT Loopback ☐

Enable NAT-Loopback (also known as Hairpinning)

Port definition as forwarding

- Destination** port number does not change
  - Single ports : 1234 : or : 123, 1234, 4545 :
  - Port Ranges : 8000-8010, 120-130 :
- 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 :

Port definition as redirection

- Destination port number changes
  - Single ports : 1234 > 3456 : Client-IP: 192.168.1.10

With Add / Remove the number of NAT rule fields can be set. You can create up to 30 of these rules.

**DMZ IP:** If received data packets cannot be assigned to a recipient via the NAT rules, they are sent to this IP.

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 FTP 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 purpose, 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 the IP packets arriving via WLAN with the IP of the radio modem LAN port.

Example: TCP:12345:192.168.1.10:snat

For further information regarding this setting please have a look here:



[https://en.wikipedia.org/wiki/Network\\_address\\_translation](https://en.wikipedia.org/wiki/Network_address_translation)

### 6.3.2 DHCP Server Settings

**Figure 57** Bridge Modes: DHCP server settings

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

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.

**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.

### 6.3.3 Static DHCP Server entries

**Figure 58** Bridge Modes: Static DHCP server entries

To ensure that LAN clients are always assigned the same IP address after switching on the HG G-76343/4/5 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.

**Static DHCP Server entries**  
Format: <IP>,<MAC>,<NAME>

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

Advantages of the NAT mode:

1. Almost any number of LAN clients can be connected to a HG G-76343/4/5.
2. In the WLAN the HG G-76343/4/5 and all LAN clients appear under a single IP address.
3. If in a project there are several units consisting of a HG G-76343/4/5 and connected LAN clients the configuration is the same for all units. Only the IP address of each HG G-76343/4/5 towards the WLAN has to be individual.
4. In a way the LAN clients are better protected against unwanted access since the HG G-76343/4/5 only forwards data for the specified ports.
5. Local broadcast packets (on the LAN side of the HG G-76343/4/5) are not sent over the WLAN.

Disadvantages of the NAT mode:

1. Access to the LAN clients via WLAN is possible only on the ports defined in the NAT rules.
2. If LAN clients offer server services on the same port numbers (e.g. FTP), the user must define port forwarding rules in a way that these services are addressed on different ports for each LAN client.



---

Make sure that there are no collisions between the port numbers and the internal interfaces of the HG G-76343/4/5.

---

The internal interfaces of the HG G-76343/4/5 are e.g.:

1. Serial port (default Port 8888)
2. Printer server (default Port 9100)
3. HG G-76343/4/5 Webserver (default port 80/https port 443, may be changed under Configuration → Admin → Webserver Port, s. 5.3.1 on page 50)
4. Relay
5. MC-Config (UDP+TCP Port 17784 + 17785)

The device lists the ports in use under Statistics → Network (see section 5.4.2 on page 57).



---

Deactivate interfaces that are not needed.

---

## 6.4 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 HG G-76343/4/5 is used for all LAN clients.



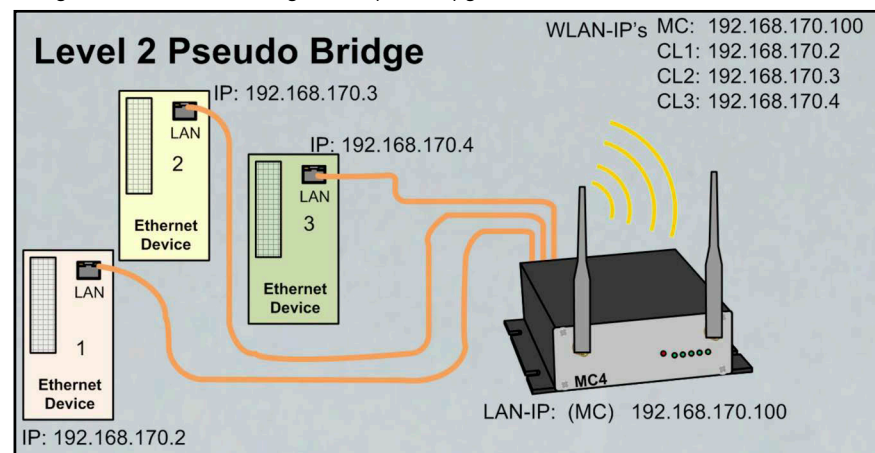
Prerequisite for this mode is that the IP addresses of all LAN clients and also the IP of the HG G-76343/4/5 are in the same network.

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  $\leftrightarrow$  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 59** Bridge Modes: Level 2 bridge example configuration



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

**Figure 60** Bridge Modes: Level 2 Pseudo Bridge Mode

**Scan LAN Clients:** If LAN clients are passive on the HG G-76343/4/5, i.e. do not send data via Ethernet themselves without a request, this function can be used to cause the HG G-76343/4/5 to regularly scan the network on the LAN side via ARP request. As a result, the HG G-76343/4/5 can quickly registered all connected LAN clients, especially after a restart.

**Forward Multicast / Broadcast:** This option determines whether broadcast data arriving at the HG G-76343/4/5 via WLAN is forwarded to the LAN side.

*Enable DHCP Relay Agent:* If the LAN clients on the radio modem obtain their IP address via DHCP, this option can support this by the HG G-76343/4/5 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 radio modem 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 a HG G-76343/4/5 at once.
2. Good transparency of the LAN clients towards the WLAN without configuration.

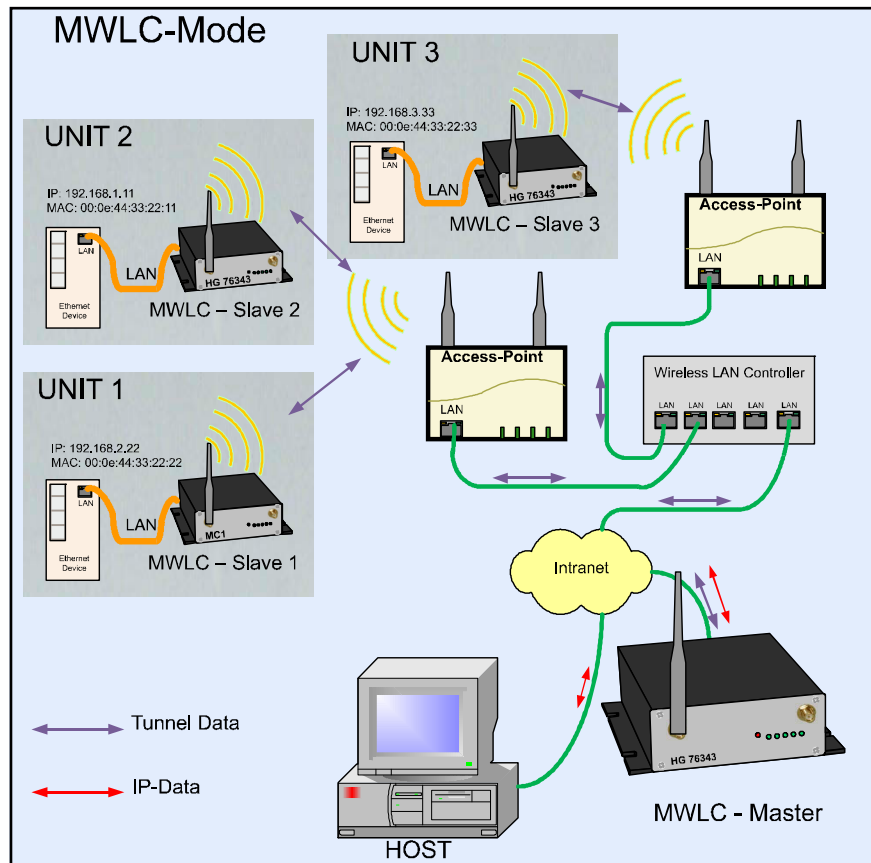
Disadvantages:

1. The HG G-76343/4/5 and all wireless clients work with their own IP addresses. These IP addresses must be within the same network.
2. Problems in some WLAN infrastructures with centralized controllers (no accessibility to the LAN clients from the WLAN side).

## 6.5 MWLC Mode

With the MWLC mode, all restrictions regarding the availability, IP address assignment and transparency especially in applications with multiple LAN clients are solved. In this mode all data packets received from the LAN clients are tunneled by the HG G-76343/4/5 (Slave) to another HG G-76343/4/5 (master) that is installed on stationary network side. The master HG G-76343/4/5 extracts the LAN client data packets and sends them into the stationary network. The HG G-76343/4/5 on the WLAN side is working in MWLC slave mode and the HG G-76343/4/5 on the stationary side is working in MWLC master mode.

**Figure 61** Bridge Modes: MWLC mode example configuration



In this mode it is irrelevant which IP addresses the clients have in relation to the HG G-76343/4/5, 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 the MWLC mode:

1. Maximum transparency of LAN client connections to the stationary network via WLAN..
2. No special configuration effort on the HG G-76343/4/5 no matter how many LAN clients are connected.

Disadvantage of the MWLC mode:

- ♦ One or two additional HG G-76343/4/5 are needed on the stationary network side.

### 6.5.1 MWLC Master

**Figure 62** Bridge Modes: MWLC Master

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.

The screenshot shows the 'Bridge mode configuration' page. At the top, there is a navigation bar with links: Home, Device, Configuration, Statistics, Support, and Logout. The page title is 'Bridge mode configuration'. Below the title, there are several settings:

- Bridge active:** A checkbox that is checked.
- Bridge mode:** A dropdown menu set to 'MWLC Master'.
- High Priority:** A checkbox that is unchecked.
- DHCP Server:** A section with the text 'DHCP server function is only available when Bridge mode is NAT or Single Client NAT.' and an 'Enable DHCP Server' checkbox that is checked.

Below each setting, there is a blue link: 'Do not disable the bridge except the wireless mode is 'accesspoint'', 'Enable high priority tunneling data.', and 'Check this box to enable the dhcp server configuration.' respectively.

### 6.5.2 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 HG G-76343/4/5, it is possible to define a second master (backup) to which the MWLC slave connects if the first master fails.

**Figure 63** Bridge Modes: MWLC Slave

**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.

The screenshot shows the 'Bridge mode configuration' page. At the top, there is a navigation bar with links: Home, Device, Configuration, Statistics, Support, and Logout. The page title is 'Bridge mode configuration'. Below the title, there are several settings:

- Bridge active:** A checkbox that is checked.
- Bridge mode:** A dropdown menu set to 'MWLC Slave'.
- Master IP:** A text input field containing '192.168.170.23'.
- Backup Master IP:** A text input field containing '192.168.170.24'.
- High Priority:** A checkbox that is checked.

Below each setting, there is a blue link: 'Do not disable the bridge except the wireless mode is 'accesspoint'', 'Enter master ip for MWLC-Mode.', 'Enter backup master ip for MWLC-Mode.', and 'Enable high priority tunneling data.' respectively.

## 7

## MQTT Client

With this function it is possible to control the radio modem internal interfaces (relay, serial) via the MQTT protocol. Furthermore you can also make settings on this page that make it possible to send status messages of the radio modem via MQTT.

Some of the parameters listed below can be given variables. The following variables are currently defined.

**Table 34** *MQTT Client: Variables*

Variable	Meaning
%dname	Device name (s. section 5.3.1 on page 50)
%wlanmac	MAC address of the WLAN interface
%SN	Serial number of the radio modem
%FW	Firmware version of the radio modem

Folgende Parameter lassen sich einstellen:

**Table 35** *MQTT Client: Parameter (part 1 of 2)*

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.. <table> <tr> <td>1) Unencrypted</td><td>Without encryption, if necessary with user + password</td></tr> <tr> <td>2) TLS Accept All</td><td>Encrypted without client authentication</td></tr> <tr> <td>3) Verify by Fingerprint ...</td><td>Encrypted: The server certificate is verified against the specified fingerprint.</td></tr> <tr> <td>4) Configured CA Cert</td><td>Encrypted: The uploaded client certificate is used for authentication.</td></tr> </table>	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.
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	<table> <tr> <td>1) disabled</td><td>Do not send status messages</td></tr> <tr> <td>2) API/Status Parts</td><td>Parts from the API/Status are sent in json format under the topic <i>Status Topic</i>. The content is determined by the paths defined under <i>Path 1...x</i> below.</td></tr> <tr> <td>3) Text</td><td>The text specified under Status Topic is sent as a status message.</td></tr> </table>	1) disabled	Do not send status messages	2) API/Status Parts	Parts from the API/Status are sent in json format under the topic <i>Status Topic</i> . The content is determined by the paths defined under <i>Path 1...x</i> below.	3) Text	The text specified under Status Topic is sent as a status message.		
1) disabled	Do not send status messages								
2) API/Status Parts	Parts from the API/Status are sent in json format under the topic <i>Status Topic</i> . The content is determined by the paths defined under <i>Path 1...x</i> below.								
3) Text	The text specified under Status Topic is sent as a status message.								
Status Interval	Time interval between status messages								

Table 35 MQTT Client: Parameter (part 2 of 2)

Parameter	Function
Path 1 ... x	<p>If <i>Status Topic Type = API/Status Parts</i> is set, parts of the API/Status to be sent are defined here</p> <p>Examples:</p> <p><code>\$.Device</code> → 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><code>\$.Device.FirmwareVersion</code> → returns:</p> <pre>{   "Device": {     "FirmwareVersion": "2.14h"   } }</pre> <p><code>\$.Wireless.Connection.SNR</code> → 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	<i>Last Will and Testament</i> : This topic is stored at the broker. The broker sends this topic with the content <i>LWT Data</i> if the client does not react within the <i>timeout</i> period (see above).
LWT Data	Last Will Text
Debug	Here you can specify a debug level with which information is written to the debug log file.



## 8

## Wireless (WLAN Interface)

In menu Wireless, all settings are made that define how the WLAN interface of the HG G-76343/4/5 device is to connect to the WLAN infrastructure on site. There are 4 sub menus with the following parameter groups that are described below:

**Table 36** *Wireless (WLAN Interface): Wireless sub menus*

Sub menu	Function
Main Parameter	Determination of physical parameters: Frequency band, transmission power, country setting, antenna configuration
SSID Profile 1	Here you define the WLAN network name to which the HG G-76343/4/5 should connect. This includes settings for the encryption used and the possibility of uploading certificates to the HG G-76343/4/5. If desired, you can create several such profiles. The number of these profiles is defined under <i>Main Parameters</i> .
SCEP	SCEP – Simple Certificate Enrollment Process: This function is only required if certificate-based authentication is defined in an SSID profile and you want the radio modem to automatically distribute or renew the certificates.
Roaming	Special settings that can support fast switching from one access point to another.

## 8.1 Main Parameter

**Figure 64** *Wireless (WLAN Interface): Wireless parameters*

**Wireless Mode:** To establish a WLAN connection with access points, *Infrastructure* is always set here.

**SSID-Profiles:** Number of different WLAN networks that should be configurable.

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

**Country selection:** Setting the country in which the HG G-76343/4/5 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 radio modem takes this parameter from the AP.

**Enable sleep mode:** This allows the energy consumption of the HG G-76343/4/5 to be reduced to a limited extent. Activating this function only makes sense for applications that have to work as energy-efficiently as possible.

The screenshot shows the 'Configuration' tab of the 'Wireless Para' section. The 'Enable Wireless Interface' checkbox is checked. 'Wireless Mode' is set to 'Infrastructure'. 'SSID Profiles' is set to '1'. 'Phy Mode' is set to '2.4+5GHz'. 'Country selection' is set to 'Germany'. 'Enable sleep mode' is unchecked. '802.11bg bitrate setting' and '802.11a bitrate setting' are both set to 'all bitrates'. 'Power selection' is set to 'Auto (MAX)'. 'Antenna gain' is set to '0'. 'Antenna selection' is set to 'Ant 1 + Ant 2'. There is a 'Filter SSID' checkbox at the bottom.



If this function is active, the data exchange via WLAN may be temporarily delayed.

**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.

**802.11a bitrate setting:** This controls the use of the minimum transmission bit rates in the 5 GHz band.

**Power selection:** With this parameter the transmitting power of the radio card in the radio modem can be reduced if necessary. This can be useful if only short distances to the APs have to be bridged and many other participants work in the frequency band.

**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 the value specified here, the WLAN driver reduces the transmission power to comply with the legal requirements depending on the country setting.

**Antenna selection:** If only one antenna connection of the HG G-76343/4/5 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.

**Filter SSID:** This setting affects the AP list displayed on the *Home* web page. If this option is active, only the APs 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.

## 8.2 Wireless Status Information Service

**Figure 65** *Wireless (WLAN Interface): Wireless Status Information Service*

This option allows the HG G-76343/4/5 to inform the status of the WLAN connection via the LAN interface to all connected devices or to a specific device.

**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:** The UDP port on which the receiving device expects data.

**Format:** Defines the content of the information to be sent.

**Example:** `SNR=%snr;APMAC=%bssid;Link=%wlstat` gives e.g.  
`SNR=34;APMAC=02:12:34:22:aa:33;Link=1`

The following values can currently be queried:

**Table 37** *Wireless (WLAN Interface): Variable formats (part 1 of 2)*

Parameter	Function
%wlstat	WLAN state: – 0 = not connected – 1 = connected
%txrate	Current transmission bit rate.
%ch	Currently used WLAN channel
%snr	SNR value = Signal-to-noise ratio value
%bssid	MAC address of the access point to which the radio modem is currently connected.
%apname	Name of the AP (not available for all APs)
%wlanip	IP address of the radio modem on the WLAN side
%wlanmac	MAC address of the radio modem on the WLAN side

**Table 37** *Wireless (WLAN Interface): Variable formats (part 2 of 2)*

Parameter	Function
%dname	device name of the radio modem
%SN	serial number of the radio modem
%FW	Firmware version of the radio modem
%Relay	Status of the on board relay

### 8.3 Wireless SSID Profile

With firmware 2.09 and higher it is possible to define several WLAN SSID profiles. This can be used to configure the radio modem to 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 parameter incl. User + Passwort)

The 802.1x certificates (Server + User) are valid for all profiles.

#### 8.3.1 SSID Profile



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.

**Table 38** *Wireless (WLAN Interface): SSID profile parameters*

Parameter	Value	Function
SSID	1-32 char.	This is the network name of the WLAN. This is specified by the AP (WLAN system) in the <i>Infrastructure</i> mode.
Priority	1 – 10	This value has only 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.

#### 8.3.2 Profile Change Action

This option is only relevant if the DHCP function is active. This is used to determine what must be done when the SSID profile is changed.

**Table 39** *Wireless (WLAN Interface): SSID profile change action*

Parameter	Value	Function
DHCP	Renew Rebind Restart	This setting determines how the radio modem behaves in relation to the active DHCP client when switching to this profile. <ul style="list-style-type: none"> <li>– With <i>Renew</i> or <i>Rebind</i> it is assumed that the same DHCP server is responsible for both profiles and the already assigned IP can still be used.</li> <li>– <i>Restart</i> restarts the DHCP procedure immediately to get a new IP address.</li> </ul>

### 8.3.3 Connect Action

This option is only relevant if the DHCP function is active. Here you can specify what should happen after the radio modem has connected to an Access Point.

**Table 40** *Wireless (WLAN Interface): SSID connect action*

Parameter	Value	Function
DHCP	No action Renew	<p>This setting determines what the DHCP client function of the radio modem should do when a connection to an Access Point has been successfully established. This action is then performed at each AP change.</p> <ul style="list-style-type: none"><li>– <i>No action</i> does nothing.</li><li>– <i>Renew</i> may be necessary for appropriately configured WLAN infrastructures, which then pass on data when a DHCP action has been performed.</li></ul>

### 8.3.4 Security Parameters

**Table 41** Wireless (WLAN Interface): Wireless Security Parameters (part 1 of 2)

Parameter	Note	Function																		
Encryption Mode		<p>Here, you specify which encryption method is to be used to communicate with the AP. In principle, the AP specifies which method is used on the WLAN network defined by <i>SSID</i>.</p> <p><b>Table 42</b> <i>Wireless (WLAN Interface): Encryption Mode</i></p> <table><tr><th>Mode</th><th>Function</th></tr><tr><td>no encryption</td><td>no encryption in use</td></tr><tr><td>WEP</td><td>64 or 128bit encryption using the RC4-algorithm</td></tr><tr><td>WPA</td><td>according to 802.11i</td></tr><tr><td>WPA2</td><td>according to 802.11i</td></tr><tr><td>WPA/WPA2</td><td>Automatic choice using what the AP is offering</td></tr><tr><td>WPA3</td><td>Only WPA3 allowed</td></tr><tr><td>WPA2/WPA3</td><td>WPA2 or WPA3 allowed</td></tr><tr><td>WPA/WPA2/WPA3</td><td>WPA, WPA2 or WPA3 encryption allowed</td></tr></table> <p><b>For WPA encryption, the WPA / WPA2(WPA3) (automatic selection) setting is recommended.</b></p>	Mode	Function	no encryption	no encryption in use	WEP	64 or 128bit encryption using the RC4-algorithm	WPA	according to 802.11i	WPA2	according to 802.11i	WPA/WPA2	Automatic choice using what the AP is offering	WPA3	Only WPA3 allowed	WPA2/WPA3	WPA2 or WPA3 allowed	WPA/WPA2/WPA3	WPA, WPA2 or WPA3 encryption allowed
Mode	Function																			
no encryption	no encryption in use																			
WEP	64 or 128bit encryption using the RC4-algorithm																			
WPA	according to 802.11i																			
WPA2	according to 802.11i																			
WPA/WPA2	Automatic choice using what the AP is offering																			
WPA3	Only WPA3 allowed																			
WPA2/WPA3	WPA2 or WPA3 allowed																			
WPA/WPA2/WPA3	WPA, WPA2 or WPA3 encryption allowed																			
Keying Protocol	only for WPA(2)	<p>Here, you can set which protocol is selected for key transmission with WPA. Only in exceptional cases, something other than <i>Auto</i> should be chosen.</p> <p><b>Table 43</b> <i>Wireless (WLAN Interface): Keying Protocol</i></p> <table><tr><th>Protocol</th><th>Note</th></tr><tr><td>TKIP</td><td></td></tr><tr><td>AES</td><td></td></tr><tr><td>Auto</td><td>The HG G-76343/4/5 prefers AES if the AP offers this method.</td></tr></table>	Protocol	Note	TKIP		AES		Auto	The HG G-76343/4/5 prefers AES if the AP offers this method.										
Protocol	Note																			
TKIP																				
AES																				
Auto	The HG G-76343/4/5 prefers AES if the AP offers this method.																			
Key	for WEP	Here the WEP key is specified as a 10 or 26 digit <b>hex value</b> . An example: If the WEP key consists of the <i>ABCDE</i> characters, the correct input is <i>4142434445</i> .																		
	for WPA	The <i>pass phrase</i> 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 long hex value is formed and stored as a key.																		

**Table 41** Wireless (WLAN Interface): Wireless Security Parameters (part 2 of 2)

Parameter	Note	Function
Key Index	nur bei WEP	Selection of the key index. Usually <i>WEP Key 1</i> is used.
Authentication	nur bei WEP	Select between <i>Open</i> and <i>Shared Key</i> Authentication. Usually <i>Open</i> is used.
Enable 802.11r	nur bei WPA	This switch can be used to activate a method that allows a quick changeover between the APs of the WLAN system. <b>This option may only be activated if the APs support this Fast Roaming function according to 802.11r and this option is activated in the AP for the SSID configured on the radio modem.</b>

### 8.3.4.1 EAP

**Table 44** Wireless (WLAN Interface): EAP Parameters

Parameter	Note	Function																									
Enable EAP		Authentication via 802.1x is activated here. The <i>Key</i> parameter under <i>Security Parameters</i> is then deactivated.																									
EAP-Type		<div>There are different EAP methods that can be selected here. Depending on the EAP method, a password has to be specified and, if necessary, certificates must also be installed.</div> <div>Table 45 Wireless (WLAN Interface): EAP Type</div> <table><tr><th>Type</th><th>User-name</th><th>Pass-word</th><th>Server-Cert.</th><th>Client-Cert. + Cert. Password</th></tr><tr><td>TLS</td><td>✓<sup>1</sup></td><td>✗</td><td>✓<sup>2</sup></td><td>✓</td></tr><tr><td>TTLS</td><td>✓</td><td>✓</td><td>✓<sup>2</sup></td><td>✓</td></tr><tr><td>PEAP</td><td>✓</td><td>✓</td><td>✓<sup>2</sup></td><td>✗</td></tr><tr><td>LEAP</td><td>✓</td><td>✓</td><td>✗</td><td>✗</td></tr></table> <div>✓<sup>1</sup> = The user usually does not necessarily have to be specified with TLS ✓<sup>2</sup> = The server certificate does not have to exist. In the sense of secure authentication, however, it is recommended to load a server certificate.</div>	Type	User-name	Pass-word	Server-Cert.	Client-Cert. + Cert. Password	TLS	✓ <sup>1</sup>	✗	✓ <sup>2</sup>	✓	TTLS	✓	✓	✓ <sup>2</sup>	✓	PEAP	✓	✓	✓ <sup>2</sup>	✗	LEAP	✓	✓	✗	✗
Type	User-name	Pass-word	Server-Cert.	Client-Cert. + Cert. Password																							
TLS	✓ <sup>1</sup>	✗	✓ <sup>2</sup>	✓																							
TTLS	✓	✓	✓ <sup>2</sup>	✓																							
PEAP	✓	✓	✓ <sup>2</sup>	✗																							
LEAP	✓	✓	✗	✗																							
Inner auth	only for TTLS and PEAP	This defines the protocol that is used during EAP authentication. <i>MSCHAPV2</i> is usually the correct setting here.																									
EAP Username	public	EAP username																									
EAP Username	private	EAP Username for the <i>inner</i> authentication. Only in special cases, this user name differs from the first entry.																									
EAP Password		EAP Password assigned in connection with the EAP username. This password is not required with the EAP type TLS.																									

### 8.3.4.2 Certificates

**Table 46** *Wireless (WLAN Interface): Certificates Parameter*

Parameter	Function
Certificate Password	With this password the HG G-76343/4/5 can access the elements of the client certificate.
Secure client key	Activating this option prevents the client certificate from being saved in the configuration file.

In the following, the user has the possibility to upload a client certificate and a total of four server certificates to the radio modem (*Upload*). Certificates which have already been uploaded can be deleted from the configuration with *Delete*.

## 8.4 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 service.

## 8.5 Wireless Roaming

In order to maintain the data connection in a mobile application or in an environment with changing reception conditions, the quality of the WLAN connection is continually checked and, if required, a connection to other, better-positioned access points (AP) is established.

For this the HG G-76343/4/5 must also scan for alternative APs on other channels in the specified frequency range. This short-term change of the channel impedes the ongoing data transmission. Therefore parameters are provided which make this scan procedure and the criteria for the change to another AP adjustable so that the data connection can be kept as stable as possible in accordance with the conditions of use.

### 8.5.1 Roaming Parameter

The roaming behavior of the radio modem is determined by the following parameters:

- The chosen frequency band (2.4 and/or 5 GHz)
- An SNR threshold that determines whether the HG G-76343/4/5 is looking for other APs in short or long time intervals.
- Specifies a (long) interval with which the radio modem scans the specified channels when the SNR value is *higher* than the specified threshold.
- Specify a (short) interval with which the radio modem scans the specified channels when the SNR value is *lower* than the specified threshold.
- Configure specific channels that the HG G-76343/4/5 is to scan.



### 8.5.1.1 AP Density

The SNR threshold value is set by the parameter *AP Density*. The following values are pre-/defined:

**Table 47** *Wireless (WLAN Interface): AP Density*

AP Density	SNR	Behavior
autodetect (default)	variable	With this setting, an algorithm is activated which varies the SNR threshold according to the found conditions. <b>This setting should be used in most cases.</b>
high	35	Depending on how <i>tight</i> the APs are mounted in the operating range of the HG G-76343/4/5, a specific threshold value can be set here.
medium	30	
low	25	
static client	20	If the radio modem is installed at a fixed location, the threshold can be set relatively low, thus avoiding unnecessary scan operations.
no roaming	0	If scanning is to be minimized or if there is only one suitable AP near the HG G-76343/4/5, the SNR value can also be set to 0 with this.
custom roaming	Para.	This allows the SNR value to be specified individually.

### 8.5.1.2 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 HG G-76343/4/5 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).

### 8.5.1.3 Min scan interval

This parameter is used to specify the time interval in seconds at which the HG G-76343/4/5 performs scans if the SNR value of the existing connection is *below* the SNR threshold. 3 seconds is the default value here.

### 8.5.1.4 Max scan interval

This parameter is used to specify the time interval in seconds at which the HG G-76343/4/5 performs scans if the SNR value of the existing connection is *above* the SNR threshold. 60 seconds is the default value here.

### 8.5.1.5 AP Scoring

The decision with which AP the HG G-76343/4/5 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.

### 8.5.1.6 Blacklist Timer

If the connection to an AP fails, this AP is initially locked for a certain time. This blocking time can be set with the parameter *Blacklist Timer*. The time is specified in seconds. A value of 0 means that the timer never expires and thus a connection to the APs in the list is possible only after a reset of the HG G-76343/4/5.

## 8.5.2 Background Scanning

The HG G-76343/4/5 supports this function starting with firmware 2.12r. If the WLAN system is configured accordingly, the IEEE **802.11k** standard offers WLAN clients the possibility of retrieving a list of their neighbor APs from the currently connected AP. The list contains the MAC addresses and the associated radio channels. This enables the WLAN client to scan more specifically for alternative APs.

**Table 48** *Wireless (WLAN Interface): Background Scanning*

Option	Function
Include advanced information	The radio modem uses the current AP list <b>and</b> the 802.11k list to select the channels on which to search for neighboring APs.
Only scan channels from neighbor information	The channels to be scanned are selected <b>only</b> from the 802.11k list.
Ignore neighbor information	The 802.11k list from the AP is <b>not</b> taken into account.

## 8.5.3 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.

## 8.5.4 Ping Test

**Figure 66** *Wireless (WLAN Interface): Enable Ping*

The ping test function is essentially an error detection function. If, during operation, and especially after a change of the AP (roaming), longer interruptions of the WLAN connection should occur, this fault can be documented in the debug log with this function. In this case it is also possible, by resetting and restarting the WLAN connection, to try to resolve the outage.

The parameters of this function are:

**Table 49** *Wireless (WLAN Interface): Ping Options*

Parameter	Value	Default	Function
Ping IP		192.168.170.100	destination IP address for the ping requests
Ping Intervall	1 - 3600	10	Interval in seconds with which the pings are sent
Wireless Reconnect		false	This option can be activated to automatically restart the WLAN connection after a certain number of ping responses fail.
Max. missing replies	1-60	10	Maximum number of successive failures before the wireless connection is restarted.

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.

### 8.5.5 Preferred / avoided access points

**Figure 67** *Wireless (WLAN Interface): Preferred/avoided access points*

Here you can define access points that should either preferred or avoided by the radio modem device when a roaming decision has to be made. **This option is only active when the AP Density parameter is set to autodetect.** The access points are identified with the MAC address of the BSSID.

The *Prefer* function makes sense if the radio modem always moves along a fixed course and in an environment with many APs. Then it may be advantageous if only certain APs should be used to run this course with as few roamings as possible.

The *Avoid* mode can be useful if access points are received good for some time, but are quickly hidden during movement. Putting these APs to the Avoid-List can lead to better roaming decisions.

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 HG G-76343/4/5 will still try to establish a connection.

*Strictly avoid* ensures that the radio modem does not connect to the listed APs even if no other suitable APs are available.

## 9

## Serial Interface

Most variants (see section 2.1 on page 10) of the HG G-76343/4/5 have a serial interface that can be controlled via (W)LAN.

## 9.1 Parameters of the Serial Interface



Altered settings, e.g. for the baudrate, need to match the settings of the devices that are connected to the serial port.

**Table 50** Serial Interface: Serial Port Parameters

Parameter	Default	Function												
Port active	off	De-/activation of the serial interface												
Device	/dev/ttymx0	Port address												
Baudrate and format	9600,8,n,1	Setting the baud rate, data bits, stop bits and parity handling												
Network configuration	TCP-Server, 8888	Sets the mode in which the serial interface can be controlled via the network. Further explanations are given in the section 9.2 on page 85												
Keep alive parameter		Parameters for the TCP server or TCP client mode to monitor the TCP connection. See section 9.3 on page 85												
Send trigger configuration	In order to avoid sending each individual serial-received character in a separate network pack, 3 criteria for collecting and sending the characters are defined. <b>Table 51</b> Criteria for sending of characters <table> <tr> <th>Parameter</th><th>Default</th><th>Function</th></tr> <tr> <td>Byte trigger</td><td>On : 16</td><td>Maximum number of characters to be collected.</td></tr> <tr> <td>Character timeout</td><td>On : 100</td><td>Definition of a maximum pause between 2 characters in milliseconds. If this time is exceeded, all characters collected up to then are sent.</td></tr> <tr> <td>Frame end trigger</td><td>Off : 0D</td><td>Definition of a character (as HEX value) which leads to the sending of the characters collected up to then.</td></tr> </table>		Parameter	Default	Function	Byte trigger	On : 16	Maximum number of characters to be collected.	Character timeout	On : 100	Definition of a maximum pause between 2 characters in milliseconds. If this time is exceeded, all characters collected up to then are sent.	Frame end trigger	Off : 0D	Definition of a character (as HEX value) which leads to the sending of the characters collected up to then.
Parameter	Default	Function												
Byte trigger	On : 16	Maximum number of characters to be collected.												
Character timeout	On : 100	Definition of a maximum pause between 2 characters in milliseconds. If this time is exceeded, all characters collected up to then are sent.												
Frame end trigger	Off : 0D	Definition of a character (as HEX value) which leads to the sending of the characters collected up to then.												
Handshake mode	Selection for the control of the handshake lines of the serial interface. See section 9.4 on page 85													

## 9.2 Network-Configuration Modes

Several modes are available for the use of the serial interfaces:

1. **TCP/IP-Server-Mode:**  
With this setting, the HG G-76343/4/5 opens a socket in the *Listen* mode and waits for a connection on a specific port (Local port). The HG G-76343/4/5 only keeps one connection at a time. In this mode, only the port number is specified as a parameter.
2. **TCP/IP-Client-Mode:**  
The HG G-76343/4/5 actively opens a TCP connection on the specified port of another network node. This network node can be another HG G-76343/4/5 or a computer that is waiting for a connection on the specified port. In addition to the port number (remote port), the IP address of the communication partner must be specified in this mode (Server IP).
3. **UDP/IP-Mode:**  
In the UDP mode, the HG G-76343/4/5 waits on the *local port* for data sent via UDP / IP. The serially received data are 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 remote port can be set to 0 . 0 . 0 . 0 or 0. In this case, the HG G-76343/4/5 inherits the sender IP + port information from the data packet initially arriving at the *local port*. The UDP mode should be used in cases where e.g. a separation of the communication partners occurs more frequently. However, it must be noted that the UDP protocol does not ensure the correct delivery of the data.
4. **Printerserver-Mode:**  
In print server mode, the HG G-76343/4/5 starts a TCP / IP socket in server mode that is waiting for connections on port 9100.

## 9.3 Keep Alive Settings

Once a TCP / IP connection is established, it remains until one of the communication partners closes the connection. If the connection between the HG G-76343/4/5 and the network communication partner is interrupted without the TCP / IP connection being closed before, the HG G-76343/4/5 may not reconnect.

The *keep alive* function transmits an *empty* data packet to the other at the time interval of *keep alive period*. If there is no response for the number of times defined with *keep alive probes*, the HG G-76343/4/5 resets the TCP socket and restarts the connection. Especially if the radio modem is working in the 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.

## 9.4 Handshake Mode Settings

This section defines how the readiness to transmit or receive data between the serial communication partners is handled. With the signals RTS, DTR, the HG G-76343/4/5 shows receive readiness. The signals CTS, DSR are input signals via which the connected serial device shows its readiness to receive.

The HG G-76343/4/5 can control the data flow remotely (remote) or autonomously (local). The user has the following modes to select from:

1. no Handshake:  
The signal CTS / DSR are not evaluated. Only RTS and DTR are set active when the serial interface is connected over the network.
2. XON / XOFF:  
The HG G-76343/4/5 sends and receives the flow control characters XON = 0x11 and XOFF = 0x13. The radio modem sends an XOFF character to the serial partner when the cache in the radio modem is almost full. When the cache is almost empty, the radio modem sends an XON character.
3. RTS/CTS:  
The HG G-76343/4/5 uses the RTS signal to show that it is ready to receive. The HG G-76343/4/5 evaluates the signal CTS to determine the readiness of the serial partner.
4. DTR/DSR:  
The HG G-76343/4/5 uses the DTR signal to show that it is ready to receive. The HG G-76343/4/5 evaluates the signal DSR to determine the readiness of the serial partner.
5. Remote:  
In this mode the HG G-76343/4/5 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 has to make further configurations 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 active		i = RI inactive

To control the output signal lines RTS and DTR, the following characters are sent to the HG G-76343/4/5 via the network:

D = Set DTR active		d = set DTR inactive
R = Set RTS active		r = set RTS inactive
6. RS422 / RS485:  
These are *special* modes, that **must be set if** the serial interface is equipped with a special **RS422 / RS485 interface IC**. In this case, the RTS line is used to do the send and receive switching. Therefore it is possible to define the activation of the transmit driver before and after sending data.

## 9.5 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 radio modem. If there are problems with data exchange on the serial interface, an exact error analysis can be carried out in cooperation with our service.

If necessary, ask our service for the exact procedure.

## 10

## Debug / Logging

The radio modem offers the following possibilities to record data and events:

1. Store system messages in RAM, FLASH or USB memory and show them under Statistics -> SystemLog (s. 5.4.1 on page 56) and make them available for download. The download can also be carried out with the MC-Config program.
2. Send system messages to a syslog server.
3. Trace the data traffic on the WLAN and/or the LAN interface. The recorded trace files can be transferred to the computer via the home page (at the bottom of that page) or via the MC-Config-Program.

### 10.1 Record System Messages

**Figure 68** Debug / Logging: Debug Log page

The possibilities described here to record system messages or traces of the data traffic are only intended to investigate occurring problems and, if necessary, to show how these problems can be solved. **In normal operation, all settings described here should be reset to the default values.** Likewise, the log files that are still present on the device should be deleted by the function Statistics -> SystemLog -> Reset System Log.

It is possible to adjust the *intensity* of the logging parameters so that specific modules of the radio modem operating system generate detailed messages in the form of formatted text lines and store them in a file. For example, if there are problems with the use of the serial interface, this program part can be specifically configured to record very precisely the occurring events. It is recommended to configure a time server (NTP, s. section 5.3.7 on page 55) to store the messages with a time stamp so that they can be better attributed to a problem.



In general, the system messages are not intended for the user to determine the cause of the fault by means of a defined error list. The DebugLog file should be sent to our service for verification. The possible system messages thus are not defined and commented in detail below.

### 10.1.1 Setting the Debug File Destination

**Figure 69** *Debug / Logging: Log file destination*

Possible targets are:

**Table 52** *Debug / Logging: Log file destinations*

Choice	Target	Note
RAM	internal RAM of the radio modem	The messages are getting lost after a power down or a reset
Internal FLASH	internal FLASH memory of the radio modem	After a power down or a reset, the following messages are written to the end of an already existing debug file. The maximum size of the file is 16 MB.
USB	External USB-FLASH memory	In this mode, a new numbered debug file is created after each reset. The file names are <i>DebugLog0.dat</i> , <i>DebugLog1.dat</i> and so on. The size of the combined files is only limited by the capacity of the USB memory.

### 10.1.2 Set Additional Debug Information

In addition to the actual message text, you can specify additional information for each message.

**Figure 70** *Debug / Logging: Debug Information*

**Table 53** *Debug / Logging: Debug Information (part 1 of 2)*

No.	Information	Note
1	Absolute Timestamp	Time format: "Hour: Minute: Second.micro second" If no timestamp has been received over the network (NTP), the time elapsed since the system start is specified here.
2	Relative Timestamp	Time as a counter of the milliseconds elapsed since the start.
3	Repeat Counter	Counter which indicates how many times this message has been issued since the system start.
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, which generated this message.



**Table 53** *Debug / Logging: Debug Information (part 2 of 2)*

No.	Information	Note
6	Class	There are classes: <ul style="list-style-type: none"> <li>– ERROR</li> <li>– WARN</li> <li>– INFO</li> <li>– TRACE</li> </ul> that are active according to the debug settings (Default, Detailed, Maximum).
7	Message	The actual message content
	Log Separator	With this parameter you can define which separator should be set between the individual elements of an output line. For example, if you want to insert the log file in an Excel list, you can take one of these characters as separator: <ul style="list-style-type: none"> <li>– Space (used in the following example)</li> <li>– Comma</li> <li>– Pipe</li> <li>– Tab</li> </ul>

Example of an output line:

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

Elements of the output line (for the numbers see Table 53 above):

**Table 54** *Debug / Logging: Elements of a Debug Log output line*

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

### 10.1.3 Syslog Server

**Figure 71** *Debug / Logging: Syslog Server*

These messages can also be sent to a Syslog server. The IP address of this server has to be defined for this. 0.0.0.0 means that this function is not active.



In order 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.

## 10.2 Traffic Dump Configuration (Recording of Data Traffic from the LAN or WLAN Interface)

This function allows data traffic to be recorded on the LAN and/or WLAN interface. The files generated thereby can later be analyzed with other programs, e.g. Wireshark®.

**Figure 72** Debug / Logging: Traffic Dump Configuration

**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.

**Table 55** Debug / Logging: Traffic Dump Configuration (part 1 of 2)

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 <ul style="list-style-type: none"> <li>– <i>Internal Flash</i>: Internal flash memory (approx. 400 MByte)</li> <li>– <i>USB</i>: External USB-Memory (depending on capacity of the memory stick)</li> </ul>
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 <i>Custom</i> self-defined filter. To do this, however, you should familiarize yourself with the filter format of the pcap module. The options are: <ul style="list-style-type: none"> <li>– no Filter</li> <li>– only own traffic</li> <li>– Custom</li> </ul>

**Table 55** Debug / Logging: Traffic Dump Configuration (part 2 of 2)

Parameter	Function	
	Dump Control	With <i>Dump Control</i> you can specify what happens when the memory limit of the internal flash or the USB memory is reached. <ul style="list-style-type: none"> <li>– The recording is stopped.</li> <li>– The oldest recording is deleted and the recording continues with a new file.</li> </ul>
	Filesize <sup>*)</sup>	If the recordings are stored in the USB memory, you can set the maximum size of the file here: <ul style="list-style-type: none"> <li>– Small = 8 MByte</li> <li>– Medium = 32 MByte (Default)</li> <li>– Large = 128 MByte</li> </ul>
Dump LAN	This activates the recording of data packets on the LAN side.	
	Monitor Dump Destination	see above at Dump Wireless
	Dump Control	see above at Dump Wireless
	Filesize <sup>*)</sup>	see above at Dump Wireless
<sup>*)</sup> = (is only displayed if Monitor Dump Destination = USB)		

If the current recording file reaches the defined filesize (s Table 55 on page 90 above) it is closed and a new file is started. The stored file is then compressed and written as \*.gz file in the file system, the original file is then deleted. Depending on the data compression rate, data traffic can be logged over a long period of time.

The compressed files can then be downloaded from the Home web page of the radio modem. The list of dump files is located at the end of the Home page below the list of access points. The structure of the file names is explained in Table 56 on page 93.

**Figure 73** Debug / Logging: Wireless Dump / Ethernet Dump file list

Wireless Dump		
Capture byte count	2666376KByte	
Recv count	16462248	
Drop count	24634/12616 (If 0)	
Recent Dumpfiles	<a href="#">391002_WLAndump_0140_20000101_073944_843916.pcap.gz</a> (21687 KByte)	
Recent Dumpfiles	<a href="#">391002_WLAndump_0141_20000101_074048_360020.pcap.gz</a> (18244 KByte)	
Recent Dumpfiles	<a href="#">391002_WLAndump_0142_20000101_074233_462674.pcap.gz</a> (21912 KByte)	
Recent Dumpfiles	<a href="#">391002_WLAndump_0143_20000101_074310_600030.pcap.gz</a> (16050 KByte)	
Recent Dumpfiles	<a href="#">391002_WLAndump_0144_20000101_074604_862172.pcap.gz</a> (19922 KByte)	
Recent Dumpfiles	<a href="#">391002_WLAndump_0145_20000101_074731_698195.pcap.gz</a> (19984 KByte)	
Recent Dumpfiles	<a href="#">391002_WLAndump_0146_20000101_074851_473225.pcap</a> (26937 KByte)	
Ethernet Dump		
Capture byte count	89640KByte	
Recv count	79175	
Drop count	0/0 (If 0)	
Recent Dumpfiles	<a href="#">391002_EthernetDump_0000_20000101_074003_654321.pcap.gz</a> (16143 KByte)	
Recent Dumpfiles	<a href="#">391002_EthernetDump_0001_20000101_074251_645069.pcap.gz</a> (16549 KByte)	
Recent Dumpfiles	<a href="#">391002_EthernetDump_0002_20000101_074643_559405.pcap</a> (23742 KByte)	

Additional information is given as to how many bytes and data packets are stored in the current dump. Also there is information about the number of data packets that have been discarded (drop count). The file names can be clicked to start a download.

## NOTICE

### Excessive stress for the FLASH memory

This type of recording on the interfaces places a heavy load on the FLASH memory.

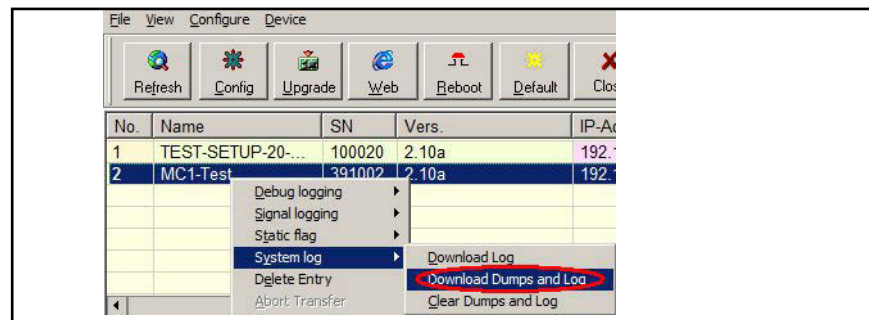
- ▶ Only activate the interface logging for problem diagnosis.
- ▶ Deactivate interface logging in production use.

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

### 10.3 Downloading Debug Files with the MC-Config Program

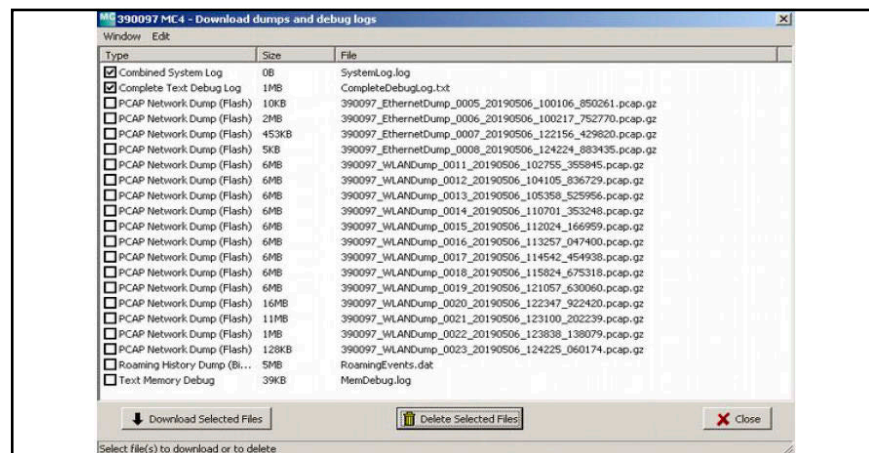
In order to download all log files in one go from the radio modem, you can select the following command in the MC-Config program via the context menu (right-click radio modem in the list) as follows:

**Figure 74** Debug / Logging: MC-Config Download Dumps and Log



Starting with the radio modem firmware 2.10b and the MC-Config version 2.0.2.32, a dialog is opened to define the folder in which the files are saved. Then a dialog opens, where you can select the log and dump files for downloading. Before opening this dialog, all active dump processes are stopped. The existing pcap files are compressed. This process may take some time. The progress is displayed in the *Status* column of the MC-Config Program. The following dialog is then displayed:

**Figure 75** Debug / Logging: MC-Config: Download Dumps and Debug Logs



This selection always shows the file *SystemLog.log* which contains many information about the current status of the radio modem with the last system messages and the current configuration data. **This file is always important when it comes to the analysis of error situations.**

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

The dump files are listed in the order they were written. First the LAN dump files then the WLAN dump files. If a time server (see 5.3.7 on page 55) could be used, the file names of the dump files, the date and the time of the start time appear. This is very helpful, in that if you know the time of an error, you can determine the dump files which could have documented this error more accurately.

The file name consists of the following parts:

**Table 56** *Debug / Logging: Structure of the file names of the downloaded dump files*

Section	Function	Note
nnnnn_	Serial-No. of the radio modem	
WLAN/Ethernet Dump		
_xxxx_	Number of the file	This is important if no time server is set up and the HG G-76343/4/5 is restarted in between.
_YYYYMMDD_	date of the recording	Without time server, the clock will start at 01.01.2000
_hhmmss_uuuuu	Start time	Hour-minute-second-microsecond. Without time server, the clock will start at 00.00.00_000000

From this list you can select one or more files and either download or delete them. Both log and dump files are shown in the list, which are stored in the internal flash as well as in a possibly installed USB memory stick. Files on the USB stick are marked with (USB).

## 10.4 Debug Configurations

This is used to define the *intensity* of the system messages for the various program sections. The program embeds messages that are marked with a specific debug level. The following debug levels are defined:

**Table 57** *Debug / Logging: Debug Levels*

Level	Function
ERROR	Occurrence of an error that prevents a desired function.
WARN	Occurrence of a condition that delays a desired function.
INFO	A message that documents an event that occurs.
TRACE	A message that documents the progress of a function.

Individual debugging levels can be set for the following program sections:

**Figure 76** *Debug / Logging: Syslog Server*

**Debug Configurations**

Debug Wireless:  [Select log configuration for wireless.](#)

WPA Supplicant details:  [Select detail level of WPA supplicant. Only increase this if connection can't be established \(Reboot needed\).](#)

Debug DHCP:  [Select log configuration for DHCP.](#)

Debug Serial:  [Select log configuration for serial ports.](#)

Debug Relay:  [Select log configuration for the relay port.](#)

Debug Aux-Input:  [Select log configuration for the auxin port.](#)

Debug Base System:  [Select log configuration for base system.](#)

Debug Network Bridge:  [Select log configuration for network bridge.](#)

**Table 58** *Debug / Logging: Individual Debug Levels*

Module	Function
Wireless	Reports events related to the WLAN interface. The emphasis is on the recording of the access points and on the roaming procedures.
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 for triggering the relay
Aux-Input	Messages generated by the module for controlling the digital input (not relevant for Götting devices)
Base System	Messages that the general operating system generates
Network Bridge	Messages generated by the bridge module.

The individual program parts have the following 4 debug levels.

## NOTICE

### Reduced System Performance

The *Maximum* level may generate such a large number of debug messages that the performance of the primary application suffers.

- Only activate this level for the program module which likely has a problem and only for as long as you are debugging.

**Table 59** *Debug / Logging: Intensity of the Debug messages*

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

## 11

## Configuration with USB Memory Stick

Starting with firmware version 2.12a there are two possibilities to use a USB stick to configure the radio modem:

1. Transfer of a configuration file from the USB stick to the radio modem during a *default reset* initiated by the reset button.
2. Permanently inserted *Config-USB-Stick* on which both the configuration and the firmware for a radio modem is stored.

### 11.1 Transfer of a configuration file during a default reset

If a *default reset* is performed via the reset button, the radio modem 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 exists, this configuration will be applied to the radio modem after the restart.

### 11.2 Application for the Config-USB-Stick

It is possible to prepare USB memory sticks in such a way that they are recognized by the radio modem as *USB-Config-Sticks* during the boot process. On the USB-Config-Stick there is a config file with a complete setup and if necessary also a file with a specific firmware for the radio modem.

The goal is to be able to quickly replace a defective HG G-76343/4/5 with a different HG G-76343/4/5 by simply plugging the USB Config Stick from the defective radio modem into the replacement device. The replacement radio modem checks during the boot process whether there is a firmware file on the stick, and whether it differs from the firmware in the replacement radio modem.

If so, the firmware from the stick is first transferred to the replacement radio modem and flashed. After the reboot, the config file of the USB Config-Stick is used for further operation. The replacement radio modem will work with the same firmware and the same configuration as the original HG G-76343/4/5.

#### 11.2.1 Initializing a Config-USB-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.

`InitUsbConfigStick` (case sensitive!)

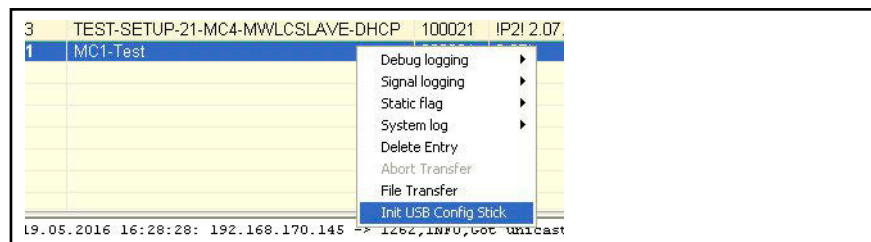


In order to start MC-Config with this parameter you can generate a shortcut to the *MCConfig.exe* file. In the properties of this shortcut the parameter can be added to the target like so: `c:\...\MCConfig.exe InitUsbConfigStick`

When started this way the additional selection *Init USB Config Stick* appears in the context menu of MC-Config.



Figure 77 USB-Config-Stick: MC-Config Init with USB Stick Config



## NOTICE

### Possible Dataloss

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

- Make sure there is no data that is still needed before initializing the USB stick.

This command **formats** 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 radio modem. After transferring the files, the radio modem 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 HG G-76343/4/5. This ensures that a change of the configuration takes place in the Config-Stick as well as a change of the HG G-76343/4/5 firmware is also stored on the USB stick. Thus, another HG G-76343/4/5 that is started with this Config-Stick will have the same function as the radio modem from which the Config-Stick was removed.



If the USB stick is removed, the radio modem makes a reset very soon. The following boot process is stopped until a Config USB memory stick is detected. Until then the radio modem remains blocked! This state is signaled with a blue flicker of the power LED.

If you want to use the HG G-76343/4/5 again without a Config-USB memory stick, you have to reset the radio modem via the Reset button to its *Factory Default* (s. 3.5 on page 17).

## 12

## REST-API

## 12.1 Functions and Command Lines

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

1. Download of the active config file
2. Download of the default config file
3. Upload of a config file
4. Upload of a firmware file
5. Status request (also s. section 12.2 on page 99)
6. Certificate upload
7. Download of a list of available WLAN+LAN recordings ((W)LAN dump files)
8. Download of single WLAN+LAN recordings
9. Download of the systemlog file
10. Download of the CA certificate from the OpenVPN server
11. Download of a configuration file for an OpenVPN client

**Table 60** REST-API: Functions and Parameters (part 1 of 2)

Function	URL	Method	Result
Download the active config file	http(s)://<radio_modem_IP>/API/Cfg/GetRunning	GET	Text
Download the default config file	http(s)://<radio_modem_IP>/API/Cfg/GetDefault	GET	Text
Upload of a config file	http(s)://<radio_modem_IP>/API/Cfg/Set	POST	
Upload of a firm-ware file	http(s)://<radio_modem_IP>/API/Firmware/Upgrade	POST	
Status request (also s. section 12.2 on page 99)	http(s)://<radio_modem_IP>/API/Status	GET	JSON
Upload a certificate	http(s)://<radio_modem_IP>/API/Cfg/ImportCertificate	POST	
Download the file list of the existing WLAN+LAN recordings	http(s)://<radio_modem_IP>/API/Debug/CaptureFiles	GET	JSON
Download a file	http(s)://<radio_modem_IP>/API/Debug/CaptureFile/<FileName>	GET	Binary

**Table 60** REST-API: Functions and Parameters (part 2 of 2)

Function	URL	Method	Result
Download the systemlog file	<code>http(s)://&lt;radio_modem_IP&gt;/API/Debug/Get/System-Log</code>	GET	Text
Download the CA certificate from the VPN server	<code>http(s)://&lt;radio_modem_IP&gt;/API/OpenVPNServer/Get-CACert</code>	GET	Text
Download of the configuration file for the VPN client	<code>http(s)://&lt;radio_modem_IP&gt;/API/OpenVPNServer/Get-ClientConfig</code>	GET	Text

## 12.2 Outputs for the Status Function

The query `http(s)://<radio_modem_IP>/API/Status` currently provides information that is divided into the following segments:

**Table 61** REST-API: Categories of the status query

Segment	Info	Elements
Device	Device information	Serial number, Firmware version, Uptime, Linux Vers, WLAN hardware
Network	Infos about the LAN-Port(s)	Link-Status (up / down) ....
CertInfo	(if available) Information on the loaded certificates	Validity period, certificate info, ...
Wireless	WLAN interface	Access point list, status of the WLAN connection, Infos about the WLAN radio channels
Input	AUX-IN digital input	Status, Mode, ...
Relay	Relay interface	Status (ON-OFF), Mode
Serial	Serial interface	Mode, Format, Status, RX-Tx-Statistics
MQTT	MQTT clients	When activated

These status values can also be called up individually by addressing exactly the desired element:

**Example** `http(s)://<radio_modem_IP>/API/Status/Network/LAN/Port/0/State`  
Link status LAN-Port 1, provides the info up or down

**Example** `http(s)://<radio_modem_IP>/API/Status/Wireless/Connection/Connected`  
provides the info true or false

In general, the Status function provides various details in JSON format. Most of the information is self-explanatory. Below is a sample status output that shows the JSON format used.

**Figure 78** Example of REST API status output (IP and Mac addresses set to 0)

```

{
  "Device": {
    "Uptime": "0 Week(s) 0 Day(s) 00:01:35",
    "UptimeSec": 95,
    "SerNum": 301132,
    "DeviceName": "HG7634X",
    "UtcTime": "10.08.2023 7:20:13",
    "UtcTimeTS": 1691652013,
    "FirmwareVersion": "2.14n",
    "KernelVersion": "Linux version 5.4.249",
    "BuildRoot": {
      "GitRevision": "7814dbce15",
      "Version": "2023.05.1"
    },
    "Wireless": {
      "Device": "WLAN Atheros AR9382",
      "Type": "IEEE802.11an"
    }
  },
  "Relay": {
    "State": false,
    "Enabled": false
  },
  "Wireless": {
    "Accesspoints": [
      {
        "BSSID": "00:00:00:00:00:00",
        "SNR": 53,
        "Noise": -93,
        "RSSI": -40,
        "APName": "",
        "SSID": "- hidden -",
        "Channel": 11,
        "LastSeen": 2,
        "ScansSinceLastSeen": 0,
        "LastScanFinished": 0,
        "RoamSuccessCount": 0,
        "RoamTimeoutCount": 0
      },
      {
        "BSSID": "00:00:00:00:00:00",
        "SNR": 47,
        "Noise": -93,
        "RSSI": -46,
        "APName": "",
        "SSID": "GastZugang",
        "Channel": 11,
        "LastSeen": 2,
        "ScansSinceLastSeen": 0,
        "LastScanFinished": 0,
        "RoamSuccessCount": 0,
        "RoamTimeoutCount": 0
      }
    ],
    (...)
  },
  "Connection": {
    "BSSID": "00:00:00:00:00:00",
    "SSID": "",
    "Duration": 0,
    "Channel": 0,
    "Frequency": 0,
    "SNR": 0,
    "RSSI": 0,
    "Noise": 0,
    "TxRate": 0,
    "Enabled": true,

```

```

        "Connected": false,
        "ConnectionType": "",
        "Client-IP": "0.0.0.0",
        "Client-Netmask": "255.255.255.0",
        "Client-Gateway": "0.0.0.0",
        "Client-DNS": "",
        "Client-Hostname": "HG7634X"
    },
    "Channel": [
        {
            "Frequency": 2412,
            "Channel": 1,
            "Noise": -94,
            "LastScanned": 0
        },
        {
            "Frequency": 2417,
            "Channel": 2,
            "Noise": -95,
            "LastScanned": 0
        }
    ],
    (...)
    ],
    },
    "Network": {
        "LAN": {
            "PortCount": 1,
            "Port": [
                {
                    "State": "Up",
                    "Speed": 1000,
                    "Duplex": true,
                    "Cross": false
                }
            ]
        },
        "Tunnel": {
            "IPSec": {
                "VirtualIP": "0.0.0.0",
                "ServerIP": "0.0.0.0",
                "TunnelRTT": 0,
                "RoutingPath": [
                    {
                        "Interface": "wlan0",
                        "InterfaceText": "Wireless LAN",
                        "Score": 0,
                        "RTT": 3000,
                        "RTTAvg": 3000
                    },
                    {
                        "Interface": "wwan0",
                        "InterfaceText": "Mobile Network",
                        "Score": 0,
                        "RTT": 3000,
                        "RTTAvg": 3000
                    },
                    {
                        "Interface": "eth0",
                        "InterfaceText": "Wired LAN",
                        "Score": 0,
                        "RTT": 3000,
                        "RTTAvg": 3000
                    }
                ]
            }
        }
    }
}

```

```
}

```

## 12.3 REST API Queries with curl

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:

**Table 62** REST-API: curl command lines

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

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

```
[Wireless]
```

```
Enabled=false
```

is transmitted, the radio modem 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/>

## 13

## Technical Data

## 13.1 Hardware

Table 63 Technical Data Hardware

Hardware		
Interfaces	Ethernet	1, 2 or 4 x LAN Port 10/100/1000 MBit/s Auto MDI/MDIX
	Serial	1 x RS232 (not for HG G-76345), 300-460,8 KBit/s, RTS, CTS, DSR, DTR, RI, DCD or RS485 (RS422)
	USB	1 x USB 2.0 for firmware updates or the logging of system messages on USB memory media or for the connection of other interfaces with USB adapters
	Relay	1 x switch over, max 1A@24 V, max 125 VAC
Antenna connectors	Ant 1	RP-SMA (optional TNC or RP-TNC)
	Ant 2	
Indicators	4 LEDs	<ul style="list-style-type: none"> <li>– Power</li> <li>– WLAN (wireless)</li> <li>– LAN</li> <li>– SER (Serial)</li> </ul>
Power supply	Connector	Hirschmann M12 5-pol. plug connector (screwable)
	Voltage range	10 – 60 VDC or 802.3af PoE via LAN Port 1
	Energy consumption	<= 5W (3W typisch)
Temperature range		0 - 60° C
Dimensions	Casing	Standard: 124 x 105 x 34 mm
	Weight	approx. 400g

## 13.2 WLAN Interface

**Table 64** Technical Data WLAN Interface

WLAN Interface		
Technology	802.11 a/b/g/n WLAN (2.4 + 5 GHz Band)	
Antennas	2 Antennas (2T2R MIMO)	
Encryption	WEP (64, 128bit) + TKIP/AES	
Security	802.11i WPA(2 + 3) – PSK 802.1x EAP-PEAP, -TLS, -TTLS, -LEAP	
Channels	<ul style="list-style-type: none"> <li>802.11b/g/n ETSI 1-13, USA/Canada 1-11</li> <li>802.11a/n ETSI 19 + 5, USA/Canada 25 (U-NII-1 + UNII-2A + U-NII-2C + U-NII-3)</li> </ul>	
Data rates	Mode	Data rates
	802.11b	1, 2, 5.5, 11 Mbps
	802.11a/g	6, 9, 12, 18, 24, 36, 48, 54 Mbps
	802.11n	MCS0-7
	802.11n (20MHz)	<ul style="list-style-type: none"> <li>NSS=1: max. 72.2Mbps</li> <li>NSS=2: max. 144.4Mbps</li> </ul>
	802.11n (40MHz)	<ul style="list-style-type: none"> <li>NSS=1: max. 150Mbps</li> <li>NSS=2: max. 300Mbps</li> </ul>

## 13.3 Output Power & Sensitivity

**Table 65** Technical Data – Output Power & Sensitivity 802.11b

802.11b		
Data Rate	Tx ± 2dBm	Rx Sensitivity
11Mbps	18dBm	≤ -91dBm

**Table 66** Technical Data – Output Power & Sensitivity 802.11a

802.11a		
Data Rate	Tx ± 2dBm	Rx Sensitivity
54Mbps	13dBm	≤ -65dBm

**Table 67** Technical Data – Output Power & Sensitivity 802.11g

802.11g		
Data Rate	Tx ± 2dBm	Rx Sensitivity
54Mbps	15dBm	≤ -75dBm

**Table 68** Technical Data – Output Power & Sensitivity 802.11n / 2,4 GHz

802.11n / 2,4 GHz				
Bandwidth	Data Rate	Tx ± 2dBm (1TX)	Tx ± 2dBm (2TX)	Rx Sensitivity
HT20	MCS7	14dBm	17dBm	≤ -71dBm
HT40	MCS7	14dBm	17dBm	≤ -69dBm



**Table 69** *Technical Data – Output Power & Sensitivity 802.11n / 5 GHz*

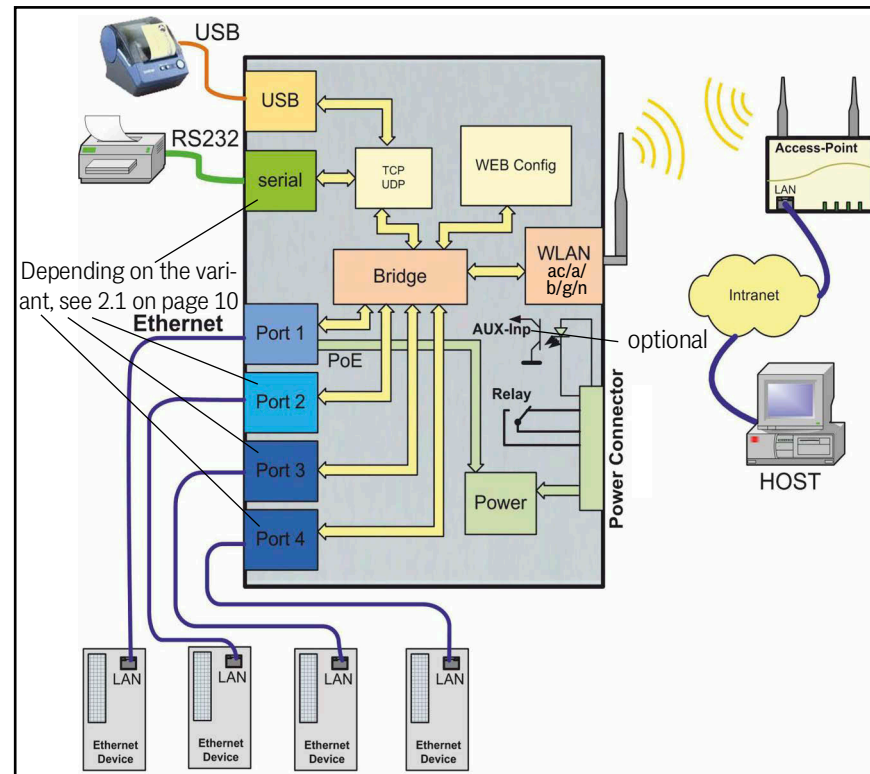
802.11n / 5 GHz				
Bandwidth	Data Rate	Tx ± 2dBm (1TX)	Tx ± 2dBm (2TX)	Rx Sensitivity
HT20	MCS7	12.5dBm	15.5dBm	≤ -74dBm
HT40	MCS7	12.5dBm	15.5dBm	≤ -71dBm

## 14

## HG G-76343/4/5-A ac (802.11ac)

Of all variants (see variant overview in section 2.1 on page 10), there is a version ac available that supports the 802.11ac standard in addition to 802.11a/b/g/n. This version is basically functionally identical to the variants described up to this point, but has additional technical specifications. This chapter describes the differences.

**Figure 79** Application example HG G-76342/4/5-A ac



## 14.1 Technical Data HG G-76342/4/5-A ac

All the technical data listed in chapter 13 on page 103 apply to the ac variant. In addition, this variant has the following features.

### 14.1.1 WLAN Interface

All values from Table 64 on page 104 apply. In addition, the following values apply:

**Table 70** Technical Data HG G-76342/4/5-A ac – WLAN Interface

WLAN Interface 802.11ac		
Technology	802.11 a/b/g/n/ac WLAN (2.4 + 5 GHz Band)	
Channels	802.11a/n/ac ETSI 19 + 5, USA/Canada 25 (U-NII-1 + UNII-2A + U-NII-2C + U-NII-3)	
Daten rates	802.11ac	MCS0-9
	802.11ac (20MHz)	– NSS=1: max. 86Mbps – NSS=2: max. 173Mbps
	802.11ac (40MHz)	– NSS=1: max. 180Mbps – NSS=2: max. 360Mbps
	802.11ac (80MHz)	– NSS=1: max. 433Mbps – NSS=2: max. 866Mbps

### 14.1.2 Output Power and Sensitivity

All values from section 13.3 on page 104 apply. In addition, the following values apply:

**Table 71** Technical Data HG G-76342/4/5-A ac – Output Power and Sensitivity

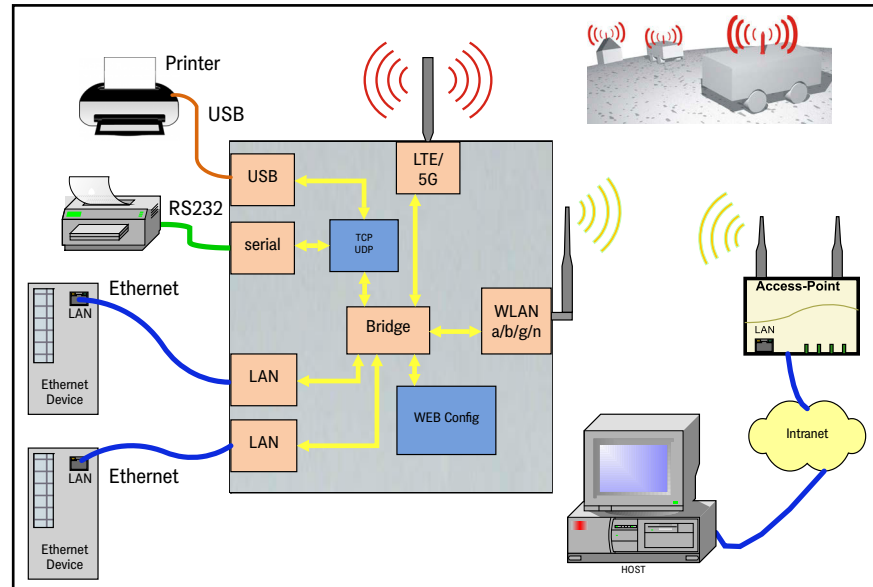
802.11ac				
Bandwidth	Data rate	Tx ± 2dBm (1TX)	Tx ± 2dBm (2TX)	Rx Sensitivity
VHT80	MCS9	10dBm	13dBm	≤ -63dBm

## 15

## HG G-76344XA/ZA 4G LTE 5G

There are versions of the HG G-76344-A variant (see variant overview in section 2.1 on page 10) that have mobile radio interfaces in addition to the WLAN interface and can be operated as an LTE router. These are basically functionally identical to the variants described up to this point, but have additional functions. This chapter describes the differences.

**Figure 80** Application example HG G-76344-A LTE



## 15.1 Variants HG G-76344-A LTE

**Table 72** Variants of the radio modem with mobile radio interface

Variant / Order No.		Mounting (s. section 3.1 on page 15)	Mobile radio interface (s. Table 73 on page 109)
HG G-76344	XA LTE	Top hat rail mounting on narrow side	Public LTE
	XA LTE-P		Private LTE
	XA LTE-5G		5G
HG G-76344	ZA LTE	Flange casing	Public LTE
	ZA LTE-P		Private LTE
	ZA LTE-5G		5G

## 15.2 Connectors

The connections on the back of the device correspond to the version without LTE shown in section 2.3.3 on page 12. The front of the device has the following interfaces, depending on the LTE version.

**Figure 81** Front panel connections of the HG G-76344-A LTE variants



## 15.3 Mobile Radio Interface

The available mobile radio interfaces (see Table 72 on page 108) provide the following functions.

**Table 73** Functions of the mobile radio interfaces HG G-76344-A LTE

Mobile radio interface	
Type	Specification
LTE	<ul style="list-style-type: none"> <li>Public LTE, 3GPP Release 11</li> <li>Cat 4, up to 150 Mbps downlink and 50 Mbps uplink</li> <li>1x antenna SMA</li> <li>Connects to 2G, 3G or 4G networks worldwide</li> </ul>
LTE-P	All the features of LTE, plus: <ul style="list-style-type: none"> <li>Private LTE, non public network, e.g. band 43</li> <li>2x antenna SMA, thereof optionally 1x GNSS</li> </ul>
LTE-5G	All the features of LTE-P, plus: <ul style="list-style-type: none"> <li>3GPP Release 15 NSA/SA operation, Sub-6 GHz</li> <li>3x antenna SMA, thereof optionally 1x GNSS</li> <li>Cat 16 downlink, up to 2,5 Gbps</li> <li>Cat 18 uplink, up to 900 Mbps</li> <li>Connects to 5G networks worldwide</li> </ul>

## 15.4 Use as an LTE Router

Just as the device communicates via WLAN, it can also be used via a public mobile network or via a private campus network. However, while the device cannot be addressed directly from the Internet in the public mobile network, since the IP address dynamically assigned by the provider cannot usually be reached from outside, such a function can very well be used in a private campus network. For this reason, the mobile device usually initiates a connection to the server.

The mobile radio module adds an extended input mask in addition to the standard setting options of the HG G-76344, in which the mobile radio specific parameters can be entered (see section 15.8 on page 113).

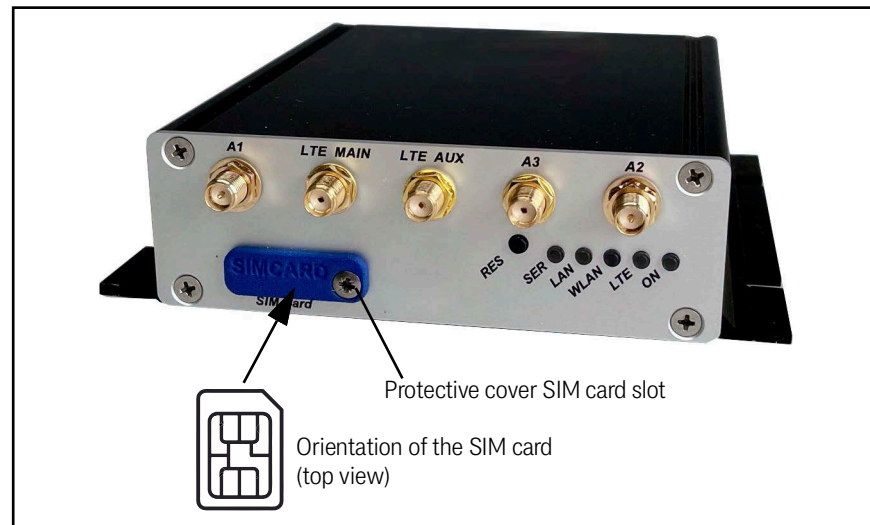
To be able to use the mobile radio interface:

- ✓ Connect suitable LTE/5G antennas for the frequency range used to the corresponding connectors on the front panel (see Figure 81 on page 109): 2 x WLAN (R-SMA), 2 x LTE or 3 x 5G (SMA).
- ✓ Insert a suitable SIM card (see following section).

## 15.5 How to Insert the SIM Card

- ✓ **Mini-SIM cards (2FF, 25 mm x 15 mm)** fit into the SIM card slot. The slot is under a protective cover.

**Figure 82** Position of the SIM card slot (in the picture HG G-76344ZA LTE-5G)



### Inserting the SIM card:

- ▶ Remove the protective cover of the SIM card slot.
- ▶ Carefully insert the SIM card completely into the slot on the front. The orientation of the SIM card is as shown above with the contacts facing up and the beveled corner on the front right.
- ▶ The SIM card must click into place.
- ▶ Replace the protective cover.  
The SIM card is inserted.

### Removing the SIM card:

- ▶ Remove the protective cover of the SIM card slot.
- ▶ Apply light pressure to the SIM card. This releases the internal lock, whereupon the card is pushed slightly out of the slot.
- ▶ Pull the SIM card out.
- ▶ Replace the protective cover.  
The SIM card is removed.

## 15.6 LTE LED

**Figure 83** Position of the LTE LED (in the picture HG G-76344ZA LTE-5G)



**Table 74** Functions of the LTE LED

Display	Function
Off	LTE is currently off
Blue/off flashing	Waiting for the LTE card to be detected until the AT interface responds.
White/off flashing	Initial initialization
Greenn/off (1:1 ratio)	Searching for provider, waiting for registration at the base station.
Green/off (1:3 ratio)	Logon to the base station OK. Wait for successful data dial-up (User+Password+APN).
Short green/blue changes	The PIN is being transferred to the SIM card.
Permanent green/blue change	PIN incorrect.
White/red change	PIN attempts are exhausted. The PUK is requested on the configuration web page.
Yellow/blue change	No SIM was detected in the slot
Permanent green	Internet connection is established.
Red flashing pattern in connected state	For 2G - 4G every 10 seconds during established internet connection: <ul style="list-style-type: none"> <li>– 1 x for 2G (GSM)</li> <li>– 2 x for 3G (UMTS)</li> <li>– 3 x for 3.5G (HSDPA)</li> <li>– 4 x for 4G (LTE)</li> </ul>
Blue flashing in connected state	For 5G/NSA: Blue flashes in addition to permanent green when 5G is present in the base station.
Permanent green + blue Note: This condition looks like a light blue.	<ul style="list-style-type: none"> <li>– For 5G/NSA: When 5G is used.</li> <li>– For 5G/SA</li> </ul>

## 15.7 Additional outputs in the web interface

In the LTE version, the following additional sections are output on the information page in the web interface (see 5.1 on page 38).

**Figure 84** LTE information in the web interface

Wireless LAN / LTE Gateway	
Home Device Configuration Statistics Support	
<b>System Information</b>	
Device Name	VPH_1
Uptime	0 Week(s) 0 Day(s) 00:06:15
Realtime clock (UTC)	11.02.2022 14:16:24
Realtime clock (Local Time)	11.02.2022 15:16:24
Serial number	317913
Firmware Version	2.12x
Kernel Version	Linux version 4.9.290
<b>Mobile Radio Status</b>	
Registration Status	registered, roaming
ICCID	8988280660010526400
IMSI	901405101052640
Base Station Area Code	FFFE
Base Station Cell ID	2432604
Base Station Signal	-71dBm
Reference signal received quality	15 (AT-Command-Result)
Reference signal received power	37 (AT-Command-Result)
Mobile Radio Standard	LTE
Provider	26201
Available Providers	(1,"Telekom.de","TDG","26201",7),(1,"Vodafone.de","Vodafone","26202",7),(1,"o2 - de","o2 - de","26203",7),(0,1,2,3,4),(0,1,2)
LTE Card Status	Ready
Internet Connection Status	Connected to Internet
IP	100.120.96.1
Traffic	Tx: 7 Pkt 1459 B Rx: 6 Pkt 1412 B
<b>Wireless Status Information</b>	
Operation Mode	Disabled
<b>Wired LAN Status Information</b>	
eth0 IEEE_rx_crc	2
LAN Switch Port 1	Link: Up Speed: 1000Mbit/s Duplex: Full MDI-X: Straight
LAN Switch Port 2	Link: down
<b>Network Information</b>	
Interface Mobile (IPv4)	IP 100.120.96.1 (DHCP successful) - Netmask 255.255.255.252 default gw 100.120.96.2
Interface LAN (IPv4)	IP 10.10.10.201 (Static IP) Broadcast 10.10.10.255 Netmask 255.255.255.0 MAC 90:5F:8D:04:D9:D9 default gw 10.10.10.201
Routing	Default gateway 100.120.96.2 on Mobile

### 15.7.1 Mobile Radio Status

**Table 75** LTE mobile radio status info in the web interface

Info	Meaning
Registration Status	Mobile network login status
ICCID	SIM card identification number
IMSI	Mobile radio subscriber identification
Base Station Area Code	Information about the rough location of the mobile subscriber
Base Station Cell ID	Information about the cell of the mobile subscriber
RSSI	Reception signal strength
RSRQ	Information about the received signal (modem-specific)
RSRP	Information about the received signal (modem-specific)
Mobile Radio Standard	Standard currently used
Provider	Selected provider
Available Providers	Available providers
LTE Card Status	Status of the radio module
Internet Connection Status	Logical connection status
IP	Assigned WAN IP address
Traffic	Packets and bytes sent and received so far



## 15.7.2 Network Information

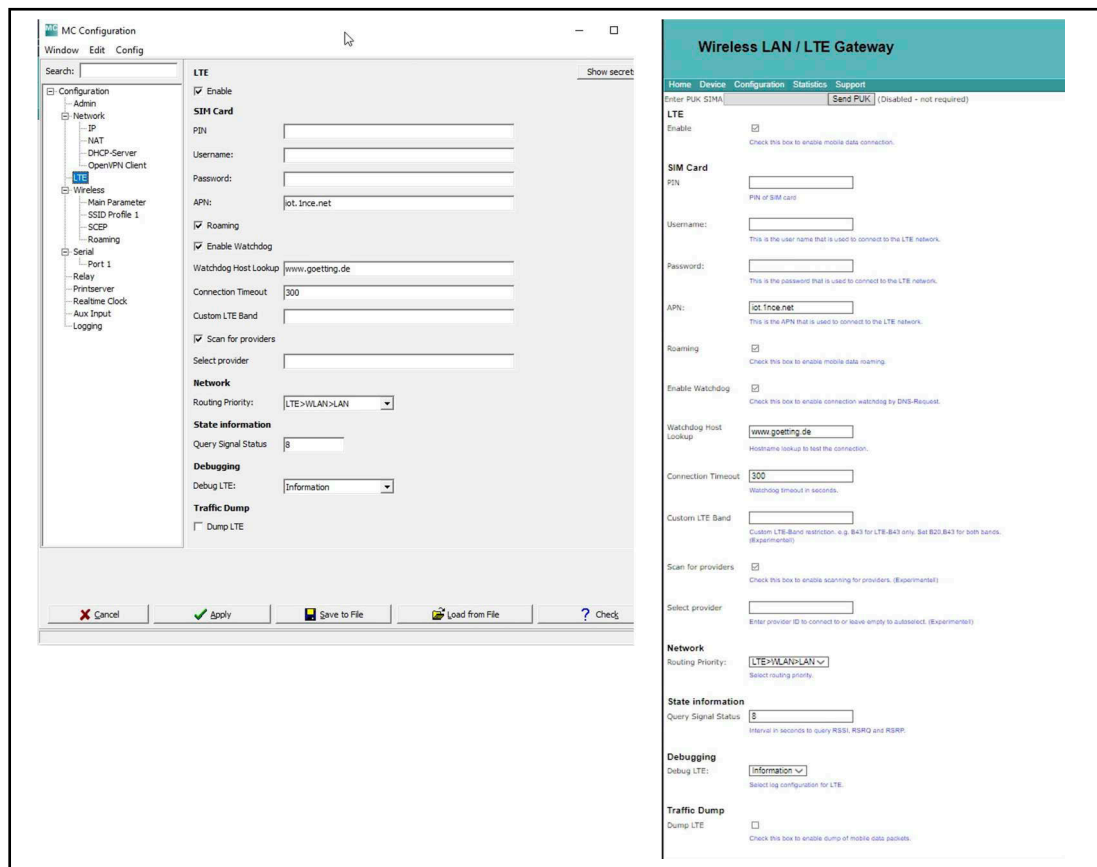
**Table 76** LTE Network Information in the web interface

Info	Meaning
Interface Mobile (IPv4)	IP-address, net mask and GW of the mobile interface
Interface LAN (IPv4)	IP address, net mask and GW of the LAN interface
Routing	Gateway address of the mobile radio interface

## 15.8 Input of the Parameters for the Cellular Connection

In the LTE version, both the MC-Config tool (see chapter 4 on page 18) and the web interface (see chapter 5 on page 38) allow you to set the mobile radio parameters.

**Figure 85** Input of the mobile radio parameters via MC-Config (left) or the web interface (right)



**Table 77** Parameters of the mobile connection (part 1 of 2)

Option	Meaning
LTE	Must be enabled to activate the LTE interface.
SIM Card	Enter the parameters of the SIM card here if required.
APN	The access point name is entered under APN. You get this name from the mobile network provider or from the configuration of the private campus network, then e.g. "intranet".

Table 77 Parameters of the mobile connection (part 2 of 2)

Option	Meaning
Custom-LTE Band	For private campus networks, a Custom LTE Band must be specified, e.g. for the frequency range 3.7-3.8 GHz B43 for 4G or n78 for 5G. For 5G/NSA, a 4G and a 5G band must be specified. Hover the mouse over the input field, then an info about the input format appears.
Scan for providers	Search for all available providers
Select provider	A specific provider can be entered here
Watchdog Host Lookup	In the <i>Watchdog Host Lookup</i> field, enter the address of any computer to which address resolution is to be performed via DNS lookup, if required. The cycle time can be entered in seconds in the Connection Timeout field and only becomes active if no data is transferred within this period. The system uses this function to determine whether an LTE or 5G connection is still available.
Network Routing priority	Selection of the routing priority
State Information	Time interval in seconds, in which the status information is read out from the radio module.
Debugging	Setting the debug level (see also 10 on page 87)
Traffic Dump	Logging the LTE data traffic (see also chapter 10 on page 87)

## 15.9 REST-API

Additional information is also output via the REST-API (see chapter 12 on page 98) for the LTE version.

Table 78 REST-API: LTE status (part 1 of 2)

LTE Status			
1	2	3	Value (example)
Device	Mobile	Device	Quectel RM500Q
		Type	5G-SA 5G-NSA 3GPP Rel.15 LTE
Modem	ICCID-SIM0		
	IMSI-SIM		
	IMEI		863305040170440
	Firmware		11.5
	Enabled		true
	Connected		false
	MobileRadioStandard		
	WAN-IP		
	CurrentProvider		
	LastDialTime		00:00:00

**Table 78** *REST-API: LTE status (part 2 of 2)*

LTE Status			
1	2	3	Value (example)
	Duration		0
	RSSI		0
	BER		0
	RSRQ		0
	RSRP		0
	SentBytes		0
	ReceivedBytes		0
	TotalSentBytes		0
	TotalReceivedBytes		0
	ConnectionCounter		0
	ResetCounter		482
	Error		No
	Warning		No

## 15.10 Technical Data

In addition to the technical data of the hardware and the WLAN interface mentioned in chapter 13 on page 103, the following technical data applies to the LTE version.

**Table 79** *Technical Data Mobile radio interface*

Mobile radio interface	
LTE/LTE-P	
Technology	LTE Cat 4, 3GPP Release 11
Antennas	1x SMA (LTE) / 2x SMA (LTE-P), thereof optionally 1x GNSS
Speed	Downlink: up to 150 Mbps Uplink: up to 50 Mbps
GNSS	GPS, GLONASS, BeiDou, Galileo, QZSS
Certificates	<ul style="list-style-type: none"> <li>Carrier: Vodafone/Deutsche Telekom/SKT/Telefónica</li> <li>Regulatory: GCF/CE/KC/NCC/RCM/FAC/NBTC/ICASA</li> <li>Others: WHQL</li> </ul>
5G	
Technology	5G NR, 3GPP Release 15 NSA/SA operation, Sub-6 GHz
Antennas	3x SMA, thereof optionally 1x GNSS
Speed	Downlink CAT 16: up to 2,5 Gbps Uplink Cat 18: up to 900 Mbps
GNSS	GPS, GLONASS, BeiDou (Compass), Galileo
Certificates	<ul style="list-style-type: none"> <li>Regulatory: GCF/CE/SRRC/CCC/NAL/KC/RCM</li> <li>Others: RoHS/WHQL</li> </ul>

## 16

---

## Open Source Compliance Information

---

Product: WLAN radio modems HG G-76343 / HG G-76344 / HG G-76345 / HG G-76346

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, email or fax to the following addresses:

**Götting KG**

Celler Str. 5

D-31275 Lehrte

Germany

Fax +49 (0) 5136-8096-80

E-Mail [opensource@goetting-agv.com](mailto:opensource@goetting-agv.com)

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 THE COSTS OF A DATA CARRIER AND THE POSTAL CHARGES TO SEND THE DATA CARRIER TO YOU. THE AMOUNT DEPENDS ON YOUR LOCATION. WE WILL ASK YOU TO APPROVE THE COSTS BEFORE WE SEND A DATA CARRIER. 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:



---

<https://www.goetting-agv.com/opensource>

---

## 17

## Statements and instructions according to FCC and Industry Canada Rules

### 17.1 Information for host integrators of the radio module

**CAUTION:** Host integrators are 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.

#### 17.1.1 Labelling 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 following 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.

#### 17.1.2 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.

#### 17.1.3 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.

### 17.2 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 be operated in 5.15 – 5.25 GHz frequency range, then it is restricted to indoor environments 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.

## 18

## List of Figures

Figure 1	Complete system (example).....	9
Figure 2	All variants: Connectors and indicators on the front panel .....	11
Figure 3	Connectors HG G-76343ZA.....	11
Figure 4	Connectors HG G-76344ZA.....	12
Figure 5	Connectors HG G-76345ZA.....	12
Figure 6	Pin assignment 5 pin. M12 socket power & relay .....	12
Figure 7	LEDs .....	13
Figure 8	Dimensions casing type XA .....	15
Figure 9	Dimensions casing type YA .....	15
Figure 10	Dimensions casing type ZA .....	16
Figure 11	MC-Config Program: Setup for the initial operation of a WLAN client .....	19
Figure 12	Initial commissioning with the MC-Config Program .....	19
Figure 13	MC-Config Program: User Interface .....	20
Figure 14	MC-Config Program: Operating elements .....	20
Figure 15	MC-Config Program: List view items .....	21
Figure 16	MC-Config Program: List view items .....	24
Figure 17	MC-Config Program: List context menu items .....	25
Figure 18	MC-Config Program: File Menu .....	26
Figure 19	MC-Config Program: View Menu .....	27
Figure 20	MC-Config Program: Configure Menu .....	27
Figure 21	MC-Config Program: Device Menu .....	31
Figure 22	MC-Config Program: Config dialog.....	32
Figure 23	MC-Config Program: Enter username and password.....	33
Figure 24	MC-Config Program: Dialogs while downloading the Config from multiple devices.....	34
Figure 25	MC-Config Program: IP Ranges.....	35
Figure 26	MC-Config Program: IP search range .....	35
Figure 27	MC-Config Program: Configuration of the logging details.....	36
Figure 28	MC-Config Program: Recording debug messages.....	37
Figure 29	MC-Config Program: Download dumps and log.....	37
Figure 30	Web interface: System information .....	38
Figure 31	Web interface: Wireless status information .....	39
Figure 32	Web interface: Wired LAN Status Information .....	42
Figure 33	Web interface: Serial1 Status Information.....	43
Figure 34	Web interface: Access point list .....	44
Figure 35	Web interface: USB Storage Status Information .....	45
Figure 36	Wireless Dump / Ethernet Dump file list .....	46
Figure 37	Web interface: Firmware upload dialog.....	47
Figure 38	Web interface: Configuration management .....	47
Figure 39	Web Interface: Network Test .....	48

Figure 40	Web interface: Admin page .....	50
Figure 41	Web Interface: Admin → URL Authentication .....	51
Figure 42	Web interface: Network > IP settings .....	52
Figure 43	Web interface: Network > Gateway Settings .....	52
Figure 44	Web interface: Network > IPV6 Settings .....	52
Figure 45	Web interface: Network > mDNS Settings .....	53
Figure 46	Web interface: Printer server configuration .....	54
Figure 47	Web interface: Example for a System Log output .....	56
Figure 48	Web interface: Example for a Statistics Network output .....	57
Figure 49	Bridge Modes: Bridge OFF .....	59
Figure 50	Bridge Modes: Bridge OFF > Gateway Settings .....	59
Figure 51	Bridge Modes: LAN Client Cloning parameters 1 .....	60
Figure 52	Bridge Modes: LAN Client Cloning parameters 2 .....	61
Figure 53	Bridge Modes: Example for LAN Client Cloning .....	62
Figure 54	Bridge Modes: NAT mode (example configuration) .....	62
Figure 55	Bridge Modes: Single Client NAT Mode .....	63
Figure 56	Bridge Modes: Forwarding rules for NAT .....	64
Figure 57	Bridge Modes: DHCP server settings .....	65
Figure 58	Bridge Modes: Static DHCP server entries .....	65
Figure 59	Bridge Modes: Level 2 bridge example configuration .....	67
Figure 60	Bridge Modes: Level 2 Pseudo Bridge Mode .....	67
Figure 61	Bridge Modes: MWLC mode example configuration .....	69
Figure 62	Bridge Modes: MWLC Master .....	70
Figure 63	Bridge Modes: MWLC Slave .....	70
Figure 64	Wireless (WLAN Interface): Wireless parameters .....	74
Figure 65	Wireless (WLAN Interface): Wireless Status Information Service .....	75
Figure 66	Wireless (WLAN Interface): Enable Ping .....	82
Figure 67	Wireless (WLAN Interface): Preferred/avoided access points .....	83
Figure 68	Debug / Logging: Debug Log page .....	87
Figure 69	Debug / Logging: Log file destination .....	88
Figure 70	Debug / Logging: Debug Information .....	88
Figure 71	Debug / Logging: Syslog Server .....	89
Figure 72	Debug / Logging: Traffic Dump Configuration .....	90
Figure 73	Debug / Logging: Wireless Dump / Ethernet Dump file list .....	91
Figure 74	Debug / Logging: MC-Config Download Dumps and Log .....	92
Figure 75	Debug / Logging: MC-Config: Download Dumps and Debug Logs .....	92
Figure 76	Debug / Logging: Syslog Server .....	94
Figure 77	USB-Config-Stick: MC-Config Init with USB Stick Config .....	97
Figure 78	Example of REST API status output (IP and Mac addresses set to 0) .....	100
Figure 79	Application example HG G-76342/4/5-A ac .....	106
Figure 80	Application example HG G-76344-A LTE .....	108
Figure 81	Front panel connections of the HG G-76344-A LTE variants .....	109
Figure 82	Position of the SIM card slot (in the picture HG G-76344ZA LTE-5G) .....	110
Figure 83	Position of the LTE LED (in the picture HG G-76344ZA LTE-5G) .....	111
Figure 84	LTE information in the web interface .....	112



Figure 85	Input of the mobile radio parameters via MC-Config (left) or the web interface (right) .....	113
-----------	--	-----

## 19

## List of Tables

Table 1	Hazard classification according to ANSI Z535.6-2006 .....	7
Table 2	Variants of the radio modem .....	10
Table 3	Pin assignment 9 pin Sub-D socket .....	13
Table 4	Functions of the LEDs .....	13
Table 5	MC-Config Program: Operating elements .....	20
Table 6	MC-Config Program: Information in the list view .....	21
Table 7	Color Coding Connection Type IP Address .....	22
Table 8	MC-Config Program: Logging settings .....	24
Table 9	MC-Config Program: List context menu items .....	25
Table 10	MC-Config Program: Functions of the view menu .....	27
Table 11	MC-Config Program: Functions of the configure menu .....	27
Table 12	MC-Config Program: Key shortcuts .....	28
Table 13	MC-Config Program: Device Polling .....	29
Table 14	MC-Config Program: Pretest .....	30
Table 15	MC-Config Program: Functions of the Device menu .....	31
Table 16	MC-Config Program: Buttons of the Config dialog .....	33
Table 17	Web interface: System Information .....	38
Table 18	Web interface: Wireless Status Information .....	39
Table 19	Web interface: Possible messages connection state .....	40
Table 20	Web interface: Display for active encryption .....	40
Table 21	Web interface: SNR Quality of the reception signal .....	41
Table 24	Web interface: Operating modes relay .....	42
Table 22	Web interface: Wired LAN Status Information .....	42
Table 23	Web interface: Relay Status Information / IO-Info (Optional) .....	42
Table 25	Web interface: Serial1 .....	43
Table 26	Web interface: Network Information .....	44
Table 27	Web interface: Configuration Management .....	47
Table 28	Web Interface: Network Test .....	48
Table 29	Web interface: configuration menus .....	49
Table 31	Web Interface: Relay Modes .....	54
Table 30	Web interface: Onboard Relay .....	54
Table 32	Web interface: Realtime Clock .....	56
Table 33	Bridge Modes .....	58
Table 34	MQTT Client: Variables .....	71
Table 35	MQTT Client: Parameter .....	71
Table 36	Wireless (WLAN Interface): Wireless sub menus .....	73
Table 37	Wireless (WLAN Interface): Variable formats .....	75
Table 38	Wireless (WLAN Interface): SSID profile parameters .....	76
Table 39	Wireless (WLAN Interface): SSID profile change action .....	76
Table 40	Wireless (WLAN Interface): SSID connect action .....	77

Table 42	Wireless (WLAN Interface): Encryption Mode.....	78
Table 43	Wireless (WLAN Interface): Keying Protocol.....	78
Table 41	Wireless (WLAN Interface): Wireless Security Parameters .....	78
Table 45	Wireless (WLAN Interface): EAP Type .....	79
Table 44	Wireless (WLAN Interface): EAP Parameters .....	79
Table 46	Wireless (WLAN Interface): Certificates Parameter.....	80
Table 47	Wireless (WLAN Interface): AP Density.....	81
Table 48	Wireless (WLAN Interface): Background Scanning .....	82
Table 49	Wireless (WLAN Interface): Ping Options.....	83
Table 51	Criteria for sending of characters .....	84
Table 50	Serial Interface: Serial Port Parameters .....	84
Table 52	Debug / Logging: Log file destinations.....	88
Table 53	Debug / Logging: Debug Information .....	88
Table 54	Debug / Logging: Elements of a Debug Log output line .....	89
Table 55	Debug / Logging: Traffic Dump Configuration .....	90
Table 56	Debug / Logging: Structure of the file names of the downloaded dump files.....	93
Table 57	Debug / Logging: Debug Levels.....	93
Table 58	Debug / Logging: Individual Debug Levels .....	94
Table 59	Debug / Logging: Intensity of the Debug messages .....	95
Table 60	REST-API: Functions and Parameters.....	98
Table 61	REST-API: Categories of the status query.....	99
Table 62	REST-API: curl command lines .....	102
Table 63	Technical Data Hardware .....	103
Table 64	Technical Data WLAN Interface .....	104
Table 65	Technical Data – Output Power & Sensitivity 802.11b.....	104
Table 66	Technical Data – Output Power & Sensitivity 802.11a.....	104
Table 67	Technical Data – Output Power & Sensitivity 802.11g.....	104
Table 68	Technical Data – Output Power & Sensitivity 802.11n / 2,4 GHz .....	104
Table 69	Technical Data – Output Power & Sensitivity 802.11n / 5 GHz.....	105
Table 70	Technical Data HG G-76342/4/5-A ac – WLAN Interface .....	107
Table 71	Technical Data HG G-76342/4/5-A ac – Output Power and Sensitivity.....	107
Table 72	Variants of the radio modem with mobile radio interface.....	108
Table 73	Functions of the mobile radio interfaces HG G-76344-A LTE .....	109
Table 74	Functions of the LTE LED .....	111
Table 75	LTE mobile radio status info in the web interface.....	112
Table 76	LTE Network Information in the web interface .....	113
Table 77	Parameters of the mobile connection .....	113
Table 78	REST-API: LTE status.....	114
Table 79	Technical Data Mobile radio interface.....	115
Table 80	Document changelog .....	128

## 20

## Index

## Numbers

2G .....	109
3G .....	109
3GPP .....	109
4G .....	108, 109
5 pin M12 Socket .....	12
5G .....	108, 109
802.11ac .....	106
9 pin Sub-D Socket Serial .....	13

## A

Access Points .....	44
Antenna gain .....	74
AP .....	44

## B

Bridge Modes .....	58
Bridge Type .....	44
DHCP Server Settings .....	65
Forwarding rules for NAT .....	64
LAN Client Cloning .....	58
Level 2 Bridge .....	58, 67
MWLC Master .....	70
MWLC Slave .....	70
MWLC-Mode .....	58, 69
NAT .....	58, 62
Single Client NAT .....	58, 62
Static DHCP Server entries .....	65

## C

Casing .....	15
Certificates .....	80
Channel Usage .....	41
Commissioning .....	15
Company names .....	129
Config-USB-Stick .....	96
Connectors .....	11
Copyright .....	129
curl .....	102

## D

Debug .....	87
Additional Information .....	88
Configurations .....	93
Downloading Files .....	92
Ethernet Dump .....	46, 91
File Destination .....	88
MC-Config Program .....	92
Wireless Dump .....	46, 91
Declaration of Conformity .....	8
default reset .....	96

## E

EAP .....	79
EU Declaration of Conformity .....	8
Exclusion of Liability .....	129
EXT4 .....	46

## F

Factory Settings .....	17
FCC .....	117
format .....	46

## G

gain .....	74
GNSS .....	109

## H

Hazard classification .....	7
-----------------------------	---

## I

IEEE 802.11 .....	82
Indicators .....	11
Industry Canada Rules .....	117
Interfaces .....	10
internal interfaces .....	66
IP Address .....	52
IP Ranges .....	34

## L

LEDs .....	13
Level 2 Pseudo-Bridge .....	44
LLMNR .....	53
Logging .....	87
Record System Messages .....	87
Recording of Data Traffic (LAN or WLAN) .....	90
Traffic Dump Configuration .....	90
LTE .....	108
connections .....	109
LED .....	111
mobile radio parameters .....	113
Mobile Radio Status .....	112
Network Information .....	113
Private .....	109
Public .....	109
REST-API .....	114
Router .....	108, 109
technical data .....	115
Variants .....	108
web interface .....	112
LTE Router .....	109
LTE-5G .....	109
LTE-P .....	109

**M**

MC-Config .....	18
Config Function .....	32
Context Menu .....	25
Debug Messages .....	36
Firmware-Updates .....	34
List View Items .....	21
Logging .....	37
Logging of Messages .....	24
Logging Parameters .....	36
Menus .....	26
Operating Elements .....	20
Operation .....	20
Startup .....	19
User Interface .....	20
mDNS .....	53
Mini-SIM .....	110
mobile radio interfaces .....	109
Mounting .....	15
MQTT .....	53, 54, 71

**N**

Noise .....	41
-------------	----

**O**

Onboard Relay .....	54
Output Power .....	104

**P**

Pin Assignments .....	12
Ping .....	82
ports .....	66
Power .....	12
Power Save .....	51
Private LTE .....	109
Public LTE .....	109

**R**

radio modem .....	9
Relay .....	12
Reset .....	17
REST-API .....	98
Status .....	99

**S**

Securing Passwords .....	51
Security Parameters .....	78
Sensitivity .....	104
Serial Interface .....	84
Handshake Mode Settings .....	85
Keep Alive Settings .....	85
Network-Configuration Modes .....	85
Parameters .....	84
TCP/IP-Client-Mode .....	85
TCP/IP-Server-Mode .....	85
Signal .....	41
Signal-to-Noise-Ratio .....	41
SIM .....	
Mini .....	110
SNR .....	41

Startup .....	16
Symbols .....	8
system example .....	9

**T**

Technical Data .....	103
WLAN Interface .....	104
trade marks .....	129

**U**

UDP/IP-Mode .....	85
URL Authentication .....	51
USB Memory Stick .....	96
Config-USB-Stick .....	96
EXT4 .....	46
format .....	46

**V**

Variants .....	10
Versions .....	10

**W**

Warning Notices .....	7
Web Interface .....	38
Access Point Information .....	44
Admin Menu .....	50
Bridge .....	53
Configuration .....	49
Configuration Management .....	47
Device Menu .....	46
Firmware-Upload .....	47
Home .....	38
IO-Info .....	42
IP settings .....	52
IPv6 Settings .....	52
Logging .....	56
mDNS Settings .....	53
Network Information .....	44
Network Menu .....	52
Parameters of WLAN Interface .....	53
Printer Server .....	53
Realtime Clock .....	55
Relay .....	54
Relay Status Information .....	42
Serial Port .....	53
Serial1 .....	43
Statistics .....	56
Support .....	57
System Information .....	38
System Log .....	56
Wired LAN Status Information .....	42
Wireless Status Information .....	39
Wireless .....	73
Wireless Roaming .....	80
WLAN client .....	9
WLAN Interface .....	73
Access Point Lists .....	83
AP Density .....	81
Background Scanning .....	82
Certificates Parameter .....	80

Connect Action .....	77	WEP .....	78
EAP Parameters.....	79	Wireless Roaming.....	80
no encryption.....	78	Wireless SSID Profile.....	76
Parameter.....	74	Wireless Status Information Service.....	75
Ping Test.....	82	WPA .....	78
Preferred / avoided access points.....	83	WPA2.....	78
Profile Change Action.....	76	WPA3.....	78
SCEP .....	80	WPA3 .....	78
SSID Profile.....	76		



## 21

## Document Changelog

The following table lists the revisions of this device description that have been published so far with the most important changes in each case.

**Table 80** *Document changelog*

Revision	Edited by	Description of changes
01 Date: 18.07.2017	RAD	Initial version of the English device description based on the German revision 04
02 Date: 11.01.2019	RAD	Changes for firmware 2.11p1. Newest A-layout with proper warning notices.
03 Date: 20.02.202	RAD	Changes for firmware 2.12k and 2.12r
04 Date: 18.02.2021	RAD	Changes for firmware 2.12s
05 Date: 08.02.2022	RAD	Newest A-layout with reduced paragraph formats
06 Date: 09.11.2022	RAD	Integration of variants with LTE and ac
07 Date: 22.11.2022	RAD	Minor error corrections in the tables on pages 27 and 28
08 Date: 13.03.2023	RAD	Changes for firmware 2.14h
09 Date: 24.01.2024	RAD	Changes for firmware 2.14p. Layout of chapter titles revised. Added this chapter document changelog.



# 22

## Copyright and Terms of Liability

### 22.1 Copyright

This manual is protected by copyright. All rights reserved. Violations are subject to penal legislation of the Copyright.

### 22.2 Exclusion of Liability

Any information given is to be understood as system description only, but is not to be taken as guaranteed features. Any values are reference values. The product characteristics are only valid if the systems are used according to the description.

This instruction manual has been drawn up to the best of our knowledge. Installation, setup and operation of the device will be on the customer's own risk. Liability for consequential defects is excluded. We reserve the right for changes encouraging technical improvements. We also reserve the right to change the contents of this manual without having to give notice to any third party.

### 22.3 Trade Marks and Company Names

Unless stated otherwise, the herein mentioned logos and product names are legally protected trade marks of Götting KG. All third party product or company names may be trade marks or registered trade marks of the corresponding companies.

# Innovation through Guidance

## **Götting KG**

Celler Str. 5 | D-31275 Lehrte

Tel. +49 (0) 5136 / 8096 -0

Fax +49(0) 5136 / 8096 -80

[info@goetting-agv.com](mailto:info@goetting-agv.com) | [www.goetting-agv.com](http://www.goetting-agv.com)



[www.goetting-agv.com](http://www.goetting-agv.com)