Specifications

and Operator Manual

Active Preselector RAP2

Version: 1.0
Created: 12.05.2025

Konstruktion & Musterbau Burkhard Reuter Ziegelstraße 54 06862 Dessau-Roßlau

Specifications

Dimensions (W x H x D):	140 mm x 38 mm x 113 mm (without connectors / control elements)
Frequency range:	70 MHz … 300 MHz
Attenuation loss:	0 ±3 dB
IP3:	>= +12 dBm
Maximum input level:	-10 dBm (without clipping), bypass: +13 dBm
Inherent noise power density:	<= -170 dBm/Hz
Power supply:	+6.0 … +15.0 V- / max. 400 mA
Connectors:	BNC 50 Ohm, hollow pin 2.5 mm, SMA
Weight:	<= 400 g
Environmental conditions:	0 ... +50 °C ambient temperature, <=90 % rel. humidity non-condensing, indoor application
Compliance:	CE according to DIN EN 55013, EN 55020, EN 60065 RoHS / WEEE Directive, ear-Reg. 27676700

All specifications are subject to design changes!

Safety precautions

Please always keep the following safety precautions in mind!

Never connect the device to any other voltage than indicated in the specifications. Under no circumstances should the device come into contact with the mains voltage of 230 V ~!

It is essential to observe the lightning protection regulations for the outdoor operation of electrotechnical systems! When connecting an antenna outside the protected area (e.g. your house), it must be professionally provided with lightning protection. The RF bypass must be equipped with overvoltage protection. In case of lightning hazard, immediately take the antenna out of operation and disconnect it safely from other devices (remove RF connection)!

Observe the permitted temperature range for starting up the device! Do not switch the device on or off again if this range is exceeded or fallen below!

The device is intended for indoor use. Do not expose it to unfavorable weather conditions (especially moisture and direct sunlight) when operating it outside protected rooms.

Always provide a safe placement on a flat, straight and solid base of sufficient carrying capacity! Always transport the device either in solid cardboard or wooden boxes (e.g. the delivery packaging), or transport it by firmly gripping the housing! The device may cause injury in the event of a fall due to its own weight!

Never expose the device to mechanical stress due to impact, pressure, vibration or shock which exceed a normal level.

If you notice any damage to the device, immediately take it out of operation (remove power supply)! If necessary, send it to the supplier for repairs.

Would you like to dispose the device due to damage or because you do not use it anymore, send it back to the supplier or return it to your local waste collection center. Never dispose of the appliance elsewhere, such as household waste. It pollutes our environment!

1 Operator Manual

1.1 Introduction

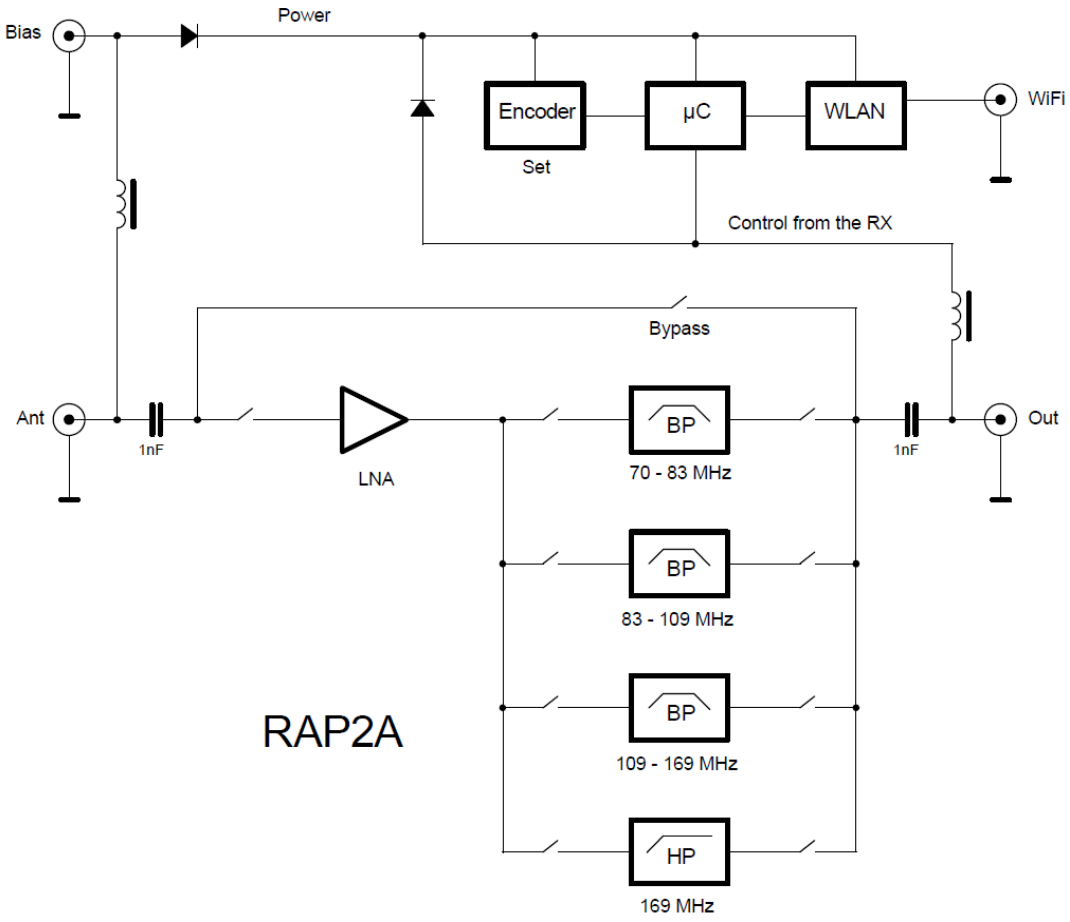
The RAP2 Reuter Active Preselector 2 is used to filter HF signals in the frequency range from 70 MHz to approx. 300 MHz. The main field of application is the pre-filtering of antenna signals for forwarding to a receiver. The receiver therefore contains a band-limited signal. This is particularly important for direct digitizing receivers (“SDR”) in oversampling mode in order to be able to implement the necessary limitation of the input spectrum to fulfill the Nyquist condition “reception bandwidth < half the sampling frequency”.

Further possible applications arise in measurement technology and general RF signal processing, e.g. to improve the output signal of signal generators (attenuation of harmonics and / or low-frequency interference signals).

The RAP2 works with broadband, switchable filters. The individual filters can be set by turning the “Set” knob on the device or by remote control with data signals at the “Out” connection. The device can also be supplied with power via the “Out” connection, so that a combined remote power supply and remote control from the RX (e.g. RSR200) or a special remote control device is possible.

In addition to wired remote control or one-button operation on the device, the RAP2 can also be controlled remotely via a wireless connection (WiFi). For this purpose, the preselector has a WiFi-compatible (IEEE 802.11 b/g/n) transceiver (station) for establishing a connection to an access point. Control can then be carried out using suitable applications (e.g. for smartphones, tablets or personal computers) from any end device connected to the access point.

The block diagram shows the structure of the signal processing with the filter’s switching options.



1.2 Filter characteristics

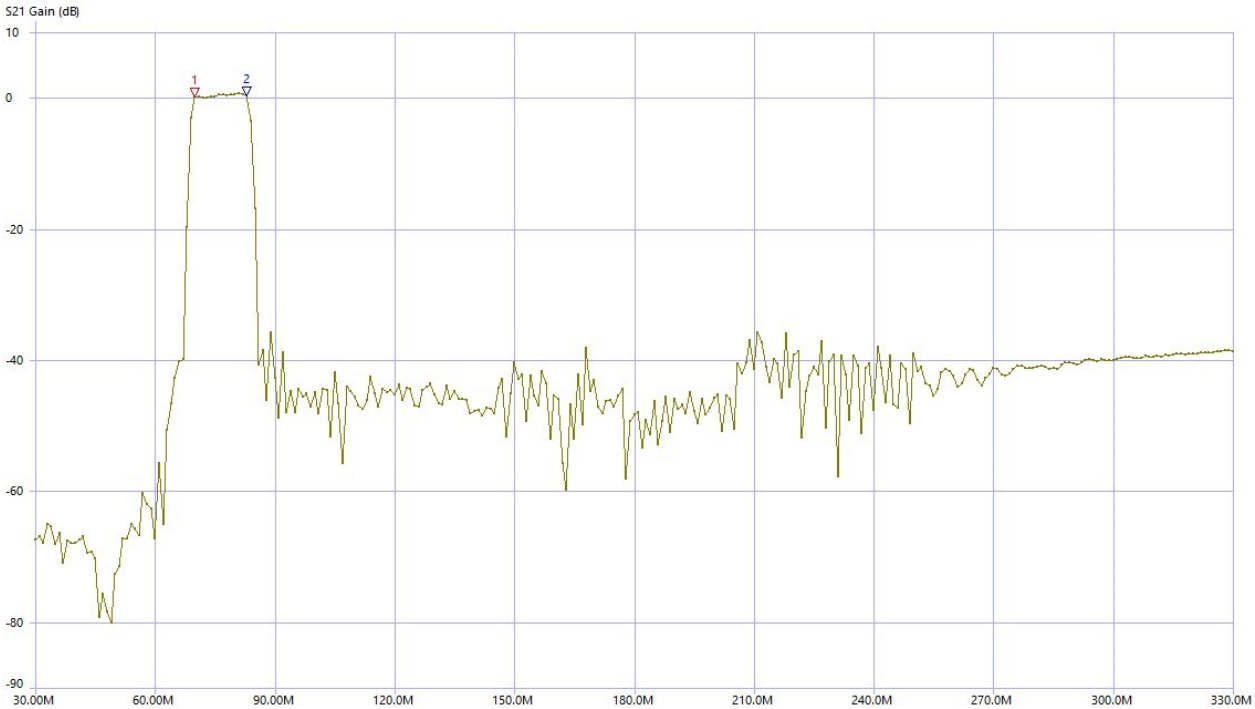
The RAP2 uses individual, permanently configured (non-tunable) band filters or high-pass filters. The band filters are designed as SAW (Surface Acoustic Wave) filters. These are characterized by high selectivity (edge steepness) and medium out-of-band attenuation. The high selectivity enables the suppression of frequencies close to the filter limits. This is particularly important for the intended main application: The selection of a Nyquist range during oversampling operation of an analog-to-digital converter (direct sampling receiver). In this case, the RAP2 acts as an anti-aliasing filter. Due to the high slope of the SAW filters, the sampling frequency can be set close to the desired frequency range and thus the largest possible interference-free range can be digitized.

The passbands of the SAW filters are optimized for use at clock frequencies of approx. 60 - 200 MHz. Depending on which filter is switched on, the clock frequency should be just below the lower or above the upper filter cut-off frequency. The nearest alias band (mirroring around the clock frequency) is then suppressed, whereby the maximum possible width of the selected band is available. Depending on the width of the filter passband and other digitization parameters, as well as other reception conditions, the clock frequency can of course also be selected as required.

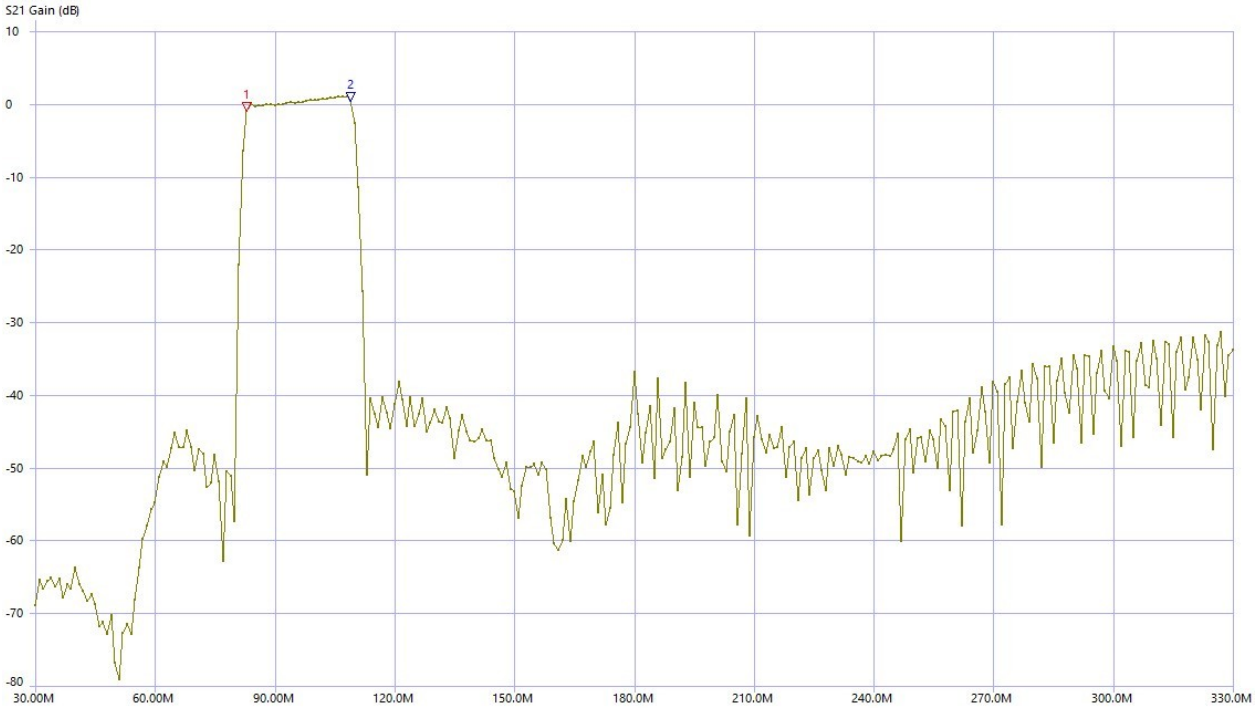
The low-pass filter for frequencies above 169 MHz enables even higher frequency ranges (e.g. DAB) to be accessed, although additional external filters may be required to limit the desired frequency range. In the ”Bypass” setting, the RAP2 can be completely bypassed.

Note: When using the RAP2 with the RSR200 receiver, the filters can be set automatically according to the selected reception frequency. In this case, the sampling frequency of the RSR200 is also automatically set to match the passband of the filters.

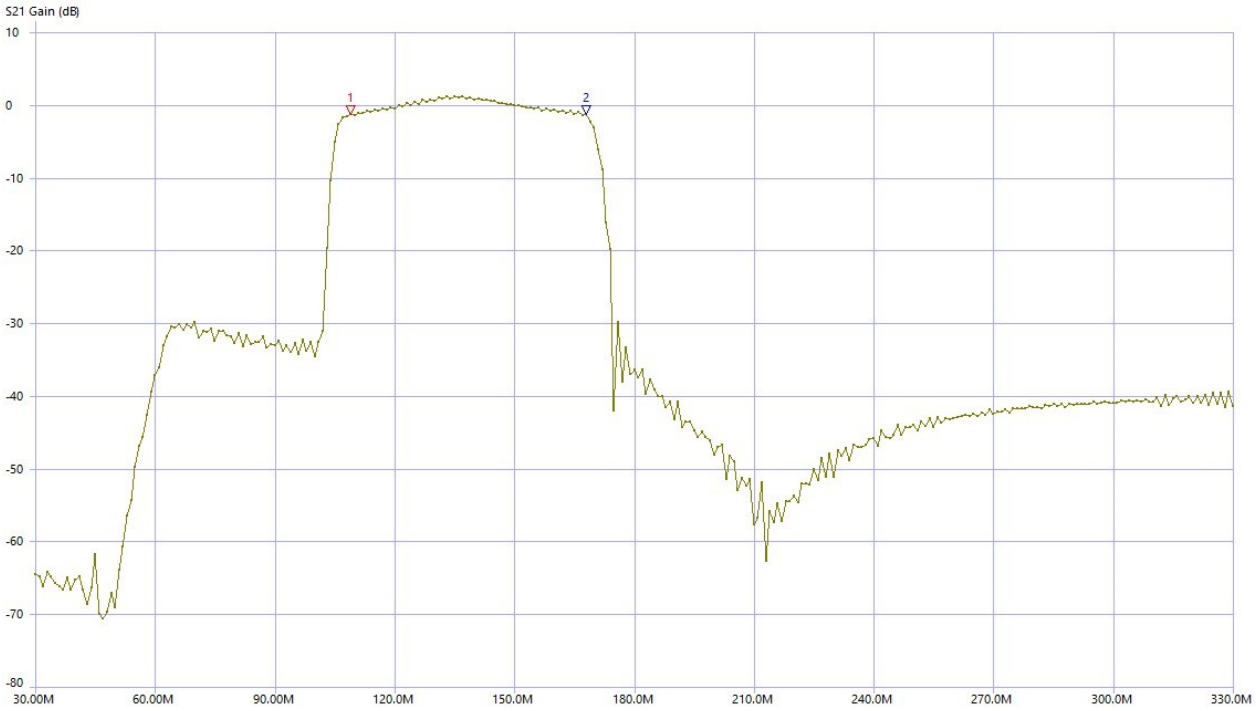
When a filter is switched on, a low-noise preamplifier (LNA) is always activated. It compensates for the passband attenuation of the filters so that the output signal has the same level as the input signal. The passband curves of the individual filters including the preamplifier are shown below.



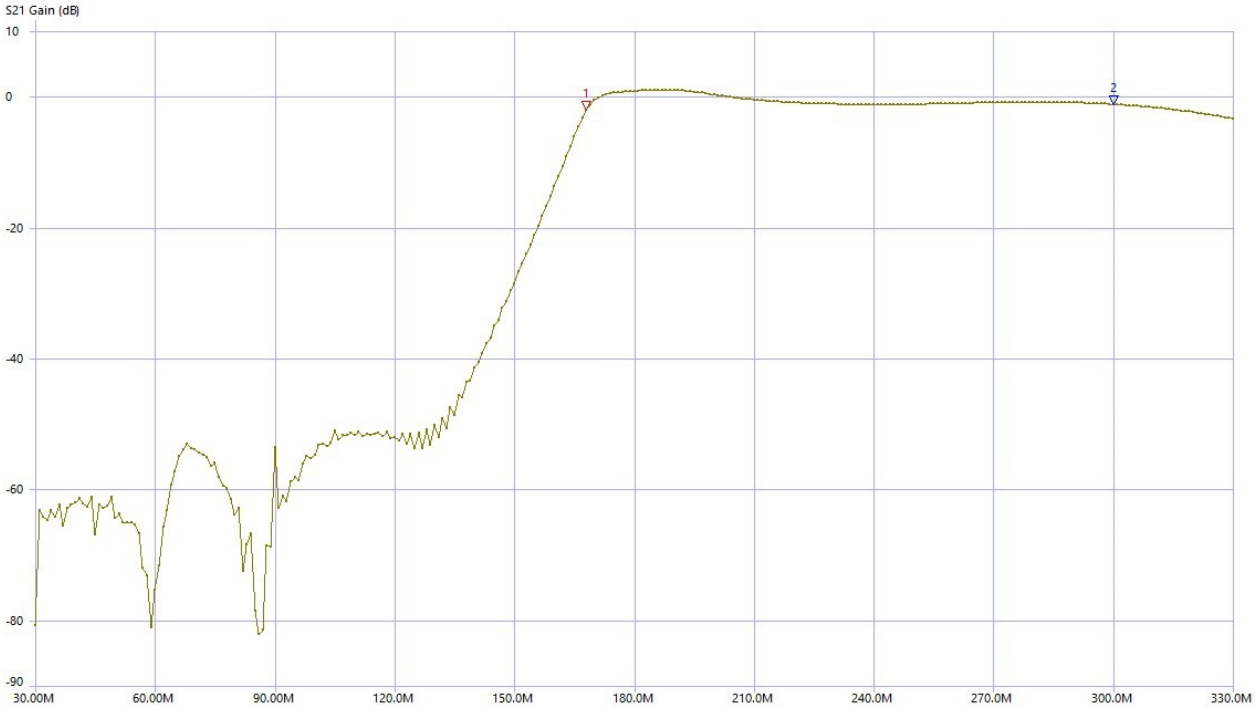
Setting 70 - 83 MHz (marker 1 - marker 2): The filter is optimal for a sampling frequency of approx. 60 - 66 MHz (digitization of the 3rd Nyquist zone). In this case, the alias band below the sampling frequency (2nd zone) is attenuated by more than 60 dB. If the sampling frequency is selected above the passband (2nd zone digitization), over 40 dB can still be achieved.



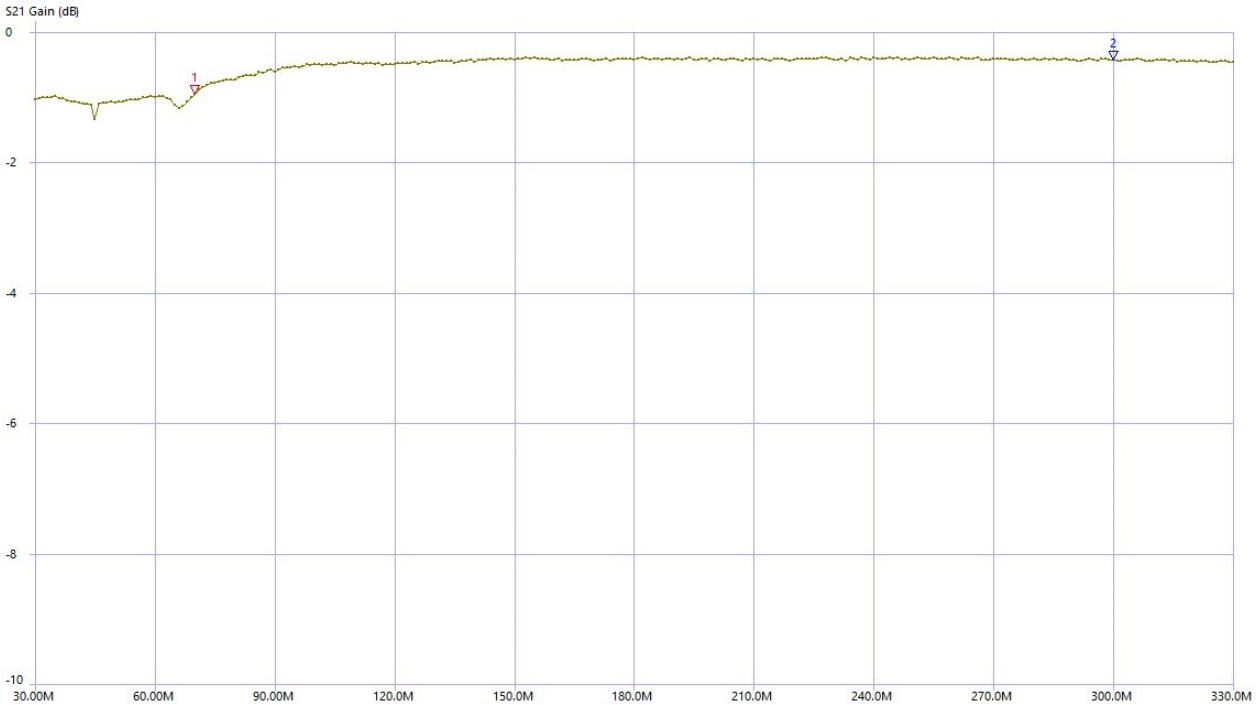
Setting 83 - 109 MHz: Digitization in 2nd or 3rd Nyquist zone. Alias attenuations of approx. 50 - 60 dB can be realized with a suitable selection of the sampling frequency.



Setting 109 - 169 MHz. A relatively wide filter for digitization mainly in the 2nd Nyquist zone. When selecting a sampling frequency of approx. 180 MHz, alias attenuations of over 40 dB are achieved.



Setting 169 - 300 MHz: Digitization from the 2. Nyquist zone with sampling frequencies from approx. 150 MHz. The high-pass filter primarily suppresses signals from the FM range up to the 2 m amateur radio range. Additional (external) filters are required for alias interference from the higher Nyquist zones.



Setting Bypass: Bypassing the preamplifier and filter.

1.3 Operation

The RAP2 is controlled using a rotary knob. A small OLED display is used to show the values. The rotary knob is a mechanically latching pulse encoder. It also has a push function. Every actuation of the rotary encoder is evaluated by a microprocessor (µC) and processed to the corresponding control of the device.

In addition, all device functions can be controlled via the WiFi interface. To do this, the RAP2 must be logged into a WiFi access point. The RAP2 can then be operated via any device connected to this access point (usually "IT technology" in the local network or Internet).

The current setting of the RAP2 is shown on the display. When the “Set” knob is turned, the filters are switched up or down one after the other. Outside the filter ranges, the system switches to “Bypass”.

Pressing the knob and turning it while it is pressed changes the brightness of the display.

Caution! The service life of the display decreases with increasing brightness! Set the brightness only as high as absolutely necessary for correct reading.

The current status of the WiFi connection is displayed below the frequency display:

– C: Connecting (attempt to establish a connection)
– L: Linked (connection successfully established)
– S: Serviced (device is actively controlled by an application via WiFi)
– No display: No connection and WiFi temporarily deactivated.

1.4 Remote control via WiFi

Remote control requires the RAP2 to log into an access point such as a WiFi router. Bidirectional control is then possible via an application on an IT device that is also connected (changes to the device are displayed in the app and vice versa).

The designation of the RAP2, under which it can be found in the network, is “RAP2x_nnnn” where “nnnn” is the serial number of the device with 4 digits (i.e. any preceding zeros) and “x” is the version of the device (currently A).

To log in to the access point, the RAP2 uses a secure connection according to "WPA2-PSK". This requires the specification of a password with which the access point allows WLAN subscribers (stations) to log in. The participant (in this case the RAP2) must know the name ("SSID") of the access point in which it wants to log in and query it to be allowed to participate in the network using the password. If the access point grants participation (it "authenticates" the station), the requester is logged in as a station and can now exchange data via the network.

Note: The access point must be configured so that it actually grants the request of the RAP2 with the correct password and does not e.g. deny it by blocking his MAC address or the like (see notes further below).

The RAP2 does not have the option (keyboard or similar) for alphanumeric entry of names and passwords. For this reason, certain simplifications and / or restrictions regarding the selection of access points must be observed.

1. Simplified / automatic login using the "WPS push button" method.

Many access points (especially routers) allow stations to log in using this method. The access point must be switched to this mode (usually automatically limited to 2 minutes), whereby it then transmits its authentication data (name and password) to all requesting stations. They therefore have all the data to be able to log in. The access point (or its operator) can then decide whether it really wants to authenticate the logged-in stations (e.g. the RAP2) or exclude it from participating in the network (e.g. unknown stations, spies and hackers).

Caution! Depending on the RAP2's firmware, it can be displayed in the list of stations found via WPS with the designation "RAP2" (possibly followed by further numbers) or as "espressif". This device must remain in the list of allowed devices.

To connect the RAP2 to the access point using the WPS push button, proceed as follows:

– Disconnect the RAP2 from the power supply, connect the antenna to the "WiFi" socket.
– Start the WPS push button method within the access point (Physical button on the router or button in configuration software). Wait a few seconds.
– Press the rotary knob on the RAP2 as far as it will go and connect the power supply.
– Release the rotary knob immediately after the display shows.

The top line of the display (where the set filter frequency normally appears) is now shown: "Search AP ...". When the connection to the access point has been successfully established, the display shows: "AP:" followed by the name of the access point (only the first 9 characters are visible). In the access point, the WPS authentication is canceled and the device found is displayed in the list of logged-in stations. An “L” appears below the frequency display on the RAP2 display to indicate successful logging in. As a check, the power supply can be briefly interrupted and restored (without pressing the rotary knob!). After a short time, the "L" must appear on the display again and the device RAP2 or espressif must be shown as connected in the access point configuration software. Now the RAP2 automatically logs into this access point each time it is switched on (if accessible).

2. Logging into a suitably configured access point

If there is no possibility of connection using the WPS method, the RAP2 can only connect to access points that use a specific password. It is called: "1234567890". Such a password is of course not secure, if only because it is publicly displayed here. This method only makes sense if an access point is used that does not allow any connections other than those to the RAP2.

To log the RAP2 into an access point with the password 1234567890, proceed as follows:

– Follow the steps as described for the WPS method (without starting the WPS on the router).
– After the "Search AP ..." message appears, turn the rotary knob **to the right** (min. approx. 90°).
– Press the knob again and release it immediately.
– The message "Scan APs ..." appears.
– The RAP2 now searches for all access points within radio range.
– After a while, the name of the first access point found appears.
– You can display the list of all the access points found by turning the rotary knob.
– Select the desired access point and briefly press the rotary knob.

If the access point allows the connection (authenticates the password 1234567890), the connection is established permanently and the "L" appears on the display of the RAP2 to indicate successful login.

If an application has access to the RAP2 and transmits control data, an ”S” appears in the display instead of the “L”. Remote control of the RAP2 is possible in this state. Control via the rotary knob is also always active, operations on the RAP2 are transferred to the app.

Instructions for successfully connecting the RAP2 to a WiFi router

The WPS push button method is standardized and should work with any router equipped with it. However, there are many different brands with many different setting options for the WLAN. Some of these can prevent a successful connection via WPS. Due to the large number of options, no general procedure for configuring the router can be given. There is also no guarantee that every device can be configured appropriately! But here are some tips on settings that should definitely be observed:

- WiFi radio channel: **MUST** (!) Be set to the 2.4 GHz band. "Auto" or similar is possible and should work. If a particular channel is to be used, identify a channel that is not used very often (there is often a graphic view of the channel assignment). A channel in the range of 8 to 13 is recommended.

- WiFi standard: 802.11 b. The "b" is important, combinations like "b+g+n" are also possible. "a" or "ac" or "a+c" usually do not work (but can be tried after successful login).

- Security / WPA encryption: WPA2 (CCMP). WPA (TKIP) or similar should also work. Stronger encryption such as "Enterprise" etc. do not work.

- WLAN access: "Allow all new WLAN devices" or similar setting. New devices must not be blocked (select "All devices may communicate with each other" or similar). Turn off the MAC filter. (Can be reactivated after successfully finding the RAP2 / espressif. Allow the MAC of the new device beforehand!)

- Activate WLAN coexistence if necessary.

Please note: After changes to the settings, a button "Apply" or "Save" or similar must often be pressed first so that these settings are not lost when changing the router menu (call up WPS).

Control via TCP connection

Caution! The exchange of self-generated data via the WLAN connection of the RAP2 represents an unauthorized intervention in the operating principle of the device! Any damage to hardware and software caused by faulty / harmful data is not covered by the warranty or guarantee!

The information about the data logs is provided without any guarantee of proper functioning when used in externally created software! There is no support for the development of software or other assistance than contained in this document.

The TCP connection is based on the server-client principle. For this purpose, the RAP2 provides a TCP server that permanently waits for connection requests from a TCP client from the network. As soon as a connection request with correct addressing (IP address and port) arrives, it is confirmed (socket connected) and the server is ready to transfer data. Only one connection can be established. Further connection requests are ignored / rejected until the existing connection is disconnected again. An existing connection is indicated with "S" in the display.

The RAP2 expects the following data packets:

Version request firmware

1. Byte	2. Byte	3. Byte
0x0D	0x12	0x00

The RSW responds to this message with a special data packet containing the version number and storage location of the programmed firmware:

1. Byte	2. Byte	3. Byte
0x0D	0xFF	Version

Version: Bit[6..0]: Version number, Bit[7] location: 0 = primary memory, 1 = secondary memory.

Note: After each successful reprogramming, the memory location is altered. This means that valid firmware is always available, even if errors occur during data transmission.

Frequency adjustment

1. Byte	2. Byte	3. Byte	4. Byte
0x0D	0xB0	FREQ low	FREQ high

FREQ low + high: Low and high byte frequency (16 bit word) in 0.1 MHz resolution.
Values smaller than 70 MHz or larger than 300 MHz switch the RAP2 to bypass. Each value in between switches the RAP2 to the appropriate filter.

Once this data packet has been received and successfully executed in the control unit, the RAP2 responds with exactly the same packet. A data packet is also output when the rotary knob on the device is pressed. The output frequency can lie anywhere within a filter range.

Further notes on controlling the RAP2 via WiFi

The programming for the data exchange of the RAP2 is done internally via a hardware-specific TCP/IP stack with associated API using standard interfaces ("sockets"). Software (an application) for establishing a connection with the RAP2 must operate this interface. Depending on the utilized computer, there are corresponding APIs for this, e.g. “INDY” for PCs.

Software development for TCP/IP with sockets offers many possibilities and thus also many "pitfalls". Here are some hints for successful control of the RAP2:

- ➔ After the RAP2 has connected to the network, a client socket must be configured which contains the IP address of the RAP2 (possibly simply determined automatically via DNS using the name “RAP2x_nnnn”) and the port number 55556.
- ➔ The socket is to be connected with the corresponding command (usually "Connect" or similar) with IP address and port of the server socket in RAP2.
- ➔ After successful connection, data can be taken from the client socket (data coming from RAP2) and sent through it (data to control the RAP2).
- ➔ The connection should be maintained as long as data is to be exchanged for the foreseeable future (usually until the program is terminated).
- ➔ Depending on the API, operating system and other settings of the program environment, there are many ways to organize the data transfer. Often small amounts of data are first collected and then sent in a larger package, and so on. (e.g. functions "Nagle" or "A-MPDU" or "A-MSDU"). This can lead to longer delays in transmission or fragmentation of data packets. Such functions should be disabled or minimized as far as possible.
- ➔ Several data packets according to the above list can be sent within one transmission (this then usually results in only one TCP packet). However, it must be guaranteed that complete instructions of correct length are always present in a package. Incomplete data / splitting of an instruction to several data packets lead to blocking of the connection.
- ➔ The data log of the RAP2 contains other instructions that are not documented here (e.g. for firmware update).

Caution! *Never send data to the RAP2 other than the data specified above! Other data can lead to the cease of function and even to the firmware in the device being completely deleted (which can not be undone)!*