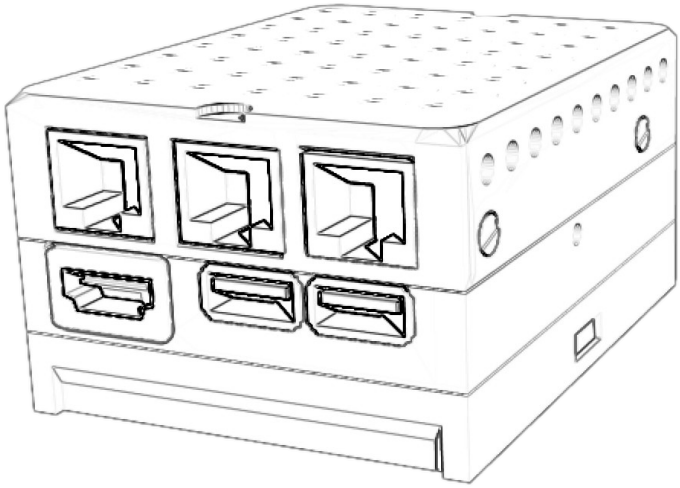
Raspberry Bridge

Technisches Handbuch



rAAAreware UG (haftungsbeschränkt)
Heidelberg

Inhaltsverzeichnis

Version 1.1, 19.01.2018

1. Über dieses Dokument

Dieses Dokument beschreibt den rAAAreware UG Raspberry Computer.
Dieser kann z.B. verwendet werden um einen MQTT Server für rAAAreware Messuhr-Module zu betreiben oder um eine Netzwerkbrücke für IoT Daten umzusetzen.

2. Features und Alleinstellungsmerkmale

2.1. OpenSource

Der Gerät kann ohne proprietäre oder eigenentwickelte Software betrieben werden. Alle eingesetzte Software ist frei verfügbar und verwendbar (OpenSource). Details zu den Lizenzbedingungen einzelner Module sind in der Raspberry Dokumentation zu finden.

2.2. Standardmodule

Um einen einfachen und kostengünstigen Aufbau zu gewährleisten wird komplett auf Eigenentwicklungen verzichtet. Stattdessen werden erprobte und in hohen Stückzahlen einfach verfügbare Standardmodule vewendet.

2.3. Lötverbindungen

Um einen Ausfall durch Kontaktprobleme und somit einen sicheren und zuverlässigen Betrieb im industriellen Umfeld zu gewähren wird auf **interne** Steckverbindungen komplett verzichtet. Alle Verbindungen zwischen den Modulen sind gelötet.

2.4. Vertikale Steckverbindungen

Alle Steckverbindungen sind vertikal ausgerichtet. Dadurch ergibt sich die geringstmögliche horizontale Kabelbelastung, welche durch mechanische Belastung einen Ausfall der Steckverbindung bedeuten kann. Ein Abknicken der Stecker wird durch die vertikale Anordnung minimiert.
Die RJ45 Steckverbindungen sind mechanisch gegen herausfallen gesichert und können daher einfach nach unten angeordnet werden. Die Stromversorgung ist nach oben herausgeführt und dadurch bei ordnungsgemäßem Einbau vor herausfallen geschützt.
Die Kontrollleuchten sind ebenso oben angebracht damit sie einfach eingesehen werden können.

3. Technischer Aufbau

Grundlage bildet ein Raspberyy PI Zero/W.

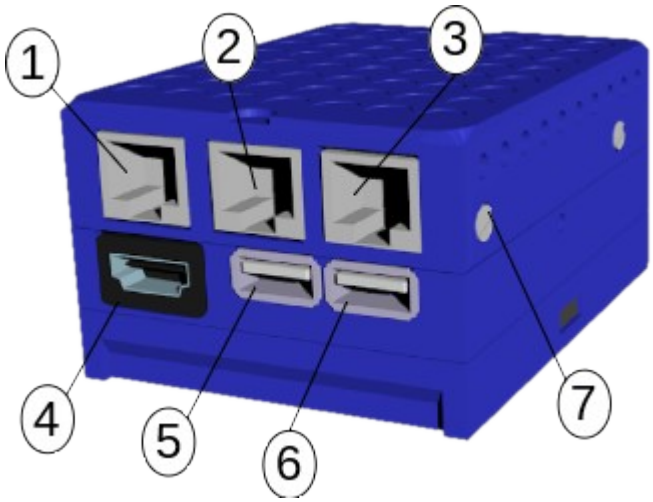
3.1. Mechanischer Aufbau

Das Gehäuse ist individuell in ABS oder PLA Kunststoff gedruckt. Dadurch können sehr schnell erforderliche Änderungen oder individuelle Anpassungen vorgenommen werden.

Die Montage erfolgt idealerweise auf eine 35 mm Hutschiene. Die Breite auf der Montageplatte beträgt 4BE.
Einzelne Module sind gestapelt angeordnet. 4 Schrauben ermöglichen eine einfache Demontage der einzelnen Module.
Unterstes Modul ist die Hauptplatine mit dem Raspberry Computer. Darüber angeordnet sind die Zusatzmodule - z.B. das Netzwerkmodul mit bis zu 3 Netzwerkkarten.

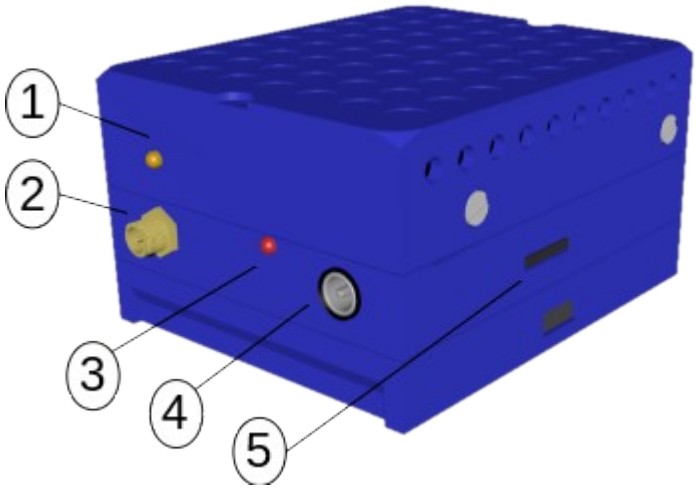
3.1.1. Ansicht Unten

1: WAN/LAN RJ45 Anschluß.
2/3: LAN Anschluß, z.B. für WLAN Accesspoints (optional).
4: HDMI Anschluss incl. mini-HDMI Adapter.
5/6: USB 2.0 Ports.
7: Verschraubung.



3.1.2. Ansicht Oben

1: LED WAN Netzwerk Aktivität.
2: RP-SMA WLAN Anschluß (optional).
3: Betriebsspannungsanzeige.
4: Versorgungsspannung (5V/1.2A).
5: MicroSD Karteneinschub.



3.2. Elektronik Aufbau

Basis bildet der Raspberry Einplatinencomputer.

Die Spannungsversorgung beträgt 5 Volt Gleichspannung.
Die maximale Stromaufnahme ist abhängig von den eingesetzten Modulen, sollte im Normalfall jedoch unter 1 A liegen.
Die Gesamtleistungsaufnahme beträgt daher <5 Watt.

Anschluss von Netzwerkkarten
Der Raspberry PI besitzt mehrere Anschlussmöglichkeiten für Netzwerkkarten:
a) Interne Netzwerkkarte und interner WLAN-Adapter
b) Externe Netzwerkkarten über USB. Bis zu 4 Netzwerkkarten.
c) Externe Netzwerkkarten über SPI Interface. Bis zu 2 Netzwerkkarte.

Die Netzwerkkarten/Netzwerkverbindungen können über Konfigurationseinstellungen z.B. Routing- oder Firewall-Funktionen für Netzwerke vornehmen.

4. Softwareinstallation und Inbetriebnahme

Grundlage der Installation ist ein Raspberry mit aktuellem Raspian Linux Betriebssystem.
Zur Konfiguration des Gerätes sind Linux Kenntnisse erforderlich.

Abhängig vom geplanten Einsatzzweck sind verschiedene Konfigurationen möglich.
Manche Konfigurationen können auch parallel konfiguriert und verwendet werden.

4.1. Betrieb als Netzwerk-Bridge

4.1.1. Konfigurationsscript

Die Installation und Konfiguration erfolgt mit dem Konfigurationspaket "rAAAreware.raspberry.bridge.setup.tar" bzw. "rAAAreware.raspberry.bridge.wlan-ap.setup.tar" für die Konfiguration mit oder ohne WLAN-Accesspoint.

Download des aktuellen Paketes unter

http://raaareware.de/downloads/kunden/zf/rAAAreware.raspberry.bridge.setup.tar
(für 3x LAN Variante)

http://raaareware.de/downloads/kunden/zf/rAAAreware.raspberry.bridge.wlan.ap.setup.tar
(für 1xWLAN, 1xLAN Variante)

Kopieren des Paketes in z.B. ~/setup.
Dort kann das Paket dann z.B. mit
`tar xfv zf.rasp.lan.setup.tar`
entpackt werden. (oder z.B. „`tar tfv zf.rasp.lan.setup.tar`“ zum Auflisten des Inhalts.)

Es besteht aus den folgenden Dateien:

init-zf (Skript)	Ersteinrichtung Hardware

config-zf.txt	Basiseinstellungen für das init-zf-Skript.
apply-ufw (Skript)	Einstellungen mit Firewallregeln für die UFW (uncomplicated firewall)
config-nat.txt	Zusätzliche
apply-defaults (Skript)	Kopiert die Konfigurationsdateien aus /default-config an die entsprechenden Positionen im Dateisystem.
default-config	Verzeichnis mit einigen einstellungsspezifischen Dateien, die, gegebenenfalls nach zusätzlichen Anpassungen, mit „sudo ./apply-defaults“ an die entsprechende Position im Dateisystem kopiert werden
driver	Verzeichnis mit Hardware-Treiber und -Einstellungen

4.1.2. Zugriff

Sowohl im konfigurierten Zustand als auch nach einer vollständigen Neuinstallation mit einem neuem Image ist der SSH-Server standardmäßig aktiviert; Zugriff ist z.B. mit jedem ssh-Client (in Windows z.B. `putty`, sowie `winscp` zum Kopieren von Dateien) über den WAN-LAN-Netzwerkport möglich.

Standardlogin des Raspberry Pi: „`pi`“ mit Passwort „`raspberry`“.

Im vorkonfigurierten Zustand ohne DHCP-Server lautet die IP-Adresse 192.168.0.2, ansonsten wird eine DHCP-Adresse bezogen.

Es kann auch ein HDMI-Kabel angeschlossen werden und direkt auf den Raspberry Piu zugegriffen werden. Hinweis: Der HDMI-Anschluss wird deaktiviert, wenn beim Booten kein Bildschirm angeschlossen ist, daher nach Anschluss des Bildschirms neu starten.

4.1.3. Erstinstallation

Nach einem kompletten Werksreset mit Neuaufspielen eines Images muss eine Basisinstallation durchgeführt werden. Dies ist normalerweise später nicht mehr nötig, kann aber trotzdem nochmal aufgerufne werden, um z.B. ein Systemupdate durchzuführen.

Zunächst die Einstellungen in `config-zf.txt` prüfen und gegebenfalls anpassen (einen Texteditor kann man z.B. starten mit „`nano config-zf.txt`“). In den beiden Archiven sind zwei leicht unterschiedliche Standardkonfigurationen, jeweils mit und ohne WLAN-Accesspoint-Funktion, vorhanden.

Anschließend das init-Skript als root aufrufen:

```
sudo ./init-zf --init
```

Das Skript muss direkt aus dem Ordner aufgerufen werden, und alle weiteren Dateien müssen auch in diesem Ordner vorhanden sein.

Dieses Skript führt Basiseinstellungen entsprechend den Einstellungen in `config-zf.txt` durch: Standardmäßig wird die Sprache und Tatstatureinstellung auf deutsch gesetzt, Bluetooth deaktiviert und, wenn nicht das Skript mit WLAN-Accesspoint

verwendet wird, auch das WLAN-Modul; der SPI-Modus für die internen Netzwerkkarten wird aktiviert sowie die passenden Treiber installiert und die Gerätenamen auf „`eth_p0`“ und „`eth_p1`“ festgesetzt. Außerdem wird beim ersten Aufruf ein zusätzlicher Benutzer angelegt (Standard: `pi-zf`).

Es wird außerdem ein Softwareupdate durchgeführt, sofern Internet verfügbar ist – daher evtl. nach durchgeführter Erstinstallation erneut aufrufen. Zugriff auf das Internet sollte über den externen LAN-Port ermöglicht werden. Es wird außerdem benötigte Software nachinstalliert (Firewall und DNS-Server, sowie optional `hostap` für den WLAN-Accesspoint), auch hierfür ist Internetzugriff erforderlich.

Grundsätzlich kann die Installation auch mehrmals aufgerufen werden.

Startet außerdem die Skripte `apply-defaults` und `apply-ufw`, sofern nicht mit der Option --`no-config` aufgerufen.

Ein Großteil der Einstellungen des init-Skripts, sowie weitere (nicht unbedingt Router-relvante) Anpassungen des Raspberry Pis können auch durch das Raspberry-Standardinstallationsskript, aufzurufen mit „`sudo raspi-config`“, durchgeführt werden. Hier kann z.B. das Booten in die grafische Benutzeroberfläche aktiviert und deaktiviert werden.

Standardlogin des Raspberry Pi: „`pi`“ mit Passwort „`raspberry`“. Bitte ändern Sie das Vorgabepasswort umgehend ab und notieren Sie sich dieses Passwort an einem sicheren Ort.

Befehl zum Ändern des Passworts für pi

```
sudo passwd
```

Um das Passwort eines anderen Logins neu zu setzen:

```
sudo passwd Benutzername
```

4.1.4. Konfigurationsanpassungen

Während `init-zf` und `config-zf` i.d.R. nur einmalig ausgeführt und nur geringfügig angepasst werden müssen, sind die anderen Dateien des Archivs für benutzerspezifische Einstellungen vorgesehen, die teilweise an eigene Erfordernisse angepasst werden müssen.

Das Verzeichnis `default-config` enthält angepasste Systemdateien mit einer Startkonfiguration. Diese werden vom Installationsskript oder durch manuelles Starten des Skripts

```
./apply-defaults --yes
```

an die passenden Stellen im System kopiert. Um eigene Anpassungen durchzuführen, die Dateien im `defaults`-Ordner editieren und dann mit `apply-defaults` übernehmen. Alternativ direkt die Systemdateien editieren, in diesem Fall aber darauf achten, dass sie bei einem erneuten Aufruf der Installationsskripte gegebenenfalls überschrieben werden.

Standardkonfiguration:

Der Router ohne Accesspoint ist standardmäßig eingerichtet mit 2 Subnetzen 192.168.1.0/24 sowie 192.168.2.0/24 an den Netzwerkschnittstellen `eth_p0` und `eth_p1`, jeweils mit DHCP Server. Der WAN-Port ist auf `eth0` eingerichtet als DHCP-Client. Findet er keinen DHCP-Server, wählt er die IP-Adresse 192.168.0.2. Die Firewall ist sehr strikt eingestellt und erlaubt nur ausgewählten Ports den Zugriff auf die Pi, und nur ausgewählten Ports das Routing aus den Subnetzen ins WAN.

Der Router mit WLAN-Accesspoint nutzt für das WLAN das Subnetz 192.168.3.0/24 und einen DHCP Server, sowie ebenfalls `eth0` als WAN-Port.

Angepasst werden muss in der Regel der Gerätename in der Datei `hostname`.

Übersicht der Konfigurationsdateien:

Folgende Dateien werden von der Konfiguration verwendet:

`dhcpcd.conf`, wird kopiert nach `/etc/dhcpcd.conf`

> Konfigurationsdatei für die IP Einstellungen der Netzwerkkarten. Diese können wahlweise
> mit festen IP oder als DHCP-Client eingerichtet werden.
> Relevante Einstellungen: IP-Adressen, DHCP-Abruf

`dnsmasq.conf`, wird kopiert nach `/etc/dnsmasq.conf`

> Einstellungen für DNS-Server und DHCP-Server.
> Relevante Einstellungen: Subnetze (abhängig von den IP-Adressen), Aktivierung des DHCP-Servers in den Subnetzen; DNS-Server in den Subnetzen

`hostname`, wird kopiert nach `/etc/hostname`

> Eine einzelne Zeile mit dem Netzwerknamen der Raspberry Pi-Box. Sollte für jedes Gerät unterschiedlich sein.

`interfaces`, wird kopiert nach `/etc/network/inferfaces`

> Auflistung der Netzwerkadapter. Muss bis auf das Aufführen der Netzwerkgeräte nicht weiter konfiguriert werden; die Netzwerkeinstellungen (z.B. IP-Adressen) werden seit einiger Zeit in `dhcpcd.conf` durchgeführt, nicht mehr in `interfaces`

`sshd_config`, wird kopiert nach `/etc/ssh/sshd_config`

> Sehr umfangreiche Konfigurationsmöglichkeiten des ssh-Servers. Kann normalerweise größtenteils unverändert verwendet werden.
> Verwenden, um einzuschränken wer und/oder von wo und/oder mit welchen Autorisierungsmethoden sich einloggen darf.

`sysctl.conf`, wird kopiert nach `/etc/ufw/sysctl.conf`

> hier muss `net/ipv4/ip_forward=1` (und analog für ipv6) gesetzt sein, damit das Routing aus den Subnetzen funktioniert, siehe auch bei „Firewall“. Ansonsten

keine Einstelllungen nötig.
Sollte die ufw nicht verwendet werden, muss die entsprechende Einstellung in der Standard `sysctl.conf` unter `/etc/sysctl.conf` durchgeführt werden.

`ufw` wird kopiert nach `/etc/default/ufw`

Standardeinstellungen für die ufw-Firewall. Aktuell keine Anpassungen.

Eine mögliche Anpassung ist die Default-Einstellung für„`Default_forward_policy`“, um das Routing aus den Subnetzen allgemein freizugeben (und gegebenenfalls einzelne Ports zu sperren). Aktuell ist aber das Routing allgemein gesperrt, außer für spezielle Ports, siehe Firewall, und das Skript `apply-ufw`

Nur für den WLAN-Accesspoint:

`hostapd`, wird kopiert nach `/etc/default/hostapd`

Aktiviert den hostapd-Dienst und verweist auf die Konfigurationsdatei (`/etc/hostapd/hostapd.conf`), ansonsten in der Regel keine weiteren Anpassungen nötig

`hostapd.conf`, wird kopiert nach `/etc/hostapd/hostapd.conf`

WLAN-Einstellungen für den Accesspoint. Wichtigste Einstellungen sind das WLAN-Passwort und die SSID. Es wird WPA 2 PSK verwendet (da die Uhren dieses unterstützen). Grundsätzlich sind hier sehr weitgehende Einstellungen möglich. Das Archiv enthält zusätzlich die Datei `hostapd.commented.conf`, die viele weitere Einstellungen mit entsprechenden Kommentaren enthält, die gegebenenfalls als Basis einer erweiterten Konfiguration genutzt werden kann. Die `hostapd.conf` enthält eine verkürzte Fassung und lediglich die tatsächlich aktiven Parametern.

Das Skript startet und aktiviert außerdem die zugehörigen Dienste, dies muss gegebenfalls manuell gemacht werden:

- Neustarten von `dnsmasq`
- Neustarten von `dhcpcd`
- Neustarten der Netzwerkadapter
- für den WLAN-Accesspoint:
  - Neustarten von `hostapd` (für WLAN-Accesspoint)
  - Deaktivieren des WLAN-Clients-Dienstes `wpa_supplicant`

4.1.5. Firewall

Die Konfiguration der Firewall erfolgt in der Datei `apply-ufw`. Es handelt sich um ein Skript mit ufw-Firewall-Regeln. Das Skript wird mit

```
./apply-ufw
```

gestartet und die Regeln aktiviert, diese bleiben dann dauerhaft aktiv, bis sie geändert

werden. Es können recht einfach weitere Regeln hinzugefügt werden. z.B. weitere Ports freigegeben werden. Die Befehle können alternativ auch direkt in der Kommandozeile eingegeben werden (z.B. wird mit `sudo ufw allow 80` der Zugriff auf den Port 80 des Raspberrys freigegeben), allerdings werden diese beim nächsten Aufruf von `apply-ufw` dann wieder gelöscht.

Als Beispiel die Firewallregeln für den WLAN-Accespoint:

```
# blocke alle einkommenden Pakete
ufw default deny incoming
# erlaube Zugriff vom Raspberry Pi aus nach auÃŸen
ufw default allow outgoing
# sperre Forwarding/Routing von einem Subnetz ins andere
ufw default deny routed

# erlaube Zugriff von außen auf den DHCP-Server
ufw allow 67

# erlaube DNS-Auflösung
ufw allow 5353
ufw allow 53

# erlaube ssh Zugriff
ufw allow in on eth0 to any port 22

# Route den mqtt port 1883 der Messuhren aus dem wlan ins wan (eth0)
ufw route allow in on wlan0 out on eth0 to any port 1883
```

Routing-Konfiguration

Damit das Routing funktioniert, müssen ein paar Grundeinstellungen durchgeführt sein (sind in den default-Dateien eingerichtet):

- `net.ip4.ip_forward=1` (in `sysctl.conf`)
- eine Firewall/NAT-Regel; diese ist in „`config-nat.txt`“ enthalten und wird immer mit aktualisiert. Wird die Konfiguration später nicht hier vorgenommen, muss unbedingt darauf geachtet werden, dass die iptables-Regeln in `/etc/ufw/before.rules` (oder einem anderen geeigneten Ort) hinterlegt ist:

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth0 -j MASQUERADE
```

(in der Datei `/etc/ufw/before.rules`, und damit auch in `config-nat.txt` wird diese Regel leicht anders notiert, da sie von ufw gelesen und ausgewertet wird).
Die Regel/die Datei muss auch angepasst werden, wenn andere Subnetze verwendet werden sollen.

Das Skript `apply-ufw` (in Kombination mit `config-nat.txt`) sollte vermutlich auch nach der Ersteinrichtung verwendet werden, um die Firewall detaillierter zu konfigurieren.

4.1.6. Wichtige manuelle Anpassungen

Anpassung der LAN-IP des Raspberrys:

- `dhcpcd.conf` Anpassung der statischen IP/DNS-Server/Gateway

Anpassung der Subnetze:

Um die Subnetzbereiche von 192.168.1.0/24 (bzw. 192.168.2.0/24 bzw. 192.168.3.0/24) zu verändern, müssen diese Werte in 3 Dateien angepasst werden:

- `dhcpcd.conf` für die IP-Adresse der Netzwerkschnittstelle (z.B. 192.168.1.1)
- `dnsmasq.conf` für den DHCP-Adressbereich (z.B. 192.168.1.100-192.168.1.200), oder z.B. auch das deaktivieren von dhcp an bestimmten Netzwerkschnittstellen
- `config-nat.txt` um das Routen ins LAN zu ermöglichen

Anpassung der WLAN-Einstellungen (Accesspoint):

- `hostapd.conf` enthält das WLAN-Passwort und die SSID
- Hinweis: Soll der Raspberry als WLAN-Client verwendet werden, muss der Dienst `wpa_supplicant` eingerichtet/verwendet werden sowie `hostapd` deaktiviert werden.

Gerätenamen:

- `hostname`, sollte für jedes Gerät unterschiedlich sein

Portfreigaben/NAT:

- siehe 4.1.5 Firewall

4.2. Nützliche Befehle

`ifconfig`
zeigt Netzwerkeinstellungen (ips, …) an

```
sudo shutdown now
sudo reboot
```
Herunterfahren bzw. Neustart

`nano`
einfach zu bedienender Texteditor

`dmesg`
Anzeige von Betriebssystemnachrichten/Fehlern/Logs
Außerdem interessant: Verzeichnis /var/log mit diversen Log-Dateien

`lsusb`
Auflistung von usb-Geräten

`ps -A`
Liste der aktiven Programme
`top`
Anzeige analog zum Windows-„Taskmanager“

`kill`
Möglichkeit zum erzwungenden Beenden eines Programms

Die meisten Dienste lassen sich Neustarten mit

```
sudo /etc/init.d/dienstname restart
```
oder alternativ über
```
sudo systemctl restart dienstname
```
Hierüber kann ein Dienst auch oft deaktiviert oder aktiviert werden, z.B.
```
sudo systemctl enable dienstname
```

```
sudo apt-get install usbmount
```
Automatisches mounten von USB Sticks.

5. Kontaktdaten

rAAAreware UG (haftungsbeschränkt)
Steigerweg 49
69115 Heidelberg
info@raaareware.de