Haunting house

A home automation story

v 0.9, 26 June 2016

Contents

1. Intro **8**

2. Disclaimer **9**

3. Organization **10**

4. Acknowledgement **11**

5. License **12**

PART I 13

6. The general idea **14**
6.1. Appartment server 14
6.2. Basement server 14

7. Basic tools **15**
7.1. Soldering iron 15
7.2. Copper Wire 15
7.3. Cable Connectors 15

8. Appartment server **18**
8.1. Intro 18
8.2. Hardware for the server 18
8.3. Power supply 18
8.4. Push Buttons / Digital Input 20
8.5. Thermostat / Analog Input 25
8.6. Relays / Digital output 26
8.7. Software stack 43
8.8. Configuration details 45
8.9. openHAB Items&Sites&Rules 49

9. Basement server **53**
9.1. Intro 53
9.2. Hardware 53
9.3. Software 57
9.4. Configuration 58

PART II 70

10. Network setup **71**
10.1. Static IP 71
10.2. Dynamic IP 71
10.3. IP address setup 71
10.4. Hostname and hosts 72
10.5. Provide DHCP services 72

11. Mass Storage 74
11.1. USB Hub 74
11.2. USB Disk 74
11.3. Directory layout 76
11.4. NFS 76
11.5. Samba 77

12. Backup 80
12.1. So why? 80
12.2. rsync 80

PART III 83

13. Access Point 84
13.1. /etc/network/interfaces 84
13.2. Disable power saving 84
13.3. Switch hostapd 85
13.4. Run hostapd as daemon 85
13.5. Experience 85

14. WAN access 87
14.1. Surfstick 87
14.2. SIM card 88
14.3. Configuration 89
14.4. Stick configuration 89
14.5. wvdial 91
14.6. SIM PIN 93
14.7. pppd 94
14.8. Network config 95
14.9. Keep alive 97
14.10. Auto disconnect 97
14.11. Security 97
14.12. Issues 98
14.13. More … 98

15. Remote Control 100
15.1. SSH 100
15.2. DynDNS 105
15.3. Reverse tunneling 106
15.4. SSH Tunneling 106

16. Thou shalt not write… 109
16.1. Do not write at all 109
16.2. Use temporary file system 109
16.3. Disable swap 109
16.4. Reduce system logging 109

17. Tweak Raspbian 110
17.1. Install minicom 110
17.2. Install screen 110
17.3. Hostname 110
17.4. Disable root login 110
17.5. Memory 111
17.6. Move root file system 111

17.7. Watchdog 111

18. What time is it? 113
18.1. Network Time 113

19. Improve logging 114
19.1. Log to temporary file system 114
19.2. Log to external disk 114
19.3. Tweak logrotate 114
19.4. Move logs 115

20. Network monitoring 121
20.1. Show statistics 121
20.2. Send statistics 121

21. Data logging 123
21.1. Data sources 123
21.2. Data sinks 125
21.3. Data visualization 127

22. Event notifications 128
22.1. Sending eMail 128

PART IV 130

23. More event notifications… 131
23.1. Sending SMS 131
23.2. Twitter 131
23.3. Push message platforms 131

24. Adding a UI device 132

25. Alternate actor technology 133

26. Access control 134

PART V 137

27. Troubleshooting 138

28. Abbreviations 139

29. *nix 101 140
29.1. Package management 140
29.2. mount 140
29.3. shebang 140
29.4. python 140
29.5. Users & Passwords 140
29.6. Service Management 141
29.7. Send command to background 141
29.8. Concatenatign output 141
29.9. whoami 141
29.10. groups 141
29.11. rm 141

29.12. File system magic 141
29.13. Networking 141
29.14. crontab 141

30. Tools 143
30.1. Connecting 143
30.2. Some network tools 143

31. File listings 144
31.1. /etc/fstab 144

1. Intro

This is the story of a home automation project. I hope it may serve as help for anyone to come who wants to make the same mistakes again…

After having setup some “simple” Homematic scenarios before, I wanted to try the “real thing”. Setup all hardware and software components by myself, in an environment that is not limited by existing solutions. I played around with a Raspberry, made some demo installs, made some LEDs switch on and off, clicked some relays…

That’s when I got the chance to make it all come true: We started to renovate a building completely, including new electricity. The challenge: The solution should not be (much) more expensive than a classical one and the tenants to come should be able to live with it, both from a usability and reliability point of view.

As far as existing “home stories” on home automation, scattered everywhere on the internet, are concerned, this is an important difference (in my humble opinion): There’s no way for your wife to shout in despair “Darling, hurry up, reboot the house, the oven is offline and the Smiths are coming…”.

2. Disclaimer

All content has been compiled with care and to the best of my knowledge. Everything you find here is working fine with me.

Much of the content is a derived work of tips and tutorials on the internet. I think what makes this book unique is the “putting the pieces together”.

However, I cannot assume liability for the up-to-dateness, completeness or accuracy of the content. Any damage or loss is up to you. Please, double check what you are doing.

I’m in no way “expert” in the domains to be explored, neither in unix nor in electrics nor electronics. So, naturally you will probably not find the best, the cheapest or nicest solution. It’s a collection of working technology…

If you belong to the folks who claim “when there’s still a button, it’s not home automation” - then simply look at it as the basic infrastructure for all the glorious things to come.

If you find any information that’s wrong or have ideas for improvement, feel free to send them to wachenburgweg@gmail.com.

And, finally: Stay away from high voltages. Anything that has to do with the plain old powerline is out of scope here.

3. Organization

You may not believe it (yet) – but this is a quite complex project. I tried my best to organize the book in way to break down the tasks and issues in small manageable parts.

This way you can decide, what's your level of sophistication and automation you want to achieve.

The first part will give you the general idea of what is expected. Then we will immediately select the tools to do so and bring up a "minimal" working system. Until now we will have designed an "island" system that can control a single apartment.

The second part will combine the islands and you will see: the whole is more than the sum of the details.

The third part will add concrete bells and whistles. This is the part that will never end, there's always one more step to go.

Part four is about the whistles to add sooner or later and some alternative approaches.

Part five is a giant appendix.

4. Acknowledgement

There's quite few in this book invented here. I hope it's the collection of topics, the production setting or the careful composition of know how that makes it worth reading.

Nevertheless – this book is written "on the shoulders of giants". Contributions that made this book possible are countless.

- Countless bloggers that build up my "Linux Know How"
- Another countless bloggers that built my "electronics expertise"
- And then the ones that made me an "Raspberry expert"
- Countless programmers that provided an incredible software stack for **free**

If you can improve this book by corrections or ideas, feel free to contact me.

And then, a special thanks to my loving and beloved wife: If she would have suspected what I am about to do and where this will end, this project would have never seen the light of day ☺

5. License

This book is covered by a Creative Commons License, the “Attribution – Non Commercial” one (CC BY-NC 3.0). In non-legalese this means you can do whatever you want with the content as long as you mention where it is from and do not take commercial advantage from it.

See http://creativecommons.org/licenses/by-nc/3.0/legalcode.

Part I

Here you will learn what this project is all about and what are the initial steps to set up the automation scenario.

6. The general idea

The idea of the architecture is simple:

We have 3 apartments, each getting its own HA central. Another HA central, with different duties, is in the basement. All systems are interconnected but the components are shielded from unauthorized access. For remote access one fine day I want to setup a cable modem or surfstick based connection.

Any part of the system should be in some sense "open" – i.e. not a proprietary technology that cannot be replaced at its "API level" by another component more or less instantly. For the purpose of this project it does not have to be "free", publicly documented or self-made.

The reason for this is simple: many components are too complex to be manufactured completely yourself in a timely fashion, in production quality or within a reasonable budget (and some of them all of this…). But you can tell the components that will lock you in a certain architecture (I only say : cloud, cloud, cloud) or provider and leave them alone.

6.1. Appartment server

A "simple" home automation device with initially the following tasks

- Control lighting via push buttons
- Control shutters via push buttons
- Control heating via thermostat and some "simple" rules

Clearly, this has the potential to grow….

6.2. Basement server

This one will eventually provide the connectivity to the whole wide world, allowing for remote operation of the complete system.

Second, I want to provide door and house communication via this device.

Last not least one can setup more central services for all participants and control for HVACR components.

7. Basic tools

7.1. Soldering iron

If you too want to build the driver component yourself, you will need an electronic soldering iron. This has not to be something special, we will not solder SMDs or expensive chips.

Having an iron at hand will be reasonable anyway if you plan to do tinkering with electric components yourself.

7.2. Copper Wire

For my project I needed two types of copper wire.

Jumper Wire (or hook-up wire?), 0,8 mm diameter with plastic insulation. This is used for wiring the low voltage components within the electric distribution.

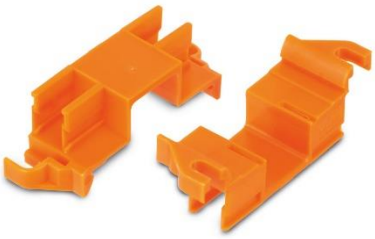
Jumper wire with coating. 0,28 mm diameter. This is used for wiring the electronic components on the proto board.

In this project we will deal with 24V and 5V components and currencies up to 500mA (that will sum up, for sure).

7.3. Cable Connectors

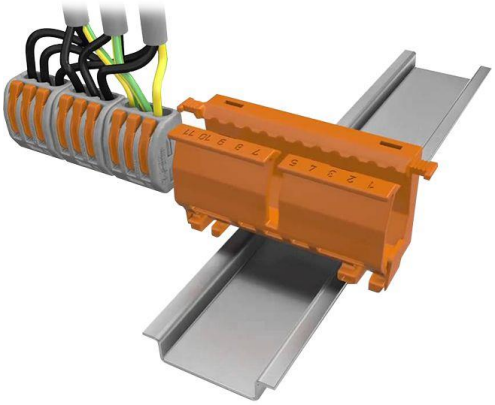
For patching the communication and other low voltage cables there is a simple connector system from “Wago”, series 243.

The Wago 243 connector. You can get this in different colors and sizes.



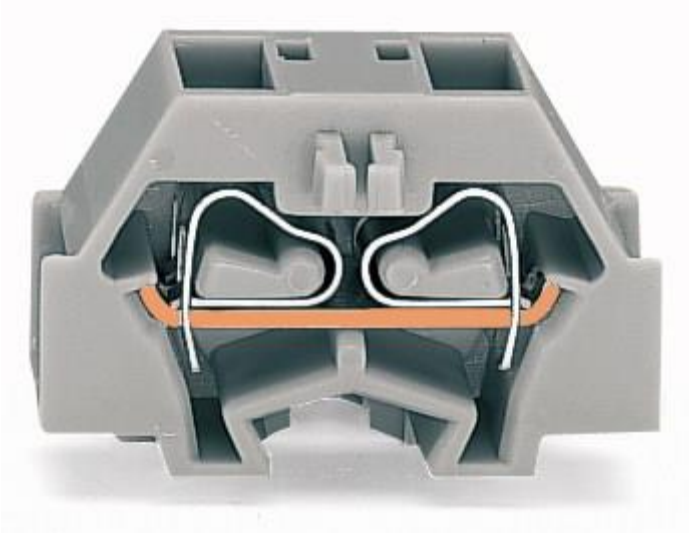
The Wago 243 holder is a great tool to mount the connectors on a DIN rail.

For patching the 240V lines I used the Wago 222 series, the 3 and 5 slot ones.



Again, the Wago 222 has a holder to mount – wherever you want.

Another very practical item is the WAGO “miniature” terminal block, e.g. 260-331.



There are a couple of other parts in this series that make life easier, just look through the catalog. I’ve used these items successfully for wiring the heating valves. As DIN rail mounts are available, using them in the cabinet for patching is another “hot spot” for the parts.

8. Appartment server

8.1. Intro

The apartment server will control the internals of a single unit. Its complexity is “modest”. We will only provide basic control, no sophisticated automation so far. It’s the modern, scalable adaption of a classical apartment installation.

First, we have a look at the hardware components, then we select and install a software stack. Finally we make some tweaks that I consider “basic requirements” for a production system.

8.2. Hardware for the server

For the central platform of this project we have the following constraints

- price tag
- power consumption
- availability of software
- availability of hardware
- availability of advice
- interoperability features
- stability/reliability

It’s not very hard to come across the Raspberry Pi seeing this list. I must admit, I am not a microcontroller or single board computer nerd. The selection process was finally driven by the question “availability” of all kind. Other SBCs may be better suited (and may be are interchangeable in the design to come). But, whatever software and hardware component you may want to use, if you don’t find a tutorial for the Pi, you will find none.

The greatest disadvantages (let’s name it challenges) I found so far for this platform:

- stability/reliability
  Based on the SD card as filesystem, one can expect failures on a regular base
- USB
  The USB connectivity for the Pi is known to be a weak spot. One may expect outages if network communication and other USB controlled communication will exceed a certain threshold.

8.3. Power supply

8.3.1. Power supply

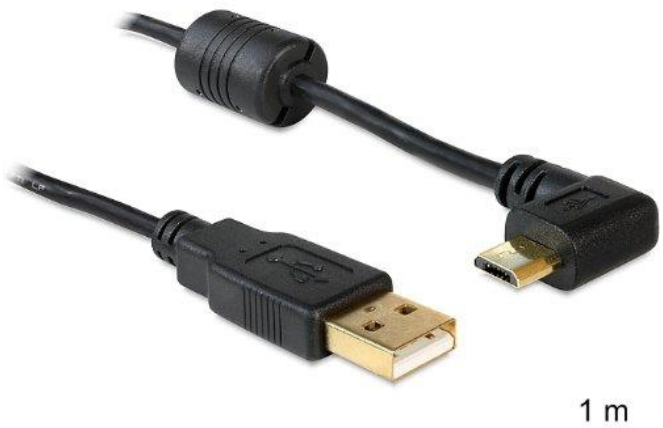
A major concern of this project is stability and as such everybody really recommends a good power supply. Using the Pi in a central installation gives you the added benefit of using a DIN rail component like the Meanwell DR-60-05. This should be enough to serve for all 5v components planned so far in the “rack”.

Here you can see a “preview” for the new electric distribution with the power supply. The power supply on the left, a 24V will drive the relays.

In addition, the internet advice is to always connect the Pi via the USB plug, this ensures leveraging the fuse and some magic on the Pi’s board take care of good “vibrations”.

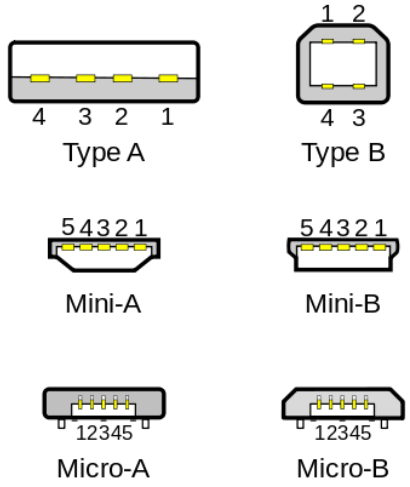
8.3.2. *Cabling*

The PI needs power via USB cable (you may opt to power via the GPIO Pins, but this is not easier in this case and seems to bring some issues if you do so). So, simple solution is to buy some preconfigured USB, cut the host adapter and patch the power line to the 5V supply, using the Wago 243 “distribution” (you can see on the left of the supply).



You will most probably find that the cables are not suited to be patched directly – this is the first time you will have to heat up the soldering iron and add some copper wire at the end.

For your reference I enclose the connector pinout here.



USB 1 standard pinout

Pin	Name	Color	Description
1	V bus	Red	+5V
2	D-	White	Data-
3	D+	Green	Data+
4	GND	Black	Ground

USB micro pinout

Pin	Name	Color	Description
1	V bus	Red	+5V
2	D-	White	Data-
3	D+	Green	Data+
4	ID		USB OTG ID
4	GND	Black	Ground

8.4. Push Buttons / Digital Input

Even in the age of smartphones you will not omit plain buttons for lights and shutters (at least if you want to avoid trouble with your sweetheart).

I looked around a lot for this one and it is not easy to decide:

8.4.1. Direct wiring

One can setup a wire based scenario, using “cheap” buttons that finally switch some GPIO directly, preferably using 24V technique. Every button is connected to a GPIO line directly. In this small use case with around 10 switches planned upfront it is a viable solution. Performed correctly one fine day you may switch the 1:1 cabling to a bus system, so there’s an upgrade possibility.

The greatest advantage of this solution (at least for my wife) was: if anything goes wrong, one can still switch to a more conservative solution later on.

The drawbacks:

- you still pay for the cabling, which is not so cheap if you don’t do it yourself.

- you loose a great deal of flexibility – you have to decide upfront how many buttons you need and where they will go finally
- it's not scalable (you need a single cable for each button planned)
- it's still homegrown (not the buttons and infrastructure, but the central)

8.4.2. *Bus wiring*

Next one is a bus system. Using KNX is an option here, but not if you want to install a "cheap" solution (there may be other opinions on this..).

There are also a couple of interesting "proprietary" solutions (e.g. Eltako and Homematic wired) and if it wasn't for the fun of the project, I would have chosen it. There's lot of information around, of the shelf products are available.

More interesting is the possibility of using an "open" bus system like Modbus, RS485, CAN or OneWire. The greatest problem here in my opinion is the availability of the button hardware itself. I didn't find any off the shelf product. One can (must) design his button and the bus endpoint logic himself. While there's lot of information available this will result in lot of work for creating you proprietary button yourself, besides the fact that this button is **really** not cheap finally.

Don't forget that you have to design the central gateway of the bus to the server also.

The advantage of bus wiring for me is the reliability while we still have a scalable solution (if you call it scalable that you **can** add another component, but you still have to tear apart your wall…).

This would have been the solution if I had unlimited time, I think. But I don't have…

8.4.3. *Radio*

Again there is a very wide choice of solutions.

Homematic, FS20, Zigbee, ZWave, Enocean,… Countless providers for radio solutions and every day more…

To be honest, I didn't test and setup a prototype for all of them, but I think important criteria is

- Power consumption
  You won't get happy if you have to switch batteries 4 times a year…
- Reliability
  Pressing a button should switch the light. Every time.
- Range
  And don't forget to differentiate between the nominal and the real one. Take into account the specific anatomy of your building.
  Maybe you should consider making real measurements – it may seem that the devices are up and running. But in reality the connection quality may be so bad that numerous retransmissions are necessary, rapidly destroying your overall bandwidth.
- Scalability
  The different technologies differ in the way they use the radio band und the legal limitations to do so. In a small apartment this may be neglected, but mid sized or great installations might have to take action to circumvent the problem.
  Some technology comes along with built-in repeater features, some technology does not provide such things at all.

- Component availability
  Best is: all components, sensors and actors, are available from your preferred technology. But, as you will see, thanks to gateways and freely available software, this is not a real problem..
- Gateway availability
  Going for a SBC and open source controlled system, this is a real showstopper. Be sure there is a component you can plug into your SBC along with the appropriate drivers for your platform.
- Number or size of providers
  Personally I would not mind going for a new gadget that may get lost in 2 years. But a commercial grade project for three apartments has a lifecycle of at least 10 to 20 years (I hope…).
- Price
  Well…
- Design
  As you like…

8.4.4. *Conclusion*

For this project I choose Enocean based buttons. The reasoning:

- Power consumption
  Well, it's "self contained". Power is harvested via a piezo element upon button press.
- Reliability
  It's an old and widespread technology, so I hoped that in this small scale project I will not meet any issues (which is not really true so far).

```
Time Travel

As of today, Enocean is not really without problems. One of the original
requirements "push a button triggers an action – every time" is not really
true. Sometimes it is necessary to repeat a button press to get it recognized.
That's a bit annoying but not really a showstopper.

More of a problem was the unexplicable degradation of a single button/receiver
combination. Only after changing the receiver stick, things got better.
```

- Range
  Range as specified and tested is enough in my max. 10m, single floor scenario.
- Scalability
  There exist really large installation, so I do not mind this one.
- Component availability
  There's a broad range of components from different suppliers.
- Gateway availability
  There are even different hardware gateways for the Pi.
- Number or size of providers
  See above.
- Price
  This are not the cheapest ones, especially in comparison with some other 433 MHZ technology, but from time to time you can hit a special offer.
- Design
  It's OK – and you can integrate to other standard (55mm) providers.

So here it is:

A plain old button – besides the interesting fact that it is radio based.

The back is even more interesting (and yes, I know, one should not show the serial). Here you find all the information to be applied when we integrate the button in the software.

This is the official Enocean USB adapter.

```
Time Travel

Maybe today i would evaluate implementing radio based buttons using the
ESP8266 – an inexpensive microcontroller with on board WIFI. This would fit
perfectly in a HA design and the component may be used for other tasks, too.

It has all kind of IOs on board, compare it with a very cheap Arduino with
built in WIFI
```

8.5. Thermostat / Analog Input

8.5.1. Requirement

In Germany one is legally forced (!) to provide a thermostat unit for each (!) room – even if we have a floor heating as in our project. Anyway, my unit must have a temperature sensor, a display and some means to enter the target temperature.

8.5.2. Direct wiring

Again, in theory you have the option of wiring a such a device directly. In practice I do not know of any unit that fulfills the requirements and has a "public" protocol that I could use with the Pi.

For sure you can fall back to the countless OneWire components with regard to sensors. In this case you have to find an alternative solution for entering the temperature (see below).

8.5.3. Radio

There's a bunch of (cheap) radio thermostats – but no public documentation for the protocol. So, if you find some, get it..

There are some enocean based units – but they are really expensive. As I need 12 of them, I skipped this option.

Finally I found a good offer for the Homematic thermostat. A cute unit with all requirements and even humidity sensor. The drawback is, that I have to add another gateway to my Pi – but that's fine anyway. It's not too expensive and now we have access to the two most used radio technologies in Germany (today).

8.5.4. Alternative

Instead of distributing a complete sensor/actor component in every room you may look at the option of including a central control panel. E.g. there are countless cheap options for a TFT touch screen in any size.

Then you can fall back to simple thermostat sensors in every room, while the temperature selection is available only on the control panel.

Such a panel can range from a simple numeric display with some buttons over a computer connected touch display (as a "console") to a remote browser client, again with different hardware options.

While I plan to have a look at such an option later on, in the first phase of the project I will stick with a console-less approach.

```
Time Travel

Displays and tablets get cheaper and cheaper. Maybe today I'd evaluate a
complete tablet based frontend and simple sensors in each room. While this
will involve more software design on the other hand you get a frontend for all
other items in your installation, too.
```

8.5.5. Conclusion

The conservative approach: we take a pack of these

Homematic Thermostat (HM-TC-IT-WM-W-EU).

Homematic USB adapter

8.6. Relays / Digital output

Next task is the interaction with the output side. This is a relatively small installation, so we do not need a lot of outputs (you will see, the 16 GPIOS used later will be enough for me). If this is not the case, a multiplexing solution is more appropriate.

Here in the first step we choose a straight forward solution:

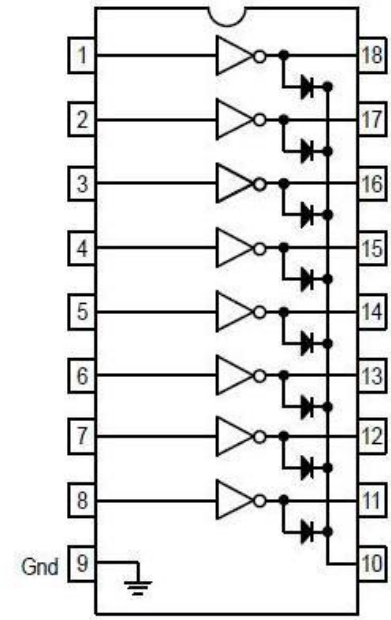
- Use 16 GPIO pins for output
- Run every output through an amplifying stage – here a darlington arry
- Connect the darlington output to either the terminal component (if output constraints are satisfied) or drive a relay.

8.6.1. *ULN 2803 APG*

Controlling relays or other components means nearly always driving currencies that are too high for a GPIO pin. There's lots of discussion in the forums on which solution will fry the pi and which will work. I think the best way to go is: make it "right" and make it flexible.

Still you will find several solution for this problem, one of them is using a darlington transistor or in this case an array of it.

The ULN 2803 takes care you don't fry your Pi. It allows for up to 50V, 500mA per Output and as such, with a price tag of ~ 70 Euro Cent, it is suitable as a joker for nearly all IO. Btw. there are some similar chips to this one, even cheaper, with comparable capabilities. Just look around for finding good tutorials.

IN 1		OUT 1
IN 2		OUT 2
IN 3		OUT 3
IN 4		OUT 4
IN 5		OUT 5
IN 6		OUT 6
IN 7		OUT 7
IN 8		OUT 8
GND You need to connect Pi and secondary power GND		5V to 50V DC

Some more advantages:

- The chip allows to work with "active high" logic from the GPIO
- You have built in protective resistors on the input, one pulling to ground and one constraining input current (see datasheet schematic diagram).
- You have built in protective diodes on the output, so driving a relay or motor is fine

And some advice:

Keep in mind, that while you may use the 5V from Pi's power, consuming too much current will make the Pi instable or completely dysfunctional. If you need the chip to decouple and protect the Pi, chances are good that you should use a separate power supply anyway.

Remember to always provide common ground to Pi, ULN2803 and secondary power.

The concrete use of this chip in my project is multipurpose. On one hand this should drive high voltage relays (see beyond), on the other hand I want to drive heating valves

directly. Some outputs will remain unused, but the multipurpose chip will surely fit in all output scenarios to come.

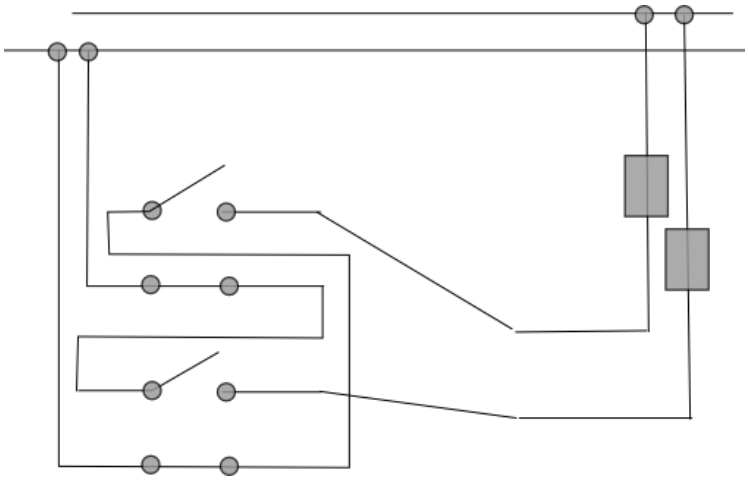
8.6.2. *Eltako Relay*

The power lines are switched using plain relays for mounting in the service cabinet.

here the R12-100 for switching light and comparable und the R12-110 for switching the shutters. I selected the 24VDC type, needing < 100mA.

Using the R12-100 type is straightforward. The control pins are connected to a GPIO and 24V.

The R12-110 controls the shutter motor, you need one for up and one for down. The R12-110 has an “opener” and a “closer”. This feature is used to forestall switching both circuits on. Here’s the wiring scheme



These relays are under heavy load, especially when reversing up and down in short period. You really should add mechanisms in the control software to delay for 200-400 ms between changing direction.

8.6.3. *Heating Valve*

The heating valves are 24VDC, the power consumption should be <100mA (Danfoss `088H3141`)

The valves are “normally open”, meaning that a correctly installed heating system should never need any power. In case of failure the heating is on.

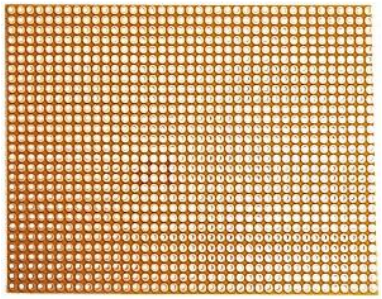
8.6.4. *Driver module*

The “driver module” is a simple connector for the Pi to the outside world, based on the ULN2803. I was eager to learn some details, so I decided to start this component from scratch.

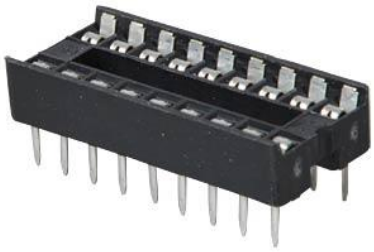
All in all I can not recommend following this strategy: It’s a lot of work if you don’t have a PCB, it’s error prone and it’s not really cheap. In some later chapters I will talk about some alternatives.

That said, let’s get together the components we need (besides the basic stuff mentioned in the beginning).

We have two ULN2803 for a total of 16 “amplified” IO ports. That’s enough for me for the moment, controlling 4 heat valves, some lights and some shutters.

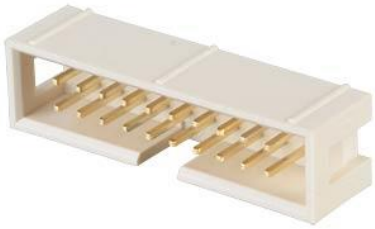


We have the prototyping board,



two IC sockets for the ULN2803,

some screw terminals. These are used for external power supply and all outputs.

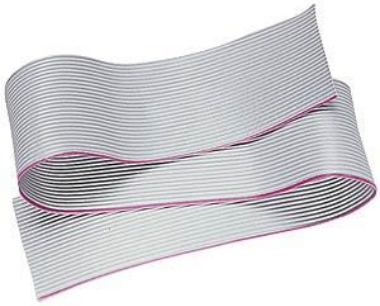


A 20 pin male connector. This is used for connecting the components inputs.

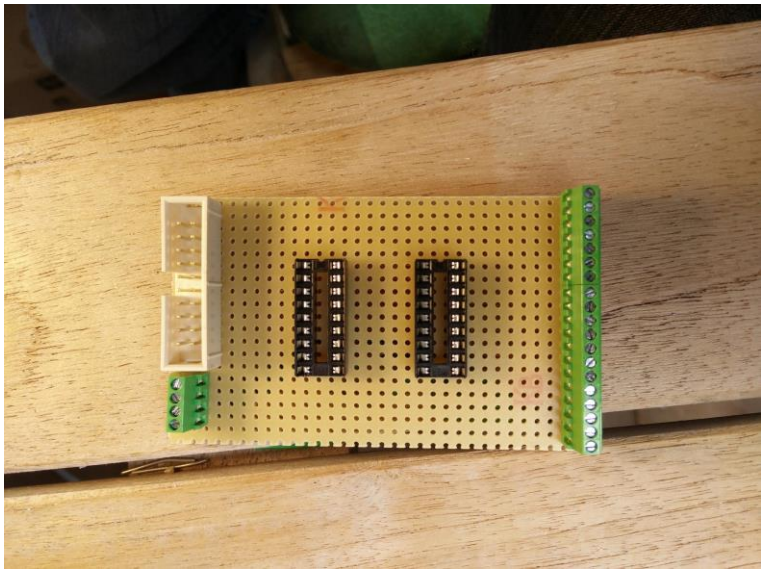
A DIN rail case, 3 units

A 20 pin female connector for the component input.

A 40 pin female connector for the Pi GPIO.



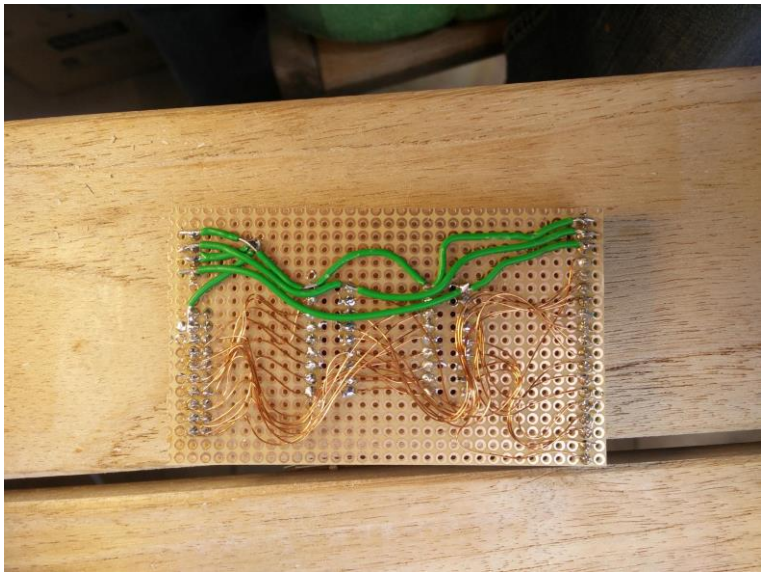
A ribbon cable, 20 cores



The module is set up on a generic prototyping board and deployed in a din rail box. The input side is a 20 pin board connector for the 16 GPIOS and GND and 4 small clamps for the secondary power. Output power ULN2803 can be supplied separately this way.

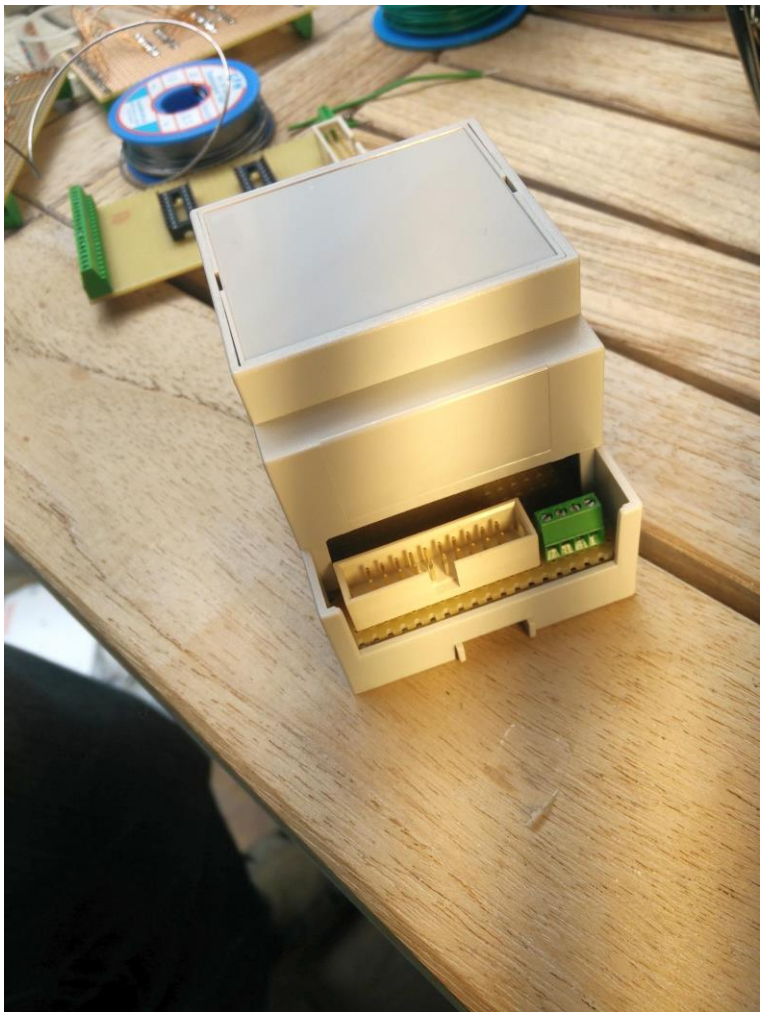
The output is 19 small clamps (well – they just fitted in a 3 unit din rail..) for 16 power outputs, common ground and the two secondary power inputs.

In the middle we have the two ULN2803 (on a socket, accounting for both my poor soldering abilities and the possibility that I may fry one of them later on). The “top” one, near to the input lets call “A”, the other “B”.

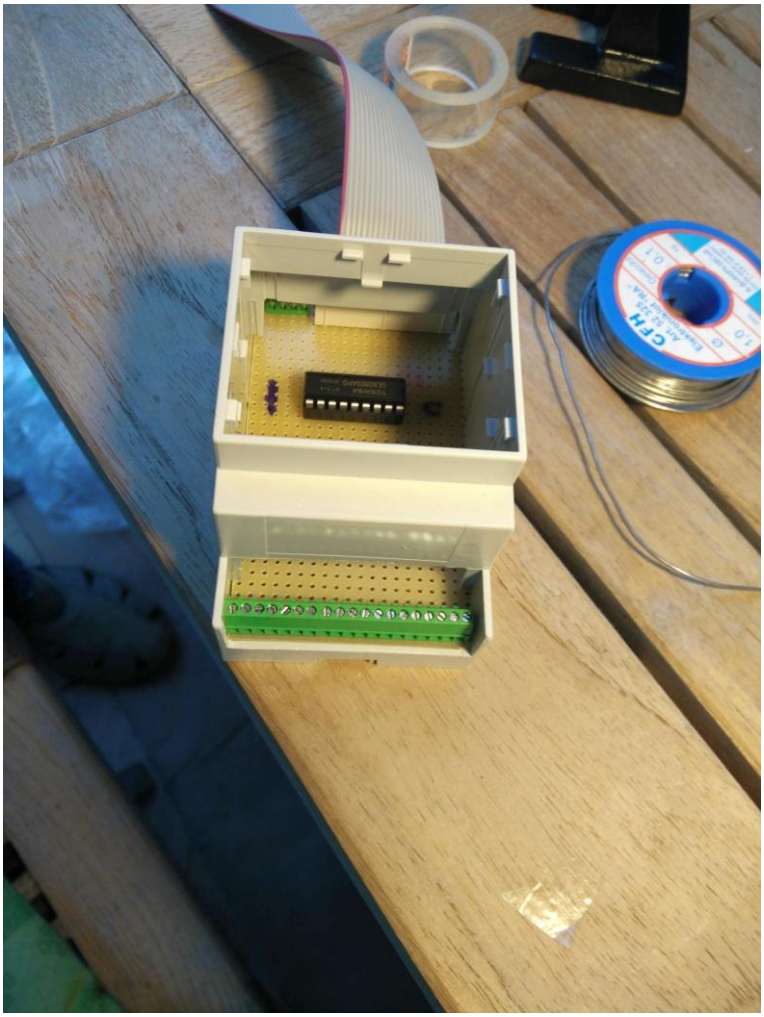


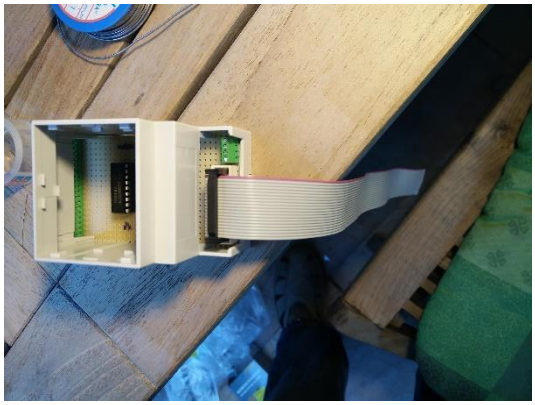
For your amusement I show the soldering side here. It's ok for me, but I can testify that these are the most expensive modules you can have. For me it was at least 2 hours per unit, 5 units in total.

Keep in mind that the overall current may be quite high and use appropriate cables for GND and plus side.

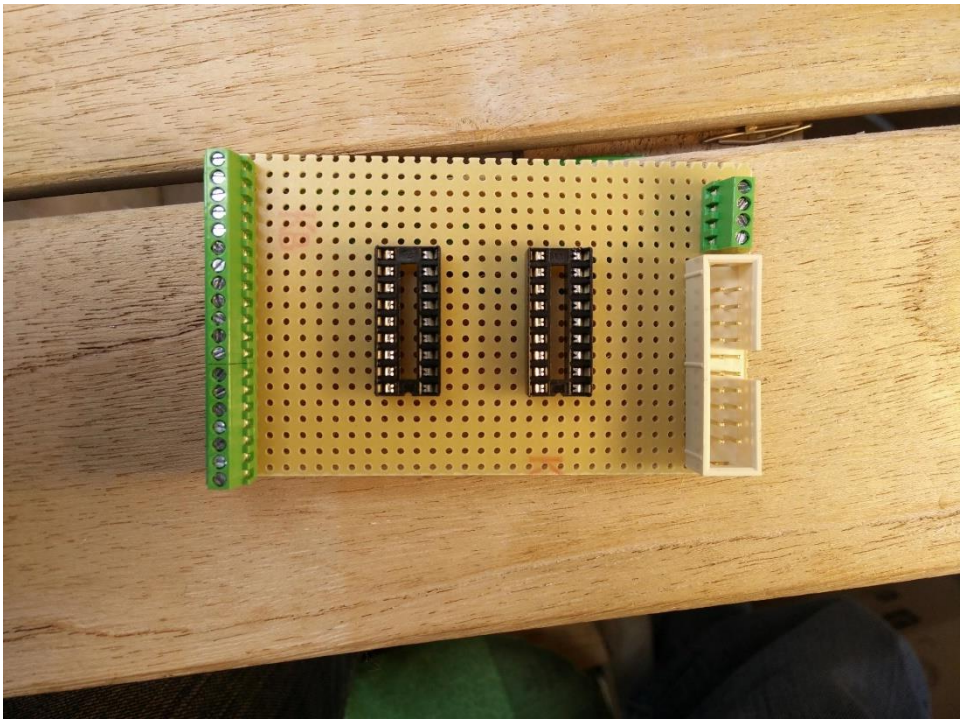


In the din rail housing, where you can't see the nasty details it already looks a little professional.





a Wiring scheme



In the following A and B reference the two ULN2803 chips.

The input power side (green clamp, upper right), numbered from top to bottom

1	GND
2	A +
3	GND
4	B +

The board connector of the “driver module” is connected as follows (where 1 is on the upper left on this picture).

-	1	2	GND
-	3	4	GND
B IN 8	5	6	A IN 8
B IN 7	7	8	A IN 7
B IN 6	9	10	A IN 6
B IN 5	11	12	A IN 5
B IN 4	13	14	A IN 4
B IN 3	15	16	A IN 3
B IN 2	17	18	A IN 2
B IN 1	19	20	A IN 1

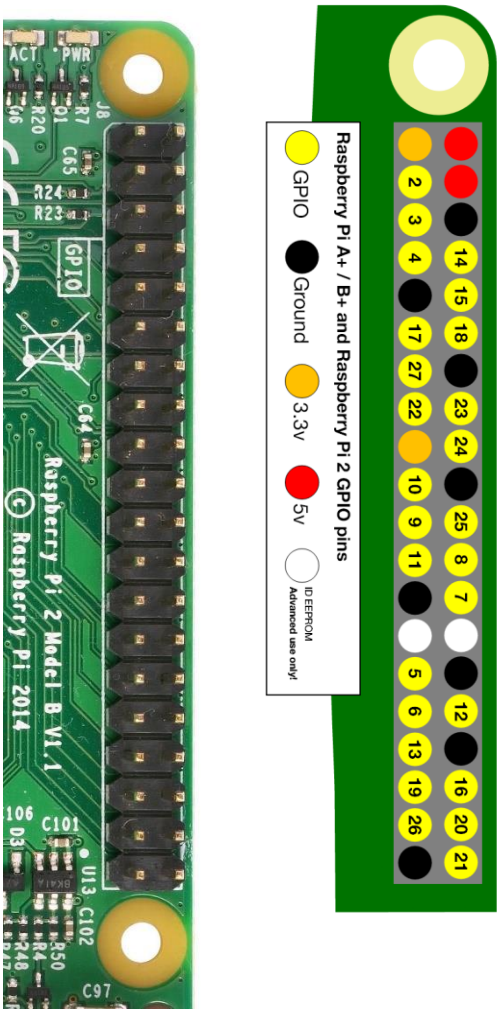
And the clamps on the output side (numbered seen from the top on the picture above)

1	GND
2	A +

3	B +
4	A OUT 8
5	A OUT 7
6	A OUT 6
7	A OUT 5
8	A OUT 4
9	A OUT 3
10	A OUT 2
11	A OUT 1
12	A OUT 8
13	B OUT 7
14	B OUT 6
15	B OUT 5
16	B OUT 4
17	B OUT 3
18	B OUT 2
19	B OUT 1

8.6.5. *Connecting the Pi*

Let's look at the Pi, this is the pinout of the connector.



	PIN	PIN	
3.3V	1	2	5V
GPIO 02 (I2C)	3	4	5V
GPIO 03 (I2C)	5	6	GND
GPIO 04 (GCLK)	7	8	GPIO 14 (TXD0)
GND	9	10	GPIO 15 (RXD0)
GPIO 17 (GEN0)	11	12	GPIO 18 (GEN1)
GPIO 27 (GEN2)	13	14	GND
GPIO 22 (GEN3)	15	16	GPIO 23 (GEN4)
3.3V	17	18	GPIO 24 (GEN5)
GPIO 10 (MOSI)	19	20	GND
GPIO 09 (MISO)	21	22	GPIO 25 (GEN6)
GPIO 11 (CLK)	23	24	GPIO 08 (CE0)
GND	25	26	GPIO 07 (CE1)
ID_SD	27	28	ID_SC
GPIO 05	29	30	GND
GPIO 06	31	32	GPIO 12
GPIO 13	33	34	GND
GPIO 19	35	36	GPIO 16
GPIO 26	37	38	GPIO 20
GND	39	40	GPIO 21

Detailed information on the Pins is available e.g. at http://elinux.org/RPi_BCM2835_GPIOs.

You can use any of the GPIO Pins, but selecting carefully may leave you the option to add other features later on. The ones selected for this project are rendered in green.

For the driver module board connector I "manufactured" a connector cable from the above GPIOs. This is the board connector wiring scheme.

- (Red cable)	1	2	GND
-	3	4	GND
GPIO 21	5	6	GPIO 20
GPIO 26	7	8	GPIO 16
GPIO 19	9	10	GPIO 13
GPIO 12	11	12	GPIO 06
GPIO 05	13	14	GPIO 25
GPIO 24	15	16	GPIO 23
GPIO 22	17	18	GPIO 27
GPIO 18	19	20	GPIO 17

The end to end connectivity on the driver module output clamps (numbered as above) with this configuration is:

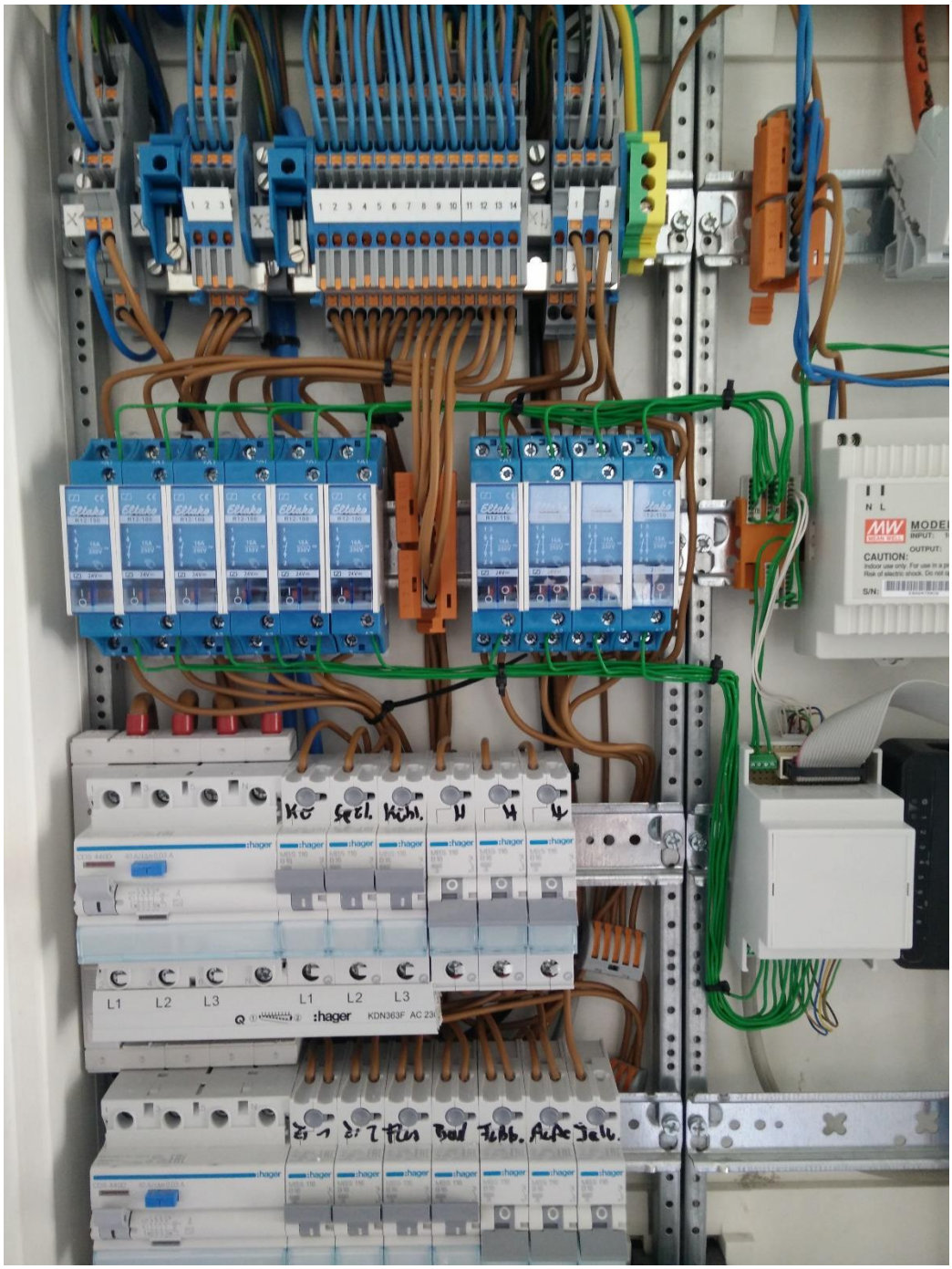
1	GND
2	A +
3	B +
4	GPIO 20
5	GPIO 16
6	GPIO 13
7	GPIO 06
8	GPIO 25
9	GPIO 23
10	GPIO 27
11	GPIO 17
12	GPIO 21
13	GPIO 26
14	GPIO 19
15	GPIO 12
16	GPIO 05
17	GPIO 24
18	GPIO 22
19	GPIO 18

8.6.6. *Distribution Box Patching*

Now we have to define a correspondence between the physical power lines and valves and the GPIOs.

The electrician was a kind one, he provided terminal blocks for every power line to the rooms. Power is distributed from the terminal blocks to the rooms in a star topology, power is switched centrally via relays.

The power line is either patched directly to a corresponding fuse (for wall outlets) or pathed to one of the relays. The relays power input is patched to the fuse for the power line. The control input (24V) is connected to the driver module.



So, even if this is not of special interest for your project i document the terminal block layout here – I recommend to do so yourself. The day you will need this table for your reference is near…

a

Floor 1

Block	Terminal	Relay	Target
1	01	-	Oven
	02	.	Oven/ Oven
2	01	.	kitchen
	02	.	kitchen / washer
	03	.	kitchen / fridge

3	01	.	roomL
	02	.	roomR
	03	.	hall
	04	.	bath
	05	.	heating
	06	.	terrace
	07	R1	kitchen
	08	R2	roomL
	09	R2	roomL
	10	R3	roomR
	11	R3	roomR
	12	R4	hall
	13	R5	bath
	14	R6	terrace
4	01		shutter left N
	02	R7	shutter left grey = up
	02	R8	shutter left black=down
	03		shutter right N
	04	R9	shutter right grey = up
	04	R10	shutter right black=down

Now you can map the power lines to the driver output. In the table below you already see the technical names for the lines that are used throughout the home automation installation from now on.

The name means for example “on floor 1, the kitchen light with index 0”. With this table (power line on the left and GPIO on the right) we are able to program the openHab items.

Target	Driver module	GPIO
wbf1_kitchen_light0_state	4	GPIO 20
wbf1_roomL_light0_state	5	GPIO 16
wbf1_roomR_light0_state	6	GPIO 13
wbf1_hall_light0_state	7	GPIO 06
wbf1_bath_light0_state	8	GPIO 25
wbf1_terrace_light0_state	9	GPIO 23
wbf1_roomL_shutter0_up	10	GPIO 27
wbf1_roomL_shutter0_down	11	GPIO 17
wbf1_roomR_shutter0_up	12	GPIO 21
wbf1_roomR_shutter0_down	13	GPIO 26
wbf1_roomL_valve_state	14	GPIO 19
wbf1_kitchen_valve_state	15	GPIO 12
wbf1_bath_valve_state	16	GPIO 05
wbf1_roomR_valve_state	17	GPIO 24
	18	GPIO 22
	19	GPIO 18

b Floor 2

Block	Terminal	Relay	Target
1	01	-	Oven
	02	.	Oven/ Oven

2	01	.	kitchen
	02	.	kitchen / washer
	03	.	kitchen / fridge
3	01	.	roomL
	02	.	roomR
	03	.	hall
	04	.	bath
	05	.	heating
	06	.	terrace
	07	R1	terrace
	08	R2	kitchen
	09	R3	roomL
	10	R3	roomL
	11	R4	roomR
	12	R4	roomR
	13	R5	hall
	14	R6	bath
4	06		shutter left N
	07	R7	shutter left grey = up
	07	R8	shutter left black=down
	10		shutter right N
	11	R11	shutter right grey = up
	11	R12	shutter right black=down

Target	Driver module	GPIO
wbf2_kitchen_light0_state	4	GPIO 20
wbf2_roomR_light0_state	5	GPIO 16
wbf2_roomL_light0_state	6	GPIO 13
wbf2_hall_light0_state	7	GPIO 06
wbf2_bath_light0_state	8	GPIO 25
wbf2_terrace_light0_state	9	GPIO 23
wbf2_roomR_shutter0_up	10	GPIO 27
wbf2_roomR_shutter0_down	11	GPIO 17
wbf2_roomL_shutter0_up	12	GPIO 21
wbf2_roomL_shutter0_down	13	GPIO 26
wbf2_roomL_valve_state	14	GPIO 19
wbf2_kitchen_valve_state	15	GPIO 12
wbf2_bath_valve_state	16	GPIO 05
wbf2_roomR_valve_state	17	GPIO 24
	18	GPIO 22
	19	GPIO 18

c Floor 3

Block	Terminal	Relay	Target
1	01	-	Oven

	02	.	Oven/ Oven
2	03	.	kitchen
	04	.	kitchen / washer
	05	.	kitchen / fridge
3	01	.	roomR
	02	.	roomL
	03	.	kitchen
	04	.	hall
	05	.	bath
	06	.	heating
	07	.	terrace
	08	R1	kitchen
	09	R2	roomR
	10	R3	roomL
	11	R1	kitchen
	12	R4	hall
	13	R5	bath
	14	R6	terrace
4	06		shutter left N
	07	R7	shutter left grey = up
	07	R8	shutter left black=down
	08		shutter middle N
	09	R9	shutter middle grey = up
	09	R10	shutter middle black=down
	10		shutter right N
	11	R11	shutter right grey = up
	11	R12	shutter right black=down

Target	Driver module	GPIO
wbf3_kitchen_light0_state	4	GPIO 20
wbf3_roomR_light0_state	5	GPIO 16
wbf3_roomL_light0_state	6	GPIO 13
wbf3_hall_light0_state	7	GPIO 06
wbf3_bath_light0_state	8	GPIO 25
wbf3_terrace_light0_state	9	GPIO 23
wbf3_roomL_shutter0_up	10	GPIO 27
wbf3_roomL_shutter0_down	11	GPIO 17
wbf3_roomR_shutter0_up	12	GPIO 21
wbf3_roomR_shutter0_down	13	GPIO 26
wbf3_roomR_shutter1_up	14	GPIO 19
wbf3_roomR_shutter1_down	15	GPIO 12
wbf3_roomL_valve_state	16	GPIO 05
wbf3_bath_valve_state	17	GPIO 24
wbf3_kitchen_valve_state	18	GPIO 22
wbf3_roomR_valve_state	19	GPIO 18

8.7. Software stack

8.7.1. *Intro*

This is the software stack to run my apartment server.

Basic requirements are:

- run unattended
- run 24/7
- reboot completely after power down
- do not allow unauthorized access
- maybe some day detect failures and reboot

8.7.2. *Raspbian*

This is the most simple choice. I didn't look for an alternative to deviate as little as possible from the widespread know how on the net (and found it was wise to do so). Even with upgrading at some point from this "Debian wheezy" based image to a "Debian Jessie" distribution I had incompatibilities that I was not able to resolve with my basic Unix know how.

Most information for the Pi and most pre-built software components use this one.

There are tons of installation manuals to do this, I will not repeat the steps in detail – only some advice for the uninitiated:

- Use high quality SD cards
- Follow the basic installation steps
    - Download image
    - Copy to card
    - Launch Pi
    - Resize Image
    - Do internationalization stuff
- Now you are fine and ready to take off. But I recommend to come back after playing around for some more detail steps (see chapter beyond) – most of them quite useful
    - Clean your image from unused stuff
        - Games/Learning stuff
        - X11
        - ..
    - User administration
    - Set a Static IP
    - Read Only SD card
- Make a backup
- Go on…

8.7.3. *Hmland*

This installation manual is in **correct** (layered) order, so "hmland" is first. This requirement stems from:

- I want to use openHAB for control
- I want to use Homematic devices
- openHab does not have a builtin engine to control this stuff, it always needs a native device to do this. And i don't want another CCU.

- So I need homegear, an open source reimplementation of the Homematic software, running on the Pi, too.
- homegear does need a “physical” device to talk to the Homematic endpoints. This is some radio chip. Again, this may be embedded in a Homematic device like the LAN adapter, USB stick or a directly soldered CC1101 radio chip.
- I decided for a simple Homematic USB stick. At this moment it was cheap, there exists a fallback scenario (use the stick in another controller) and it was few work (I thought so..).
- This stick can not be controlled by homegear directly
- This is where hmland comes into play. Some enlightened guy has a module that controls the stick and behaves like a Homematic LAN adapter, which you can use in homegear, which is needed by openHAB. So easy.

hmland is not prebuilt for the Pi, but even me was able to do it in minutes. Follow the instructions and everything is fine. If compiled and moved all the stuff to

```
/opt/hmcfgusb/
```

Some caveats:

- hmland should start as a daemon ???, do the init.d stuff
- You can use “hmland –r” to do a fast debug
- Letting hmland serve only on the loopback (127.0.0.1) is a good idea. What happened to me one day was that the loopback interface disappeared (from /etc/network, dunno why) and hmland didn’t start any longer. It takes some time to find the reason, maybe you are warned.

8.7.4. *Homegear*

In the chapter before we motivated already why we need homegear. I must say this is a nice and powerful piece of software itself. The forums are responsive and development is active.

We simply use it as a gateway from openHAB to Homematic devices – this is by far only a piece of its features. If we’d skip the requirement for Enocean compatibility (and the option to support a lot of more bindings), we would have easily stopped with our software stack at this point.

The install of the pre-built Pi package is effortless. Setup is done in /etc/homegear, log is written to /var/log/homegear/ by default.

The working data set is found in /var/lib/homegear, most importantly the device databases. Consider these when setting up backups.

One thing you may consider:

- Enhance the init.d script to require “hmland” in the startup

8.7.5. *Java*

openHAB is a Java application, we will need an up-to-date installation. I choose and recommend the Oracle JDK.

8.7.6. *openHAB*

openHAB should be the workhorse for the system. With a Pi 2 I assume there's plenty of memory and CPU for this quite big component.

This is a central hub (pun intended?) for a huge set of so called bindings. Bindings abstract the source and sink of sensor and actor communication and allow for the routing of information via rules.

This way I can get an event from an Enocean component and route it to a GPIO based relay actor, the same way with the information from a Homematic thermostat to a GPIO based driver for an electric valve.

Besides fulfilling this basic integration requirement, openHAB leaves tons of possibilities to scale the solution up own day:

- call external web services
    - calendar based control
    - notification
- internal web services
    - control any feature via web service
- integrate other actor / sensor communication protocols
- integrate system level via "exec"
- time based events
- persistence and monitoring
- web ui

One word of advice: for this installation I used version 1.7.2. Most development effort is spent on the upcoming version 2.0. With this background information and some playing around with the software you can quickly get the impression that you're on the dead end of an initial design prototype. The community has collected a lot of knowledge and ideas, that now are realized in a "completely" new product.

So the bad news is that many issues on the 1.7.2 version will never get fixed or urgent features will never be implemented. You will have to work around different issues and you will fight with suboptimal design decisions.

The good news is – I still think this a very good idea and I hope that 2.0 will bring a lot of compatibility along with solutions for all the nasty ticks of the current version.

```
Time Travel

At the point of this writing 2.0 is entering beta, what a pity that I'm not
able to switch the installation and make my tenants beta testing… but you
know, never change a running system…
```

The installation of 1.7.2 itself is not as straightforward as one may think. There are at least two "mainstream" installation instructions. One works by "apt-get" the installation, but this one didn't work for me. Manual installation using the "wget" approach worked fine, but you have to set up some things yourself, most importantly the init.d scripts.

8.8. Configuration details

8.8.1. *Raspbian*

Maybe it's not so obvious, so a little explanation: I have the following chapters on handling the Pi:

- Installation (above)
  This one is about the most basic steps to get the system running and general advice that is needed on any system. You've got a "multi purpose" Pi now.
- Configuration (this one)
  This is about special setup needed for our apartment server and the software stack we will use here. Things like user setup, GPIO stuff…
- Advanced (beyond)
  Here we **may** dig even deeper to make the Pi even more well suited for an home automation server. It's quite system specific (and you may ruin your system doing it ☺).

8.8.2. *Hmland*

The hmland is quite simple to setup. Any change is made directly in the init.d script.

- port
- logging
- special options

Especially for achieving "low write profile" there's nothing you must do here, the defaults are fine.

8.8.3. *Homegear*

a Configuration

Homegear configuration is done in two files for my scenario.

First, we look at "/etc/homegear/main.conf". Besides logging (see chapter below), for me there was no need for further changes.

The next one will be "/etc/homegear/physicalinterfaces.conf". Here you setup the real devices and communication channels.

I only set up an id and "rfKey", the base for the AES encryption with the Homematic endpoints. Everything else is default with my installation.

```
## The device family this interface is for
[HomeMaticBidCoS]

## Specify an unique id here to identify this device in Homegear
id = wbf2
## Specify a 16 byte (32 characters) long AES key here to protect your
wireless communication
## !!! IMPORTANT: Never ever lose this key.  That would render your devices
useless.
## To remove the key from your devices, you need to factory reset them
# wbbase
#rfKey = 00000000000000000000000000000000
```

As the documentation states, keep this key in a safe place just in case. Loosing the key will render your Homematic equipment useless.

b Important commands

To deal with homegear, you have to setup some configuration on the commandline, as this information is not stored in config files but in a database.

To enter "command mode" type

```
sudo homegear -r
```

while the homegear daemon is already running.

Now you enter the homegear commandline. On any context you can enter “help” to get directives on what you can do.

The first thing to do is selecting the Homematic family of devices (there are short forms of the respective commands, for readability reasons I give only the long forms here)

```
families select 0
```

In the Homematic context you can do some magic with “virtual” Homematic devices, but we don’t need none of this. We want to access the “main” device to handle “peer” gadgets.

```
devices select 1
```

Here’s where we want to work. You can

- list all peers “peers list”
  This gives you a informative list of all peers paired with the device
- reset a paired peer “peers reset <id>”
  You can unpair and remove the peer. The peer is reset to factory state. This is important if you want to add the peer to another Homematic device later, otherwise the AES key is not removed.
- select a peer for further inspection “peers select <id>”
  To go on working with a dedicated peer, you must select it.
- enter pairing mode for new peers “pairing on”
  If you want to add new peers to the device, you should do this using the pairing mode. After enabling pairing mode, for 60 seconds the device scans for peers that enter pairing mode themselves. After the pairing mode is finished, you can look up the peers detected using “peers list”.

c Send a list of all devices to a file

```
sudo homegear -r | tee /home/pi/homegear-peers.txt
```

In the homegear commandline enter

```
families select 0
```

devices select 1

peers list

and you will get

```
>
> families select 0
```

```
Device family "HomeMatic BidCoS" selected.
For information about the family's commands type: "help"
(Family)> devices select 1
Device selected.
For information about the device's commands type: "help"
(Device)> peers list
         ID | Name              |  Address | Serial Number | Type | Type String                | Firmware | Config Pending | Unreach
------------|-------------------|----------|---------------|------|----------------------------|----------|----------------|---------
            |                   |          |               |      |                            |          |                |
          1 |                   |   123450 |     LEQxxxxxxx | 00AD |          HM-TC-IT-WM-W-EU |      1.2 |             No |     Yes
          2 |                   |   123451 |     MEQxxxxxxx | 00AD |          HM-TC-IT-WM-W-EU |      1.2 |             No |     Yes
          3 |                   |   123452 |     LEQxxxxxxx | 00AD |          HM-TC-IT-WM-W-EU |      1.2 |             No |     Yes
          4 |                   |   123453 |     LEQxxxxxxx | 00AD |          HM-TC-IT-WM-W-EU |      1.2 |             No |     Yes
------------|-------------------|----------|---------------|------|----------------------------|----------|----------------|---------
(Device)>
```

d Pairing

Enter the pairing mode for the main Homematic device

```
families select 0
devices select 1
pairing on
```

Now enter the pairing mode for each peer you want to add.

e Database

The database for the devices and peers is written to /var/lib/homegear/db.sql. For my installation i pre-built 3 different device configurations in my lab, not in the production environment.

To do this, I setup all devices for a single installation

- Change RF key
- peer all device
- backup db

Then I “reverted” by

- delete BidCos central device (via homegear commandline)
- create new one
- replay steps above

8.8.4. *openHAB*

a Intro

openHAB is **big**. There’s fewer documentation than there should have been, and I think because of this there’s a lot of third party advice of how to do something. The bad news is that this is often incomplete, outdated or plain wrong.

I will give you the info I have built up so far with no guarantee that this is the best practice way or that it still holds true at the time of your reading..

b Bindings

- homematic
- enocean
- GPIO
- HTTP
- EXEC

c UI

For this installation a UI is not planned immediately. The user will interact using physical sensors. Nevertheless, I created sitemap for “personal use”.

I bet some geeky tenant will show up soon and requesting remote access…

8.9. openHAB Items&Sites&Rules

As openHAB is at the center of all automation here, we have this special chapter that finally puts together the concrete components.

As already said, this is not a really “complex” automation scenario and you can argue that openHAB is a bit oversized. You’re right if you will stop after these initial steps – but I bet you wont.

8.9.1. The great plan

As always it is important to have a “great plan”.

One of my most stressed points in real life is “naming”. You will never get a scalable and maintainable solution if you do not strive for consistent naming. Every change or issue will send you in a nightmare of “wtf”…

One of the caveats in openHAB declarations is the namespacing (a sure indication that this is still on the hobbyist scale..).

Even so you can have different declaration files like “unit1.items” and “unit2.items” all of them live in the same namespace. You can’t simply add a new floor to a central installation by copying the “items” file to a new name, the namespace must be explicit in the items name. There’s no concept of an include with a parameter either.

So, for our project we have to duplicate the item definitions and choose a slightly different name prefix or suffix in each one.

I further recommend using names that seem reasonable compatible to a later integration in scripting environments. This means using only

- a-z, A-Z
- 0-9
- underscore

8.9.2. Items

I recommend using a consistent naming scheme, e.g.

<site>_<group>_<target>_<property>

Example

```
wbf1_kitchen_light1_state
```

site	wbf1 | wbf2 | wbf3
group	kitchen | bath | hall |

	roomL | roomR | terrace | heating | service | <any top level group you think off>
target	switch<n> | light<n> | shutter<n> | therm<n> | valve<n>
property	state | up | down | <other item boolean properties> lowbat| rssi | <other item meta properties> tempAct | tempSet | humidity | <other item sensor data>

8.9.3. *Enocean*

The enocan binding allows to include Enocean push buttons in your installation easily.

All buttons come with an id printed on them – this is the ”id” parameters for the binding string in the item definition, eg. “ab:cd:f0:e3”.

In addition you must declare the enocean item type “eep” (Enocean equipment profile, ???link) (which is “F6:02:01” for the common push button). Enocean is a well documented technology you find all supported item types in the respective specification.

Depending on the item types, additional “channel” and “parameter” arguments may be given.

All in all the syntax for the binding is

```
enocean="{id=<myid>, eep=<mytype> [, channel=<mychannel>] [,
parameter=<myparameter>]}
```

Depending on the openHAB item type a lot of magic is done behind the scenes, you can map the button to a switch, a dimmer or a rollershutter.

a Push button

I only use the push button in my installation, so i only dare to rant about this one.

A push button (of type “F6:02:01”) as described in the Enocean Equipment Profile specification, supports an enumeration of buttons “AI”, “A0”, “BI”and “B0”.

In an unknown logic this transforms to openHAB parameters

- channel “A” and “B”
- optional parameter “I” and “0”

You can map the item to a “Switch” type, with 2 different behaviors.

- enocean="{id=00:00:00:00, eep=F6:02:01 , channel=A}”
  This will result in a switch that updates to on when AI is pressed, nothing happens when the button is released. The switch is turned of when A0 is pressed. You need two physical button sensors to control the switch

- enocean="{id=00:00:00:00, eep=F6:02:01 , channel=A, parameter=I}”
  This will result in a switch that updates to “ON” when AI is pressed, and to “OFF” when the button is released. Nothing happens when A0 is pressed.

8.9.4. *Homematic*

The homematic binding addresses Homematic devices.

a Thermometer

from
https://forum.homegear.eu/viewtopic.php?f=23&t=169&p=1147&hilit=boost_state#p1147

"CONTROL_MODE" ist nur lesbar und zeigt dir den aktuellen Modus an.

"BOOST_STATE" ist ebenfalls nur lesbar und wird als Ereignis gesendet, sobald "BOOST" aktiviert wurde. Die angegebene Zeit ist die Dauer des Boostmodus ab diesem Ereignis.

AUTO_MODE, BOOST_MODE, COMFORT_MODE und LOWERING_MODE sind vom Typ "Action", d. h. sie haben eigentlich keinen Wert. Übergeben musst du aber einen "Boolean" "true". Durch setzen der Variablen setzt du den entsprechenden Modus.

MANU_MODE akzeptiert als Parameter die manuell einzustellende Temperatur als Float, d. h. es wird sowohl der Modus "manuell" aktiviert als auch die manuelle Temperatur gesetzt.

Fehlt noch PARTY_MODE. Da sollte immer PARTY_MODE_SUBMIT verwendet werden, da sonst unnötig viele Pakete über den Äther gesendet werden. Siehe:
https://forum.homegear.eu/viewtopic.php?f=17&t=115&p=736&hilit=PARTY_MODE_SUBMIT#p736

8.9.5. *GPIO*

a Playground

```
cd /sys/class/gpio
sudo sh -c 'echo 17 > export'
sudo sh -c 'echo out > gpio17/direction'
sudo sh -c 'echo 1 > gpio17/value'
sudo sh -c 'echo 0 > gpio17/value'
sudo sh -c 'echo 17 > unexport'
```

b Item definition

Example

```
Switch btnTest “Test” { gpio=”pin:17” }
```

c Caveats

Caused by the way the Pi and openHAB interact with the GPIO you have some things to consider

- Initial GPIO direction
- Initial GPIO value
- GPIO access rights

d openHAB GPIO control

If you do not run openHAB as <root>, you must allow access to the GPIO resources

```
sudo adduser openhab gpio
```

openHAB will really try to release its GPIO resources, but its better not to rely on this, there are enough reasons why you may find dangling state when starting up to always set up GPIO before properly. For the setup defined in this project you should add the following code to your startup script

```
echo unexport GPIO
echo 17 > /sys/class/gpio/unexport
echo 18 > /sys/class/gpio/unexport
echo 27 > /sys/class/gpio/unexport
echo 22 > /sys/class/gpio/unexport
echo 23 > /sys/class/gpio/unexport
echo 24 > /sys/class/gpio/unexport
echo 25 > /sys/class/gpio/unexport
echo 05 > /sys/class/gpio/unexport
echo 06 > /sys/class/gpio/unexport
echo 12 > /sys/class/gpio/unexport
echo 13 > /sys/class/gpio/unexport
echo 19 > /sys/class/gpio/unexport
echo 16 > /sys/class/gpio/unexport
echo 26 > /sys/class/gpio/unexport
echo 20 > /sys/class/gpio/unexport
echo 21 > /sys/class/gpio/unexport
```

8.9.6. Controlling

a Heating

9. Basement server

9.1. Intro

As previously said, this one mainly handles door communication. In the more advanced parts this component will receive additional services (WAN, network file system) for the complete installation.

In these times I simply found it anachronistic to install an expensive proprietary solution that finally will provide less features than a plain telephony based infrastructure.

9.2. Hardware

9.2.1. *Server*

Well, here the same reasoning as in chapter “apartment server” applies. To no surprise we choose a raspberry here.

9.2.2. *Switch*

As we will have a bunch of components attached to the basement server, we will need a little switch. I thought about being clever and take an “oversized” one, having 8 ports at hand.

I decided for no special reason for a EDI ES-3308PV3. Be warned: they are always to small…

At the moment these components are connected:

- The three apartment satellite Pis
- The indoor DECT gateway
- The outdoor VOIP adapter
- The heating

9.2.3. *Doorphone outdoor*

The outdoor part was quite problematic to decide.

There are interesting attempts in the community to create the station completely from scratch ("Doorberry"). But I think there are a some problems to overcome that should not be underestimated

- An outdoor installation has heavy requirements regarding humidity and temperature
- Some complain about poor speech quality, both on the hearing and speaking side.
- The risk of needing "maintenance" on the doorphone (reboot, change SDcard,..) is higher than with a standard product.
- The price difference to a prebuilt module is not that big to justify the risk in my opinion

In short, I wanted a shrink wrapped product.

A proprietary solution was not viable, leaving only an analog or IP based component.

While my initial intention was to go for a completely IP based system, I abandoned the plan simply for pricing reasons. The cheapest solution, based on an EntryCom Vario IP is around 300€ more expensive than a plain analog solution.

The alternative is a plain a/b outdoor telephony station with an ATA adapter. The devices of choice were an "Auerswald Dialog 304" and a "GrandStream HandyTone 701". This sums up to a total of ~270 €. In my opinion this is a valid fallback.

The connections are straightforward, the Auerswald is very good documented.

9.2.4. *Doorphone indoor*

While “open” outdoor solutions still seem a little bit exotic and expensive, indoor ones are less problematic.

I decided to go for a complete phone instead of a slimmed dedicated doorphone. The main reason: I didn’t find a dedicated indoor doorstation based on a/b or IP. But the whole wide world of standard phones is available here…

One possibility is to use a simple (20€) analog phone and an ATA adapter to attach to asterisk. Here i disliked the idea of a stationary phone for this new installation, something cordless would be fine…

At least in Germany a “Fritz!Box” is an interesting component to look at. It has

- Router
- Switch
- DECT base
- Analog phone input
- Telephony software

built in. As you may not need the WAN feature you can buy very cheap ones used around 40€. There’s no way to pay less…

The solution I finally selected was DECT based, too. I liked the idea of taking the door bell, door phone and door opener simply with you… With a new product “Gigaset Go Box” I found an interesting solution to do it all digital. It has VOIP support for 6 channels on the incoming side, 6 DECT channels on the handset side. This is enough and even has a small buffer to play around one day.

Along with some “cheap” handsets you are very flexible with your new “door opener”.

One should also consider the drawbacks of the telephony approach:

- You can accept the “call” only as long the phone is ringing
- You need a time based automatic hangup (as the visitor will not hangup himself)
- After timeout, the indoor can no longer simply off-hook the phone and talk to the outside – you have to dial a number to reconnect. The outside phone must support auto-accept.
- You have to enter a code combination to open the door instead of a simple push button (at least in a basic installation).
- Some people may see handling this “many buttons” a bit scary in comparison to a plain doorphone.

```
Time Travel

I have had no user acceptance problem with the “doorbell” so far.
```

9.3. Software

9.3.1. *Raspbian*

The same basic rules apply to the Raspbian used in this installation.

9.3.2. *Freeswitch*

This is a short story. While having tested successfully freeswitch on my PC and decided to go for it, I didn’t manage a clean install on the Pi. I liked Freeswitch very much for its design and ideas, but hey, it must solve a problem, not create one.

There’s an old installer for the 1.4 version and maybe its working.

For the 1.6

- There’s no Pi package
- You have to switch to Debian Jessie
- You have to compile yourself
- There’s no dedicated help for this setup

I tried the above and failed. Especially switching the distribution did some harm to the already existing installations of my home automation stack.

If you are more of a unix geek you may get it up and running and I assume that a running freeswitch is just fine…

9.3.3. *Asterisk*

After some failed attempts to stick with the freeswitch know how I gathered on the PC platform, for the sake of eventually coming to a working end I finally installed asterisk.

Installing asterisk was a breeze (even if not the newest release, but my requirements are not on the edge of technology). With a little know how on the tasks and architecture of a telephony software, getting a basic understanding and setting up a working environment was a matter of hours.

```
sudo apt-get install asterisk
```

9.4. Configuration

9.4.1. *Asterisk*

Again, there are a lot of tutorials available. One particular important resource is the (free) “Asterisk-the definitive resource”.

The first step in this environment is a relatively small one. We have to go for some configuration files. You will find them in /etc/asterisk.

For our system we only need to look at

- modules.conf
- sip.conf
- extensions.conf

It’s best to leave all other files untouched.

a modules

Asterisk has a hell of extension modules and I do not claim to know what they do. I can again recommend the excellent book and internet resources.

For me it was important that I have a small footprint, all modules that are immediately needed and a bunch that I plan to use in the near future.

An important point is the “autoload=no” in the header. We do not want asterisk to load anything it stumbles upon. For the rest I started with a listing of all available modules and moved backwards…

Most important is the support of SIP. The rest are dependencies or “future feature” modules (musiconhold, playback).

This is the /etc/asterisk/modules..conf

```
[modules]
autoload=no


load => res_cliorginate.so
load => res_crypto.so
load => res_curl.so
load => res_http_post.so
load => res_http_websocket.so
load => res_musiconhold.so
load => res_rtp_asterisk.so
load => res_speech.so
load => res_srtp.so
load => res_stun_monitor.so
load => res_timing_timerfd.so

load => app_authenticate.so
load => app_confbridge.so
load => app_dial.so
load => app_echo.so
load => app_exec.so
load => app_macro.so
load => app_mp3.so
load => app_originate.so
load => app_page.so
load => app_playback.so
load => app_playtones.so
load => app_read.so
load => app_saycountpl.so
load => app_senddtmf.so
```

```
load => app_sendtext.so
load => app_softhangup.so
load => app_system.so
load => app_transfer.so
load => app_verbose.so

load => chan_local.so
load => codec_alaw.so
load => codec_gsm.so
load => codec_ulaw.so

load => format_gsm.so
load => format_wav_gsm.so
load => format_wav.so

load => func_base64.so
load => func_curl.so
load => pbx_config.so
```

b sip

SIP (session initiation protocol) is the most important component here. It's the heart of VOIP connections.

The outdoor and indoor phones are finally terminated on the asterisk machine, dispatching door bell and internal calls using the SIP protocol – just as if they were on different corners of the world.

Every participant is mentioned in the sip.conf

```
[wbf901]
type=friend
host=dynamic
secret=password
context=wb

[wbf101]
type=friend
host=dynamic
secret=password
context=wb

[wbf201]
type=friend
host=dynamic
secret=password
context=wb

[wbf301]
type=friend
host=dynamic
secret=password
context=wb
```

c extensions

Extensions finally define what asterisk should do when a certain number is dialed. The dial codes are the default codes used by the Auerswald outdoor phone (except the 901).

Here we have our minimal rule set. If for example the first button is pressed, a "101" is dialed. This in turn is sent (through the Grandstream) to Asterisk which will activate the wbf101 participant. This participant is attached to Asterisk in the form on one of the IP slots of the Gigaset Go Box.

This is /etc/asterisk/extensions.conf

```
[wb]
exten => 101,1,Dial(SIP/wbf101,20)
exten => 201,1,Dial(SIP/wbf201,20)
exten => 301,1,Dial(SIP/wbf301,20)
exten => 901,1,Dial(SIP/wbf901,20)
```

Well, from here everyone should be able to discover that maybe our software installation is not really challenged with what we do. But then, there are a lot of bells and whistles we can attach using asterisk, especially in combination with the other home automation components.

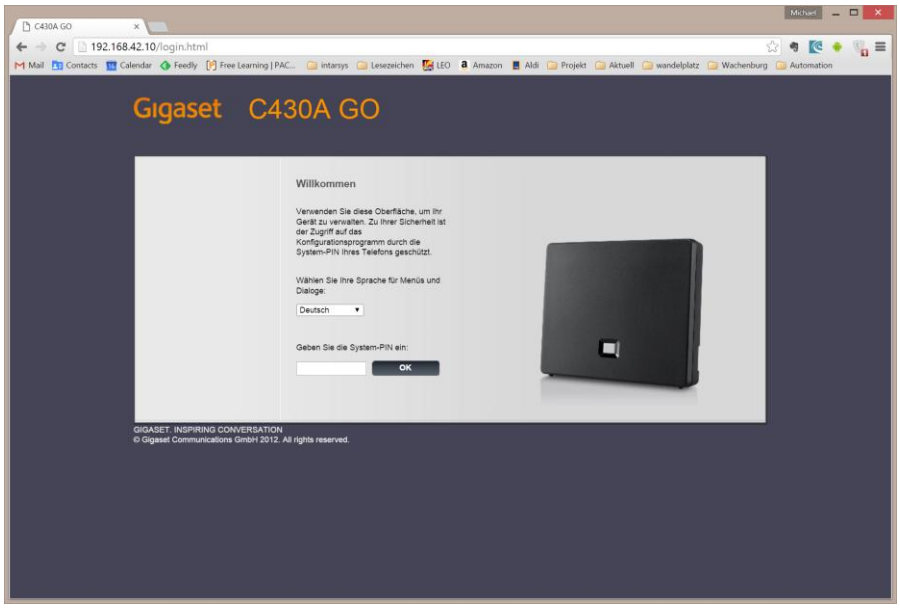
How about some interactive voice response implementation, sending your annoying visitor to the neighbor next door, a mailbox registering a short message for you or forwarding the visitor to your cellphone.

Dialing special numbers (initiating a call or even while talking to somebody) can trigger scripts or enter the openHAB scene…

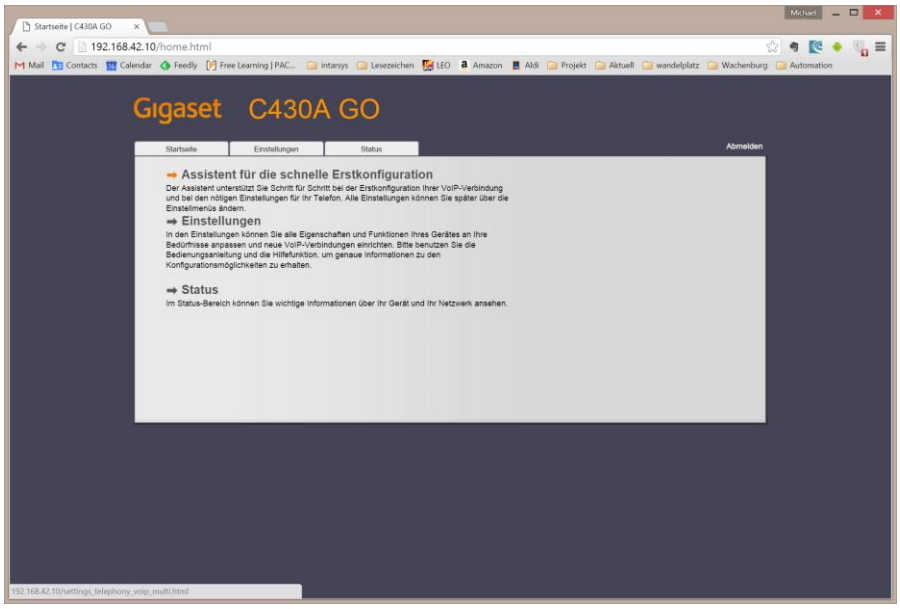
9.4.2. *GO/Box 100*

This small box is the in-door part of the door com.

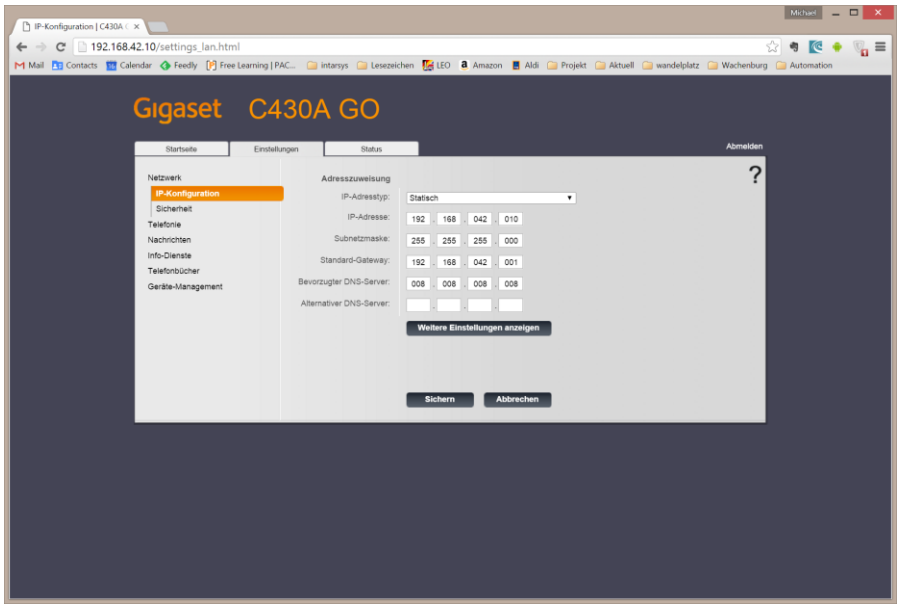
We will go through the configuration and connection to Asterisk shortly.



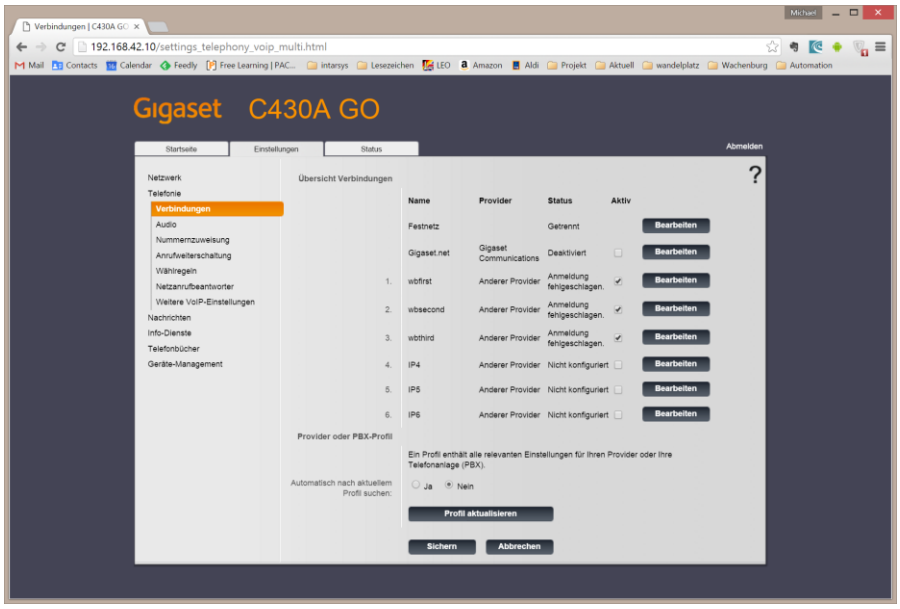
I really recommend changing the PIN – you surely don't want some geeky nerd in the house reconfigure your system.



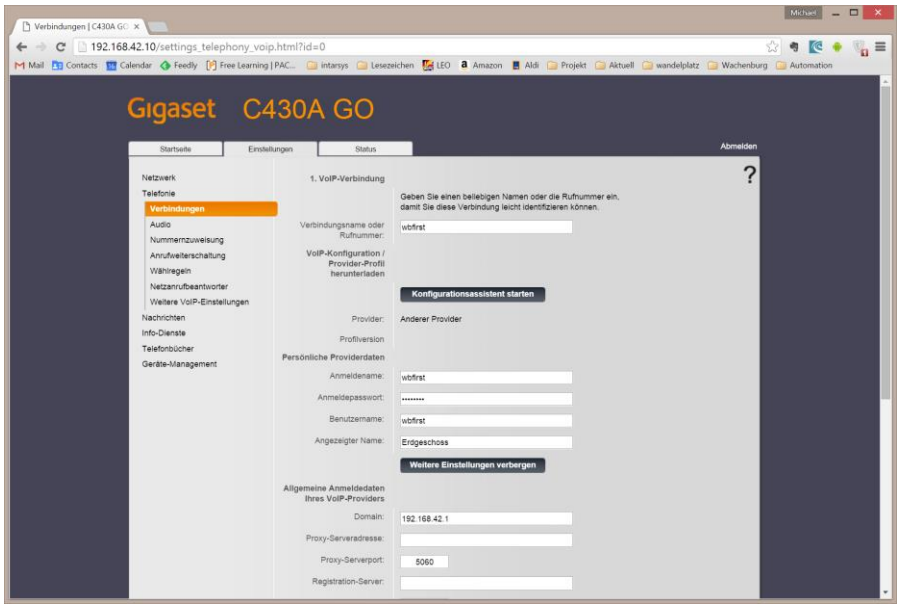
From the start page, we go immediately to the settings.



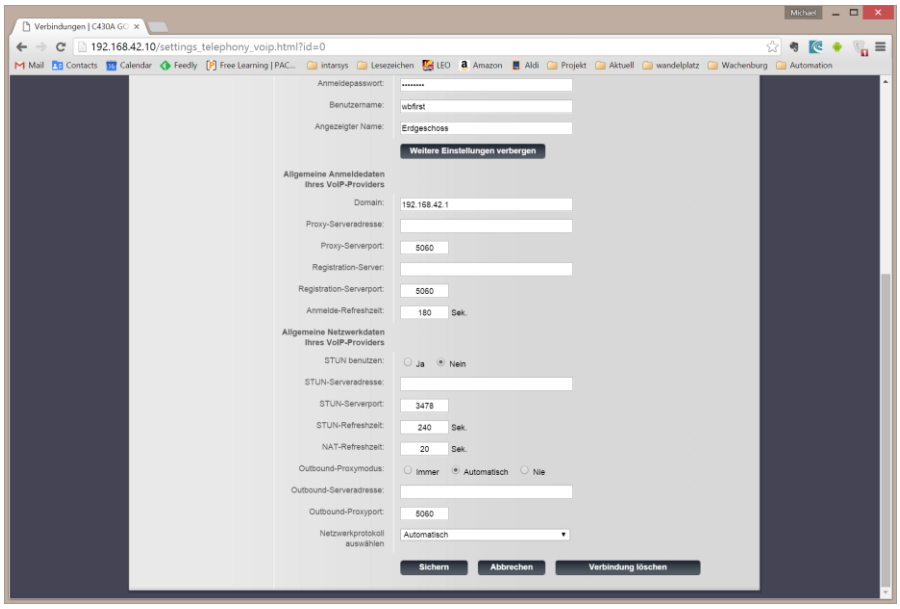
I setup every HA component with a static address – you may go for DHCP, but I recommend setting sticky address assignment.

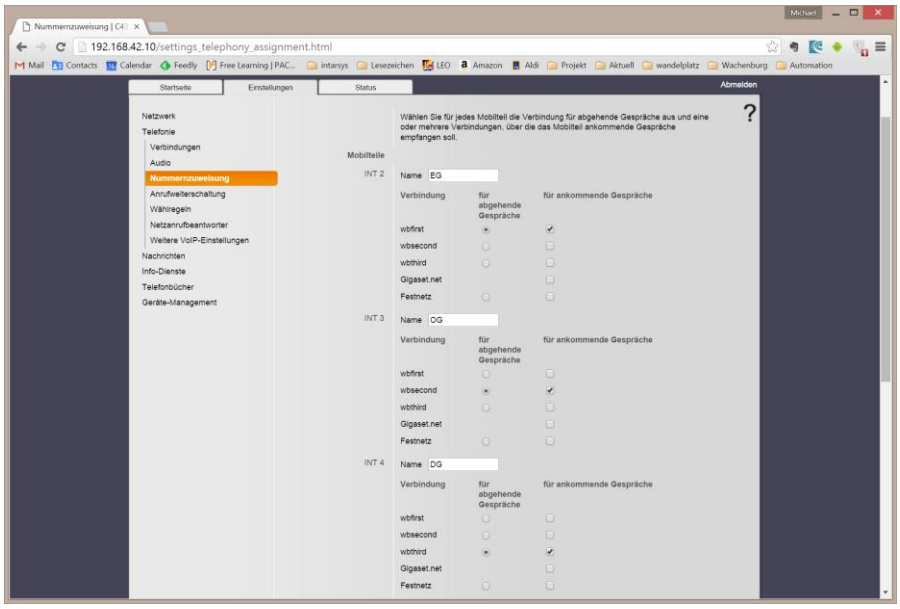


I set up 3 independent IP accounts as clients to the Asterisk VOIP server.

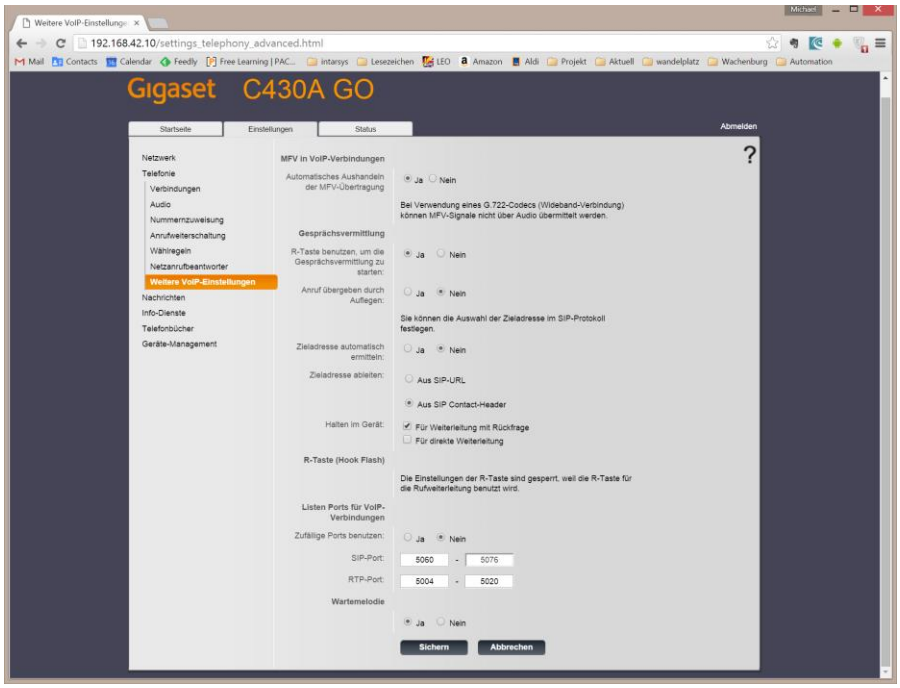


As Asterisk is running on the “gateway” itself, the server IP is 192.168.42.1, the rest is default.





Next, we setup the three handsets and assign each an IP account of its own. This does not mean that we cannot make in-house calls using the handsets.

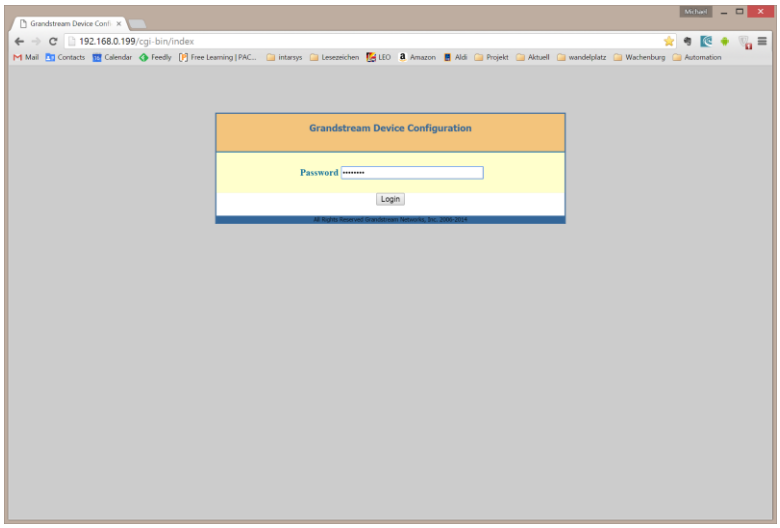


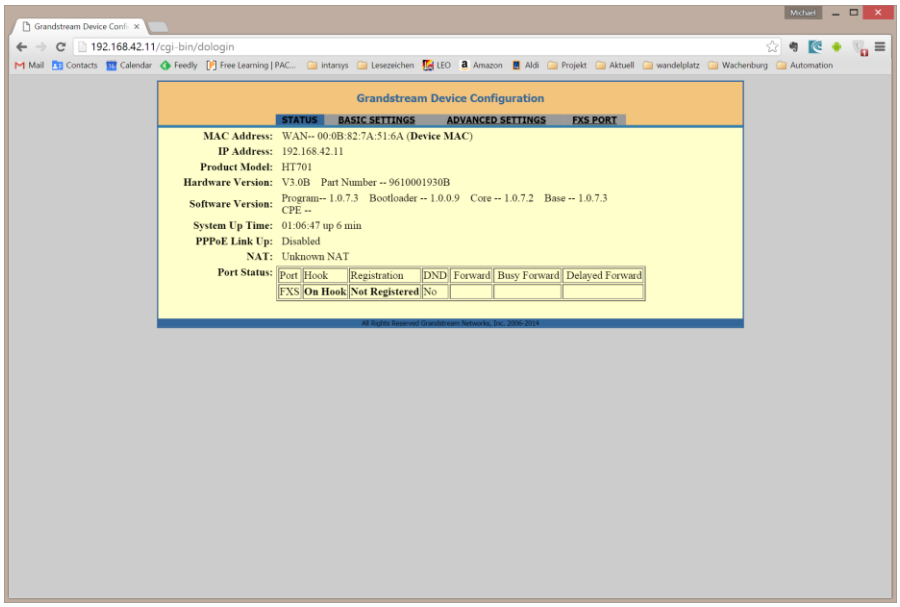
The rest is standard again.

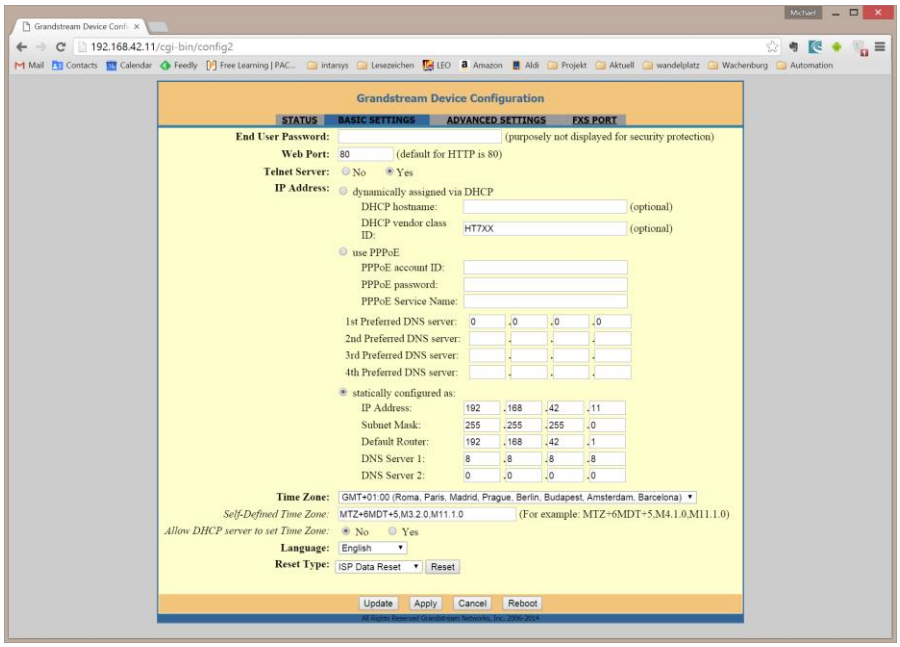
No you should be able to contact the handsets via Asterisk.

9.4.3. *Grandstream HT701*

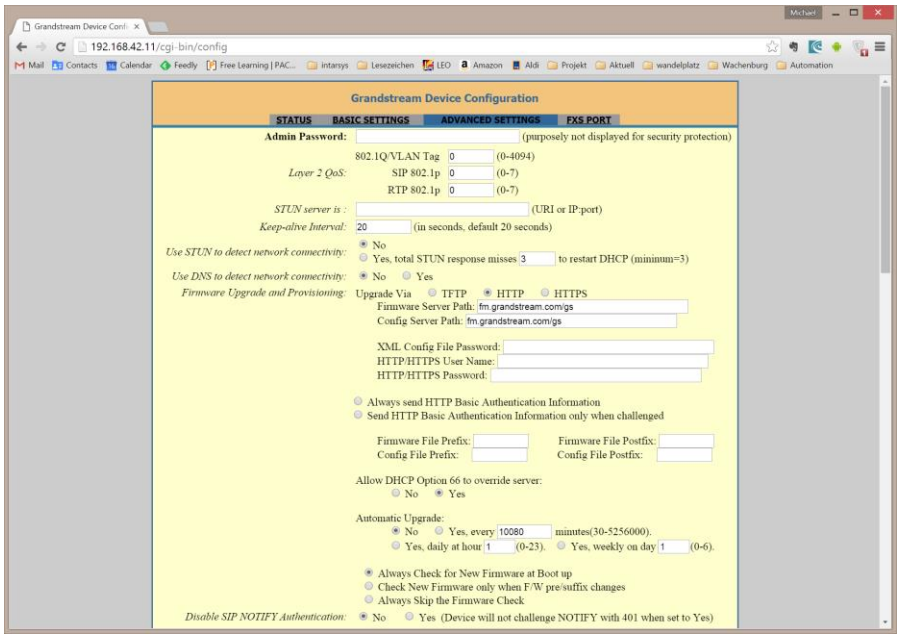
This component is the interface between the analog outside phone (Auerswald) and the VOIP based internals.

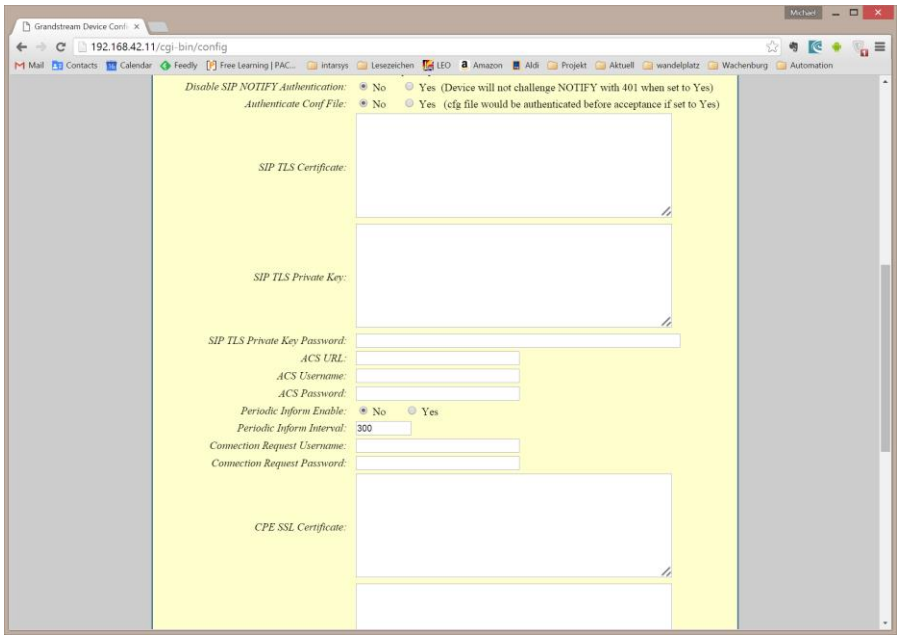


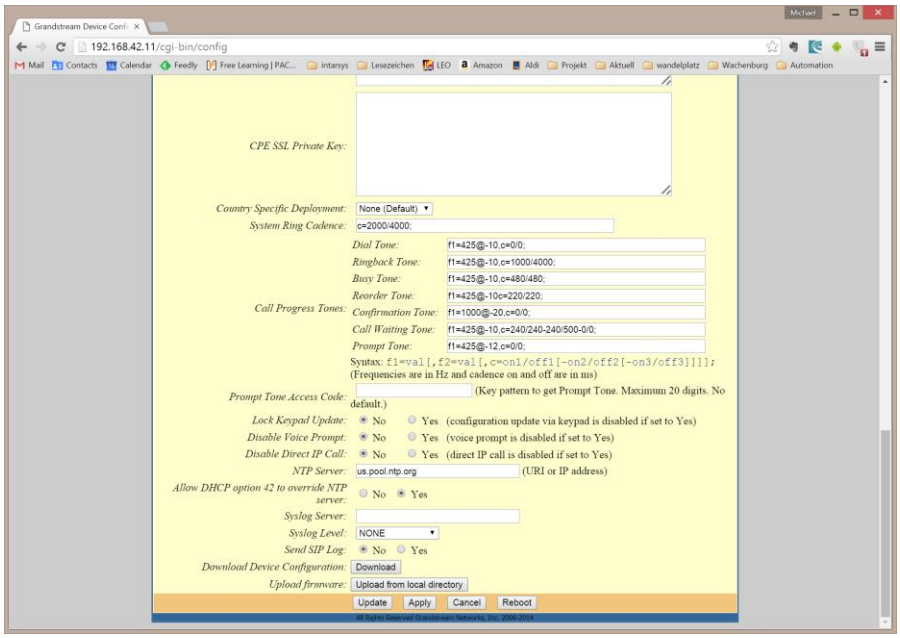




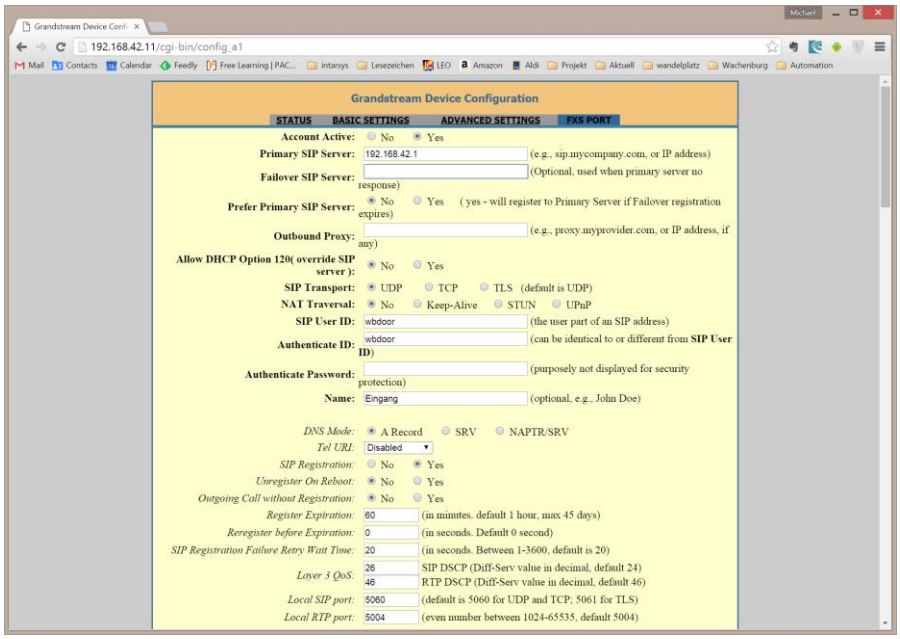
Once again I use static IP.


Grandstream Device Conf
192.168.42.11/cgi-bin/config
Grandstream Device Configuration
STATUS
BASIC SETTINGS
ADVANCED SETTINGS
FXS PORT
Admin Password:
(purposely not displayed for security protection)
802.1Q/VLAN Tag 0 (0-4094)
Layer 2 QoS:
SIP 802.1p 0 (0-7)
RTP 802.1p 0 (0-7)
STUN server is :
(URI or IP:port)
Keep-alive Interval: 20 (in seconds, default 20 seconds)
Use STUN to detect network connectivity:
No
Yes, total STUN response misses 3 to restart DHCP (miminum=3)
Use DNS to detect network connectivity: No Yes
Firmware Upgrade and Provisioning:
Upgrade Via TFTP HTTP HTTPS
Firmware Server Path: fm.grandstream.com/gs
Config Server Path: fm.grandstream.com/gs
XML Config File Password:
HTTP/HTTPS User Name:
HTTP/HTTPS Password:
Always send HTTP Basic Authentication Information
Send HTTP Basic Authentication Information only when challenged
Firmware File Prefix:
Firmware File Postfix:
Config File Prefix:
Config File Postfix:
Allow DHCP Option 66 to override server:
No Yes
Automatic Upgrade:
No Yes, every 10080 minutes(30-5256000).
Yes, daily at hour 1 (0-23). Yes, weekly on day 1 (0-6).
Always Check for New Firmware at Boot up
Check New Firmware only when F/W pre/suffix changes
Always Skip the Firmware Check
Disable SIP NOTIFY Authentication: No Yes (Device will not challenge NOTIFY with 401 when set to Yes)

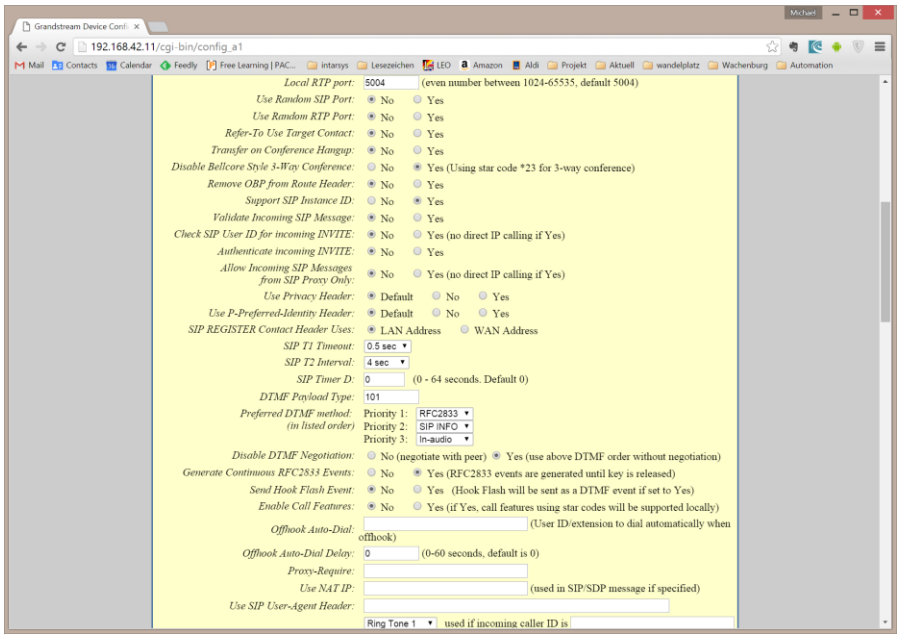

Grandstream Device Conf
192.168.42.11/cgi-bin/config
Disable SIP NOTIFY Authentication: No Yes (Device will not challenge NOTIFY with 401 when set to Yes)
Authenticate Conf File: No Yes (cfg file would be authenticated before acceptance if set to Yes)
SIP TLS Certificate:
SIP TLS Private Key:
SIP TLS Private Key Password:
ACS URL:
ACS Username:
ACS Password:
Periodic Inform Enable: No Yes
Periodic Inform Interval: 300
Connection Request Username:
Connection Request Password:
CPE SSL Certificate:

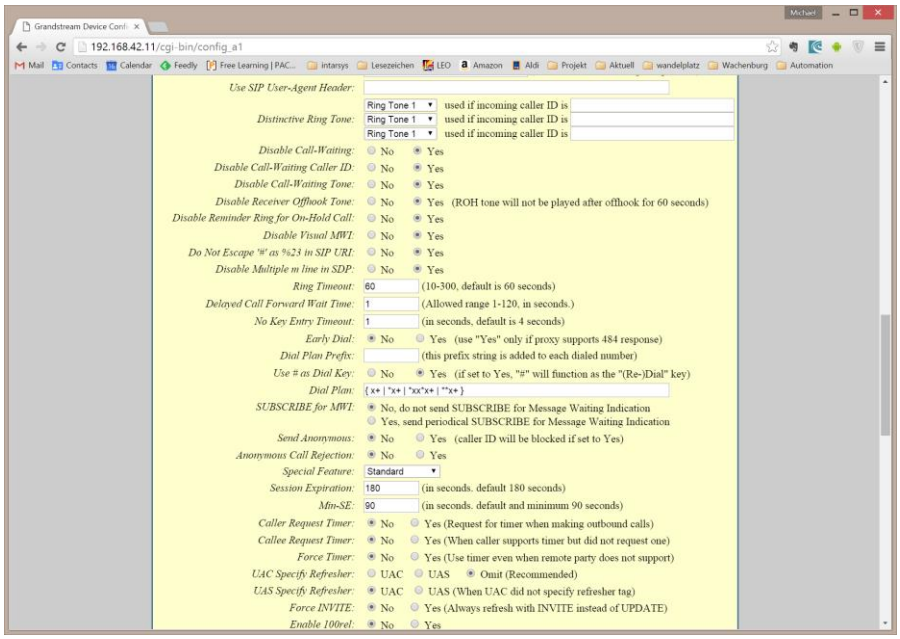


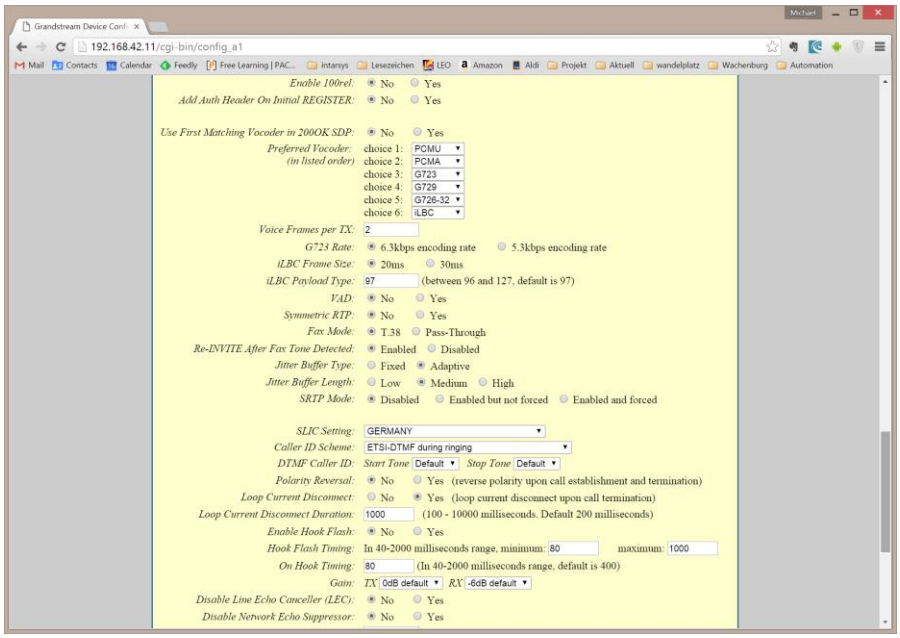
The call progress tone generator settings were trial and error and I really did not get it as smooth as I thought it should be: The analog outdoor phone for example was not able to detect the tone when hung up.

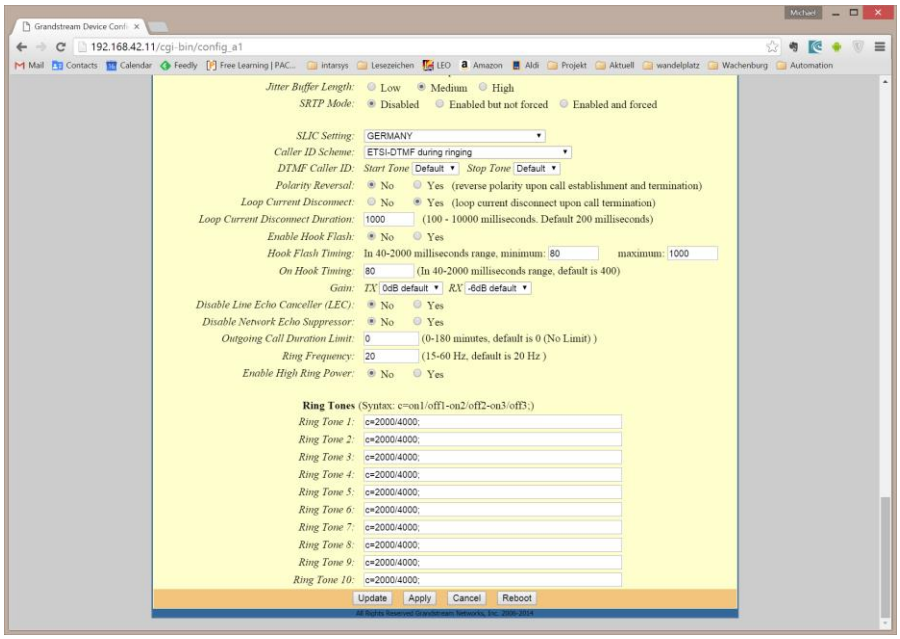


The SIP configuration is mostly standard.


Grandstream Device Conf
192.168.42.11/cgi-bin/config_a1
Local RTP port: 5004 (even number between 1024-65535, default 5004)
Use Random SIP Port: No Yes
Use Random RTP Port: No Yes
Refer-To Use Target Contact: No Yes
Transfer on Conference Hangup: No Yes
Disable Bellcore Style 3-Way Conference: No Yes (Using star code *23 for 3-way conference)
Remove OBP from Route Header: No Yes
Support SIP Instance ID: No Yes
Validate Incoming SIP Message: No Yes
Check SIP User ID for incoming INVITE: No Yes (no direct IP calling if Yes)
Authenticate incoming INVITE: No Yes
Allow Incoming SIP Messages from SIP Proxy Only: No Yes (no direct IP calling if Yes)
Use Privacy Header: Default No Yes
Use P-Preferred-Identity Header: Default No Yes
SIP REGISTER Contact Header Uses: LAN Address WAN Address
SIP T1 Timeout: 0.5 sec
SIP T2 Interval: 4 sec
SIP Timer D: 0 (0 - 64 seconds. Default 0)
DTMF Payload Type: 101
Preferred DTMF method: (in listed order) Priority 1: RFC2833 Priority 2: SIP INFO Priority 3: In-audio
Disable DTMF Negotiation: No (negotiate with peer) Yes (use above DTMF order without negotiation)
Generate Continuous RFC2833 Events: No Yes (RFC2833 events are generated until key is released)
Send Hook Flash Event: No Yes (Hook Flash will be sent as a DTMF event if set to Yes)
Enable Call Features: No Yes (if Yes, call features using star codes will be supported locally)
Offhook Auto-Dial: (User ID/extension to dial automatically when offhook)
Offhook Auto-Dial Delay: 0 (0-60 seconds, default is 0)
Proxy-Require:
Use NAT IP: (used in SIP/SDP message if specified)
Use SIP User-Agent Header:
Ring Tone 1 used if incoming caller ID is


Grandstream Device Conf
192.168.42.11/cgi-bin/config_a1
Use SIP User-Agent Header:
Distinctive Ring Tone: Ring Tone 1 used if incoming caller ID is
Disable Call-Waiting: No Yes
Disable Call-Waiting Caller ID: No Yes
Disable Call-Waiting Tone: No Yes
Disable Receiver Offhook Tone: No Yes (ROH tone will not be played after offhook for 60 seconds)
Disable Reminder Ring for On-Hold Call: No Yes
Disable Visual MWI: No Yes
Do Not Escape '#' as %23 in SIP URI: No Yes
Disable Multiple m line in SDP: No Yes
Ring Timeout: 60 (10-300, default is 60 seconds)
Delayed Call Forward Wait Time: 1 (Allowed range 1-120, in seconds.)
No Key Entry Timeout: 1 (in seconds, default is 4 seconds)
Early Dial: No Yes (use "Yes" only if proxy supports 484 response)
Dial Plan Prefix: (this prefix string is added to each dialed number)
Use # as Dial Key: No Yes (if set to Yes, "#" will function as the "(Re-)Dial" key)
Dial Plan: { x+ | *x+ | *xx*x+ | **x+ }
SUBSCRIBE for MWI: No, do not send SUBSCRIBE for Message Waiting Indication
Yes, send periodical SUBSCRIBE for Message Waiting Indication
Send Anonymous: No Yes (caller ID will be blocked if set to Yes)
Anonymous Call Rejection: No Yes
Special Feature: Standard
Session Expiration: 180 (in seconds. default 180 seconds)
Min-SE: 90 (in seconds. default and minimum 90 seconds)
Caller Request Timer: No Yes (Request for timer when making outbound calls)
Callee Request Timer: No Yes (When caller supports timer but did not request one)
Force Timer: No Yes (Use timer even when remote party does not support)
UAC Specify Refresher: UAC UAS Omit (Recommended)
UAS Specify Refresher: UAC UAS (When UAC did not specify refresher tag)
Force INVITE: No Yes (Always refresh with INVITE instead of UPDATE)
Enable 100rel: No Yes





With most of the settings you may play around until you're satisfied with voice quality (along with the settings of the outside phone). You can easily see that the installation is not really a corner case for the Grandstream.

One thing that was important with me: To get the Auerswald reliably "hooked" after calling, I had to enable "Look current Disconnect".

Part II

Now we have some island components – already with nice functionality, but we can do better. Here are the basic steps to provide interoperability.

10. Network setup

10.1. Static IP

To set up a static IP address, you have to edit the /etc/network/interfaces in your Pi. A typical configuration would look like this, important settings are bold.

```
# Ethernet
auto etho
allow-hotplug eth0
iface eth0 inet static
address 192.168.42.210
netmask 255.255.255.0
gateway 192.168.42.1
```

For sure you have to take care to use an address that is unique in your network and that does not lie in the dynamic address range of your DHCP server.

It may be necessary to disable the DHCP daemon on your Pi to make things work

```
sudo service dhcpcd stop
sudo update-rc.d -f dhcpcd remove
```

To activate your new settings, you must restart the network

```
sudo /etc/init.d/networking restart
```

10.2. Dynamic IP

If you want to run a Pi with dynamic IP address, you can use the following configuration in /etc/network/interfaces

```
# Ethernet
auto etho
allow-hotplug eth0
iface eth0 inet dhcp
```

You should assure that somewhere in the network a DHCP server is up and running…

10.3. IP address setup

To administrate your network, it is important to have convenient access to the components. While the system has a DHCP server, I found it the easiest way to give each of the components a static IP.

Hostname	IP	services
wbbase	192.168.42.1	isc-dhcp-server, asterisk, samba
wbf1	192.168.42.210	hmland, homegear, openhab
wbf2	192.168.42.220	hmland, homegear, openhab
wbf3	192.168.42.230	hmland, homegear, openhab
wbgo100	192.168.42.10	VOIP Client(s)
wbht701	192.168.42.11	VOIP Adapter
wbpellematic	192.168.42.2	Heating
DHCP Clients	192.168.42.1xx	… all the rest

10.4. Hostname and hosts

If you want your Pi to have a more meaningful hostname (or as in this case you don't want your Pi's to have all the same name), you should change /etc/hostname

```
wbf1
```

This information is simply required on every Linux and used in many places where the identifying the host is required (mail,…).

In addition you should edit the /etc/hosts, the poor mans DNS, so that accessing the component using its hostname will resolve to the correct component. And if you are already about to edit the file, you should add all other components in your network as we do not set up a local DNS. This allows to access the components via their logical names instead of the IP addresses.

/etc/hosts

```
127.0.0.1      localhost
127.0.1.1      raspberry

192.168.42.1         wbbase
192.168.42.210       wbf1
192.168.42.220       wbf2
192.168.42.230       wbf3

192.168.42.2         wbpellematic
192.168.42.10        wbgo100
192.168.42.11        wbht701
```

10.5. Provide DHCP services

If you want one of your Pi's to provide a DHCP server (mmmh, your gateway maybe..) you should install and configure the DHCP server.

For me, using the ISC server simply worked.

```
sudo apt-get install isc-dhcp-server
```

An error message at this point is OK, as the default configuration is not working yet. You must edit the configuration at /etc/dhcp/dhcpd.conf

This is what is working for me – the important pieces are bold. You have to mention the gateway ("option routers"), the DNS servers ("option domain-name-servers", here a Google server), a flag that this is the one and only valid DHCP source ("authoritative") and then the definition of the subrange of addresses that are available for dynamic clients.

```
# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# option definitions common to all supported networks...
option domain-name "wb.local";

default-lease-time 86400; # 24 hours
max-lease-time 172800; # 48 hours

option routers 192.168.42.1;
option domain-name-servers 8.8.8.8;
```

```
authoritative;

subnet 192.168.42.0 netmask 255.255.255.0 {
  range 192.168.42.100 192.168.42.199;
}
```

Restart the DHCP server after configuration changes

```
sudo service isc-dhcp-server restart
```

11. Mass Storage

Storing data on the SD card has some serious drawbacks

- Many operations will wear out the SD card
- SD card capacity is quite restricted
- Each unit has its own card, central storage is not available

The solution is to add some mass storage as a service.

11.1. USB Hub

While you may get away with connecting smaller gadgets directly to the Pi's USB, sucking all of the power it has to give and pushing it to the limit of getting unstable (well, maybe this sounds a little dramatic…) – attaching a USB powered disk is definitely **not** what you want to do.

I bought a small USB hub that can neatly be hidden beneath the Pi in the cabinet, in this case a i-tec 4-Port USB 2.0 component.

11.2. USB Disk

Checking the available disks for the Pi can be done using

```
sudo fdisk -l
```

You will see something similar to

```
Disk /dev/mmcblk0: 7948 MB, 7948206080 bytes
4 heads, 16 sectors/track, 242560 cylinders, total 15523840 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xa6202af7
```

```
        Device Boot      Start         End      Blocks   Id  System
/dev/mmcblk0p1            8192      122879       57344    c  W95 FAT32 (LBA)
/dev/mmcblk0p2          122880    15523839     7700480   83  Linux
```

This is the SD card “disk” and its partitioning.

Plugging in a USB disk will change the matter – you will see an additional disk now:

```
Disk /dev/sda: 500.1 GB, 500107861504 bytes
255 heads, 63 sectors/track, 60801 cylinders, total 976773167 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x386abe69

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1            2048   976768064   488383008+   7  HPFS/NTFS/exFAT
```

This one is preformatted NTFS on a Windows system.

To get this far you must have installed the NTFS support on the PI. This is easy, simply

```
apt-get -y install ntfs-3g
```

Now we need a “mount point” on the Pi, this is a location in the “main file system” where the USB disk is “mounted”, i.e. the USB disk filesystem is seen as if it is underneath this mount point.

```
sudo mkdir /media/wbdisk
```

Furthermore we need the UUID of the disk, as the name device name “/dev/sda1” is assigned dynamically and may change in other circumstances. To get the UUID enter

```
sudo blkid
```

This will show you something like

```
/dev/mmcblk0p1: SEC_TYPE="msdos" LABEL="boot" UUID="15CD-3B79" TYPE="vfat"
/dev/mmcblk0p2: UUID="13d368bf-6dbf-4751-8ba1-88bed06bef77" TYPE="ext4"
/dev/sda1: LABEL="wbdisk" UUID="340CC0590CC017AE" TYPE="ntfs"
```

Now we have everything we need to mount the disk for further use. Manually you can mount the disk using

```
sudo mount -t ntfs-3g -o utf8,noatime /dev/sda1 /media/wbdisk
```

and unmount

```
sudo umount /media/wbdisk
```

As we don’t want to do this anytime we launch the Pi, we make this a permanent feature. To do this edit the /etc/fstab file and add a line like this. Do not forget to use your correct UUID and file system driver.

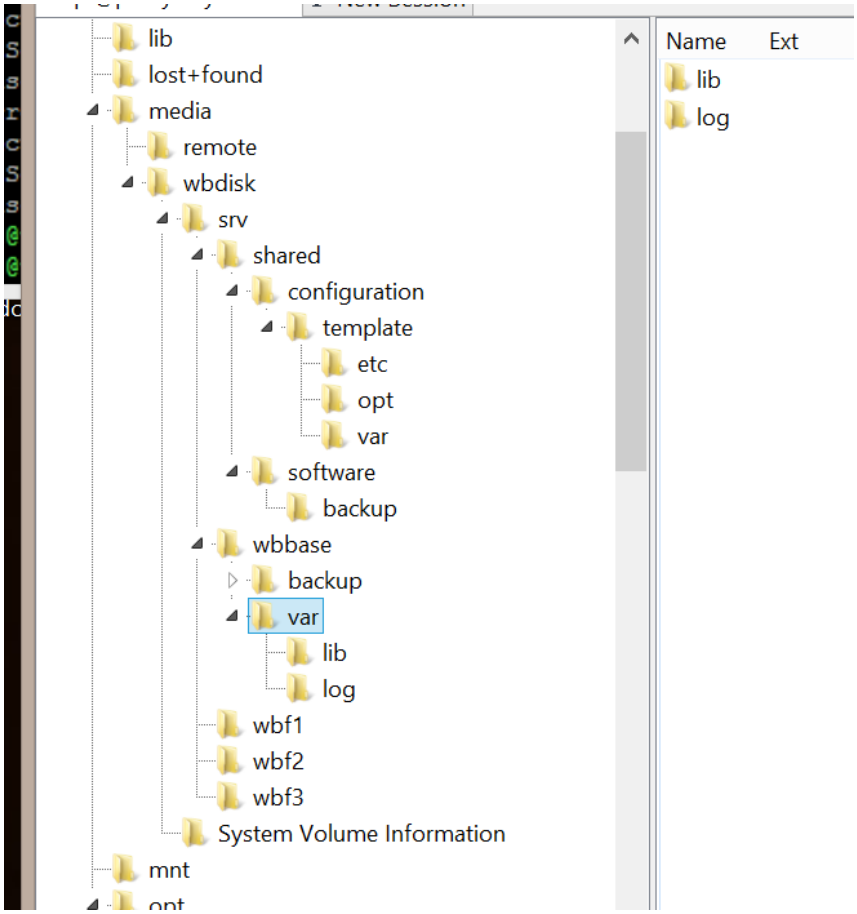
```
# here's the USB disk
UUID=340CC0590CC017AE    /media/wbdisk/      ntfs-3g      utf8,noatime  0
```

11.3. Directory layout

Now lets design the layout in the USB disk itself.

We already know that storage devices are mounted at /media and that we called our device “wbdisk”.

On this device I’d like to mark a section as reserved for server storage, “srv”. Below we make a directory for “shared” data and one for each active participant, this makes up for “wbf1”, “wbf2”, “wbf3” and “wbbase”.



If you make extensions to this layout, ensure that you create directories upfront that you want to reference from mounts, they are not created automatically for you.

In the client directories i have created a layout mirroring the original file system layout whenever I wanted to switch from the original data location to a server based one.

11.4. NFS

There must be a reason we added a USB disk and here it is: we add a network file system (NFS) and have plenty of space for writing logs, database and whatsoever…

So far as theory is concerned. NFS may be an easy to install, performant solution, but it’s an island. For me ease of access from other platforms (ok, lets give it a name: Windows) is crucial and that’s where NFS simply fails.

I decided quickly (after having nearly havocked my Windows installation in the attempt to access the shares) to migrate to Samba.

11.5. Samba

11.5.1. Misc

https://wiki.samba.org/index.php/Mounting_samba_shares_from_a_unix_client

11.5.2. Pi server

Working with NFS when we also want to include a Windows PC in the network is a pain. For the sake of interoperability we switch to Samba here.

Install

```
apt-get install samba samba-common-bin
```

Configuration

```
sudo nano /etc/samba/smb.conf
```

Here we will setup a share for every client and a shared one, using the already defined directories on the mounted USB disk. As you can see, we do not care much about privacy at this point – this may or may not be appropriate for you.

At the end of the file, below all other sections add:

```
[wbf1]
path = /media/wbdisk/srv/wbf1
writeable = yes
guest ok  = yes

[wbf2]
path = /media/wbdisk/srv/wbf2
writeable = yes
guest ok  = yes

[wbf3]
path = /media/wbdisk/srv/wbf3
writeable = yes
guest ok  = yes

[wbbase]
path = /media/wbdisk/srv/wbbase
writeable = yes
guest ok  = yes

[shared]
path = /media/wbdisk/srv/shared
writeable = yes
guest ok  = yes
```

Most probably, at least to support hardlinks, you will want to add this in the [global] section. Be sure to add this near the beginning of the configuration file.

```
 unix extensions = yes
 follow symlinks = yes
```

After a change to the configuration, you must restart the samba service.

11.5.3. Pi client

To access a Samba share, the client must install

```
apt-get install cifs-utils
```

As this is available by default on the standard Raspbian, you should be able to omit this.

Now you can mount the network share on your client.

We create a mount point in each client at

```
mkdir /media/remote/wbdisk/private
mkdir /media/remote/wbdisk/shared
```

The mount point must belong to the root user. It is a very clever idea to name the mount points locally using the same name (they will be mapped to a different server location later). This gives you the ability to reuse the same scripts on every component (e.g. backup scripts) without any change.

Now you can mount the shares, for example for “wbf1” with the commands below. This will work only if you have guests allowed on the server. Omitting “-o guest” will nag you with a password prompt.

Note how each component will map its private share to a dedicated directory on the server.

```
mount -t cifs //wbbase/shared /media/remote/wbdisk/shared -o guest
mount -t cifs //wbbase/wbf1 /media/remote/wbdisk/private -o guest
```

Here we use the network aliases defined in /etc/hosts, you can use the IP address if you want.

to manually unmount you can call

```
umount /media/remote/wbdisk/shared
umount /media/remote/wbdisk/private
```

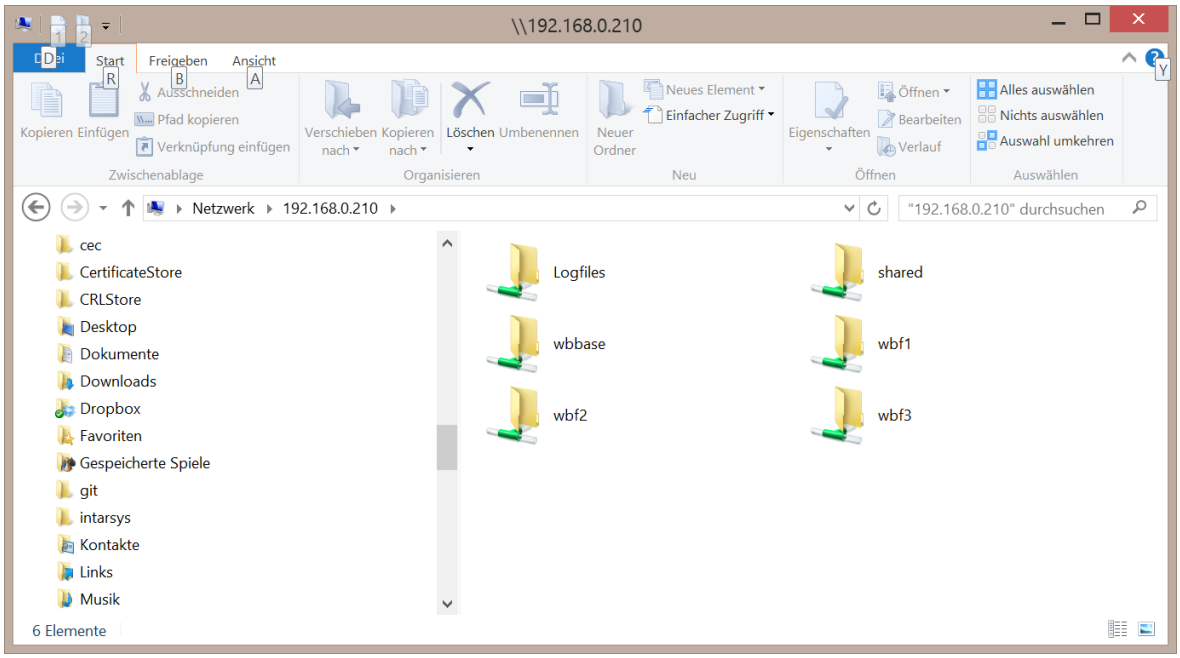
Eventually we want to make this bindings permanent, so we change the /etc/fstab and add

```
//wbbase/shared /media/remote/wbdisk/shared cifs auto,guest,_netdev 0 0
//wbbase/wbf1 /media/remote/wbdisk/private cifs auto,guest,_netdev 0 0
```

11.5.4. Windows client

Well, a windows client should be able to access the share without effort, you only have to use the IP address as in the standard installation the Pi names are not propagated to Windows (this can be done, though).

Open an explorer and type “\\<address>” in the address field (don’t forget the backslashes”.


\\192.168.0.210
Start
Freigeben
Ansicht
Ausschneiden
Pfad kopieren
Verknüpfung einfügen
Kopieren
Einfügen
Zwischenablage
Verschieben nach
Kopieren nach
Löschen
Umbenennen
Organisieren
Neuer Ordner
Neues Element
Einfacher Zugriff
Neu
Eigenschaften
Öffnen
Bearbeiten
Verlauf
Öffnen
Alles auswählen
Nichts auswählen
Auswahl umkehren
Auswählen
Netzwerk
192.168.0.210
"192.168.0.210" durchsuchen
cec
CertificateStore
CRLStore
Desktop
Dokumente
Downloads
Dropbox
Favoriten
Gespeicherte Spiele
git
intarsys
Kontakte
Links
Musik
Logfiles
shared
wbbase
wbf1
wbf2
wbf3
6 Elemente

12. Backup

12.1. So why?

Even if it seems to be unnecessary (well, it isn't) – consider setting up a backup.

In the beginning my intention was to setup each station and then keep copies of the respective SD cards. On failure I'd simply plug in the SD copy and things are all right. So while in theory this was a good idea, in practice it's not really feasible.

Already after 5 days of "production" the image of the respective clients was outdated because of little tweaks in the settings, added operating system features and so on.

Having a live backup possibility is the best you can do (IMHO). So after we already decided to go for a fully networked system, added an USB disk and installed Samba, why wouldn't we provide a simple backup... Simply starting the script after some non trivial changes is a very simple task and gives you a quite good feeling when going to sleep…

12.2. rsync

rsync is a classical tool for synchronizing two file system hierarchies. It is widespread and has a very efficient implementation. Because of its many options it may seem intimidating at first, but you have come this far, so give it a try.

First, I created a directory at /opt/backup for all backup related scripts.

Then we create the following shell script. While there exist much more sophisticated scripts and full fledged programs, it will do the job. The skeleton to this script and the parameters used are borrowed from a plethora of rsync related blog entries, blame all errors on me and all fame on them.

This is my /opt/backup/backup.sh (don't you forget to make it executable).

```
#!/bin/sh

SOURCE=/
DEST=/media/remote/wbdisk/private/backup/
TODAY=$(date +%Y-%m-%d)

rsync -avqRH -stats --delete-during --exclude-from=/opt/backup/exclude.txt \
  "${SOURCE}"  "${DEST}${TODAY}/" --link-dest="${DEST}last/" > \
  /var/log/rsync.log
ln -nsf "${DEST}${TODAY}" "${DEST}last"

exit 0
```

First, we have some variable definitions to ease script changes. With

```
SOURCE=/
```

we backup everything starting from root (exceptions see later).

```
DEST=/media/remote/wbdisk/private/backup/
```

The destination is our private share on the Samba server. Notice that you have to create the target "backup" directory by hand.

```
TODAY=$(date +%Y-%m-%d)
```

This is a helper variable that holds a date string with year, month and day. We will use this for incremental backups.

```
rsync -aqRH
```

Option	Description
-a	combines –rlptgoD
-r	Copy subdirectories
-l	Copy symbolic links
-p	keep permissions
-t	keep timestamps
-g	keep group settings
-o	keep owner settings
-D	keep device files
-q	suppress non error messages
-R	use relative path names
-H	preserve hard links

```
rsync … -stats
```

Create statistical output at the end of the backup

```
rsync … --delete-during
```

I have a incremental backup where I delete files in the destination when they are deleted in the source. “delete-during” keeps time and memory consumption low.

```
rsync … --exclude-from=/opt/backup/exclude.txt \
```

Now this is important: we create a file with a list of exclusions I do not want to be backed up, starting from my SOURCE.

For me this is /opt/backup/exclude.txt

```
/proc/*
/sys/*
/dev/*
/boot/*
/tmp/*
/run/*
/mnt/*
/media/*
/var/log/*
/var/run/*
/var/lock/*
```

Most (all?) “dynamic or transient parts of the system are ignored.

```
rsync … "${SOURCE}"  "${DEST}${TODAY}/" --link-dest="${DEST}last/"
```

This is the copy itself, from SOURCE to DEST/TODAY, so we create a new directory every day we create a backup. Together with the symbolic link feature “—link-dest” we ensure that files that are unchanged exist only once in the target. As this needs the underlying “symbolic link” feature of the file system, be sure your target does support this (e.g. by activating it in your samba configuration).

```
rsync … > /var/log/rsync.log
```

For everything we have done so far, a detailed log file is written.

After rsync is ready we create a new symbolic link to the new backup named “last”. This is in turn the reference for the next incremental backup.

```
ln -nsf "${DEST}${TODAY}" "${DEST}last"
```

Now you can start the backup manually or add it to crontab. I decided against a scheduled backup as I do not expect extensive working on the configuration or content.

Part III

We have a basic system up and running. Now we can start with the bells and whistles that will improve the design and bring the project from lab to real life.

13. Access Point

wbf1, wbf2 and wbf3 should provide Access Point features. The eth0 and wlan0 interfaces need to be bridged only.

This is a very special chapter and not everything I did here is really understood.

First, I made the mistake of getting one of the much praised Edimax WLAN sticks (EDIMAX-7612UAn V2). While these are plug and play with regard to WLAN client mode building an access point is not. The problem with them is that they need a driver that is not available by default for the “hostapd” package.

- Switch hostapd
- Configure hostapd
- Switch of power saving
- Run hostapd as daemon
- Install dhcp server
- Configure dhcp server

13.1. /etc/network/interfaces

The following network configuration describes two network interfaces, eth0 and wlan0 that “bridge” the traffic between them

```
##############################
# The loopback network interface
auto lo
iface lo inet loopback

##############################
# The cable network interface
auto eth0
allow-hotplug eth0
iface eth0 inet manual

########################
# The WLAN interface
auto wlan0
allow-hotplug wlan0
iface wlan0 inet manual

##############################
# The bridges
#
auto br0
iface br0 inet static
address 192.168.42.1
netmask 255.255.255.0

bridge_fd 0
bridge_stp off
bridge_ports eth0 wlan0
```

13.2. Disable power saving

If you want your access point to be available reliably, you should also disable power management for the WLAN.

```
sudo nano /etc/modprobe.d/8192cu.conf
```

You should enter the following content

```
# Disable power management
options 8192cu rtw_power_mgnt=0 rtw_enusbss=0
```

13.3. Switch hostapd

"hostapd" is a piece of software that allows your computer to act as an access point. The only problem is: the driver it relies on is not available for the chip on the Edimax wlan component. Now you have two options: use another WLAN component (providing a NL80211 driver) or use another hostapd package. Using forum KnowHow is tried the second approach.

There are different tutorials regarding how to work around the hostapd issue

[hostapd original] http://www.tacticalcode.de/2013/02/raspberry-pi-als-accesspoint-oder-wlan-bridge.html

[hostapd 2.0] http://www.jenssegers.be/43/Realtek-RTL8188-based-access-point-on-Raspberry-Pi%29

[hostapd 2.2] http://lispm.blogspot.de/2015/03/edimax-ew-7811un-als-wlan-access-point.html

Well, first I tried the original Pi configuration – which can not work because of the "nl80211" driver needed and not available for the Realtek chip.

Then I looked around and found I need to build the hostapd from scratch from Realtek sources (that are quite outdated). This failed for me, I still don't know why.

Some helping hand offered a prebuilt version (still hostapd v0.8). I installed it and really was lucky, hostapd started… but this time I could not connect to the WLAN it offered, even so I saw the SSID in my clients.

The next step was to update to a newer precompiled version, v2.2. This time when starting, hostapd terminated with a failure (that even was not identifiable in the log, at least for me). As a last try I played around with the hostapd settings and found out that after disabling 802.11n (HT capabilities) completely – the daemon finally started. I could connect to the Pi on my new WLAN…

Unfortunately I can not say what were the exact reasons for the different failures.

13.4. Run hostapd as daemon

Now we want the access point to be available after every reboot. You can achieve this by changing the hostapd configuration.

```
sudo nano /etc/default/hostapd
```

Remove the hashmark from the following line

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

13.5. Experience

While I do not really need AP features for my project, I wanted it to be available for later extensions (anything from table UIs to MQTT components).

But: I didn't get it to run reliably. After a lot of spurious failures where connection to the PI no longer was possible, I stopped this experiment and opted for stable production of the basic components.

Maybe some guru may have advice on this…

14. WAN access

This is one of the most interesting features, unfortunately this has been one of the worst experiences when setting up. But, one info at a time…

The HA system as it is planned is an “island”, we do not have internet access as the network is physically and logically detached from any internet service that a resident may have. A full fledged internet account is oversized for this installation and as such much to expensive. The only remaining alternative is GPRS/UMTS – a very interesting one from the nerd point of view and as such the solution of choice.

The driving forces to install this feature are easy to guess

- Internet access for easy system maintenance (local -> WAN)
  For me this means update and installation of software packages. There are solutions for “offline maintenance”, but they are too complex imho.
- Push Notifications (local -> WAN)
  For exceptional states the system should be able to proactively inform the operator (yes, that’s me). The channels available are eMail, SMS and even phone calls, as we have set up Asterisk.
- Remote monitoring and control of the HA system (WAN -> local)
  This makes the HA much more operating friendly – I do not have to visit the building every time a user claims to have a problem, some scenarios can be handled in the home office now.

```
Time Travel

I must admit, I underestimated the use of the remote access feature. This has
proven one of the most useful “whistle” I’ve added so far.
```

This results in the following technical requirements:

- Low bandwith
- Low volume
- High availability

This may be completely different for your installation, so carefully check the requirements.

The initial steps are easy enough:

14.1. Surfstick

To cling to a known name like “HUAWEI” seemed a good approach here, too. I found an unlocked HUAWEI E353 stick for a reasonable price.

Important: whatever stick you have, chances are good that your Pi can not provide enough current for the stick. Plan to buy a powered USB hub anyway.

Inserting the stick may be not so simple, too – in my case the central server is in the basement, connectivity is bad. Enclosing the stick within the distribution box will make things even worse.

In my special case, the stick is attached via a 5m USB cable and resides in the hallway on the ground floor.

Another possible issue: there are surfsticks around that are **not** modems, they identify themselves as complete USB Ethernet devices. Configuration is different for these.

14.2. SIM card

There's a myriad of providers and sub-providers, I can't advise any special of them. What you should take into account in your selection:

- Do I have network coverage where the stick is going to be installed
- Do I need access from outside to the HA system
  This is an important point. Some (if not all) providers and some plans completely disable external access (your stick/your Pi is not visible from the internet side of the world). This means that e.g. a DYNDNS account is not possible. For me this was not a point of concern, as (heavy) external access is not planned and (see chapters below) for special cases there are workarounds.
- Data volume
  You should make some assumptions for the data volume to be expected based on your "driving forces" defined above. For me a low volume account is more than enough.

14.3. Configuration

Here's where trouble begins.

There are a lot of tutorials around – but, at least for me, the information was not really enough to solve the problems that came up. One of the reasons for this is the very complex infrastructure when it comes to networking in linux (at least from my noob point of view). When it comes to "merging" information from different tutorials, be sure all of them base on the same initial networking tools. As far as my basic understanding goes, you will find the following approaches.

- Old fashioned networking is configured via /etc/network – modern approach is via NetworkManager
- Old fashioned WAN access is done via modems (wvdial) and pppd – modern approach is to use QMI
- You can have a wvdial first or pppd first approach
- There are "magic scripts" like the famous "sakis3g" that will fiddle around with the basic infrastructure behind the scenes.

I choose to go by "classic networking via modems, wvdial first", again having many information and well tested settings around. The steps from here seem quite clear from a high level view:

- The stick is inserted and recognized as a modem
- the wvdial software is instructed how to talk to the modem
- when wvdial has setup the modem and initiated a connection, control is handed to pppd
- pppd negotiates the session with the provider and sets up a new network adapter (ppp0).

Now lets look this up in detail.

14.4. Stick configuration

After inserting the stick, try to look it up via *lsusb*

```
pi@wbbase ~ $ lsusb
Bus 001 Device 002: ID 0424:9514 Standard Microsystems Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp.
Bus 001 Device 004: ID 1a40:0101 Terminus Technology Inc. 4-Port HUB
Bus 001 Device 007: ID 12d1:1506 Huawei… E398 LTE/UMTS/GSM Modem/Networkcard
```

With a little luck you find something like this and you're done. Your stick is found and recognized as a modem. You can see this on one hand in the name part or as the nerd that you are you recognize the **ID 12d1:1506.** The first part of the ID is a vendor specific number, here HUAWEI, the second is the device type, here a modem.

Many sticks are recognized as a mass storage device. I found a clever article on this with the following explanation:

"This is a clever default behavior on windows. On the mass storage part we have windows drivers that enable access to the stick, after access the stick is automatically switched to modem mode. Plug and play…"

On the Pi things are different. Here you have to switch the stick yourself. The software doing this is called "usb-modeswitch" (what a surprise). So, if you have only mass storage so far, install it..

```
sudo apt-get install usb-modeswitch
```

After installation and stick insertion you should finally see the modem variant. If not, bad luck. You should really have bought a stick that is already in the standard configuration or that does not need a switch at all. But not all hope is lost, you can add the information yourself – but this is beyond this chapter, look here http://wiki.ubuntuusers.de/USB_ModeSwitch/ for example.

When the stick is recognized as a modem, you should lookup the device name associated with it, you will need this later for the dialer or PPP connection. Having a look in the dmesg after inserting the stick you will find something like this.

```
[2934611.713325] usb 1-1.5.2: new high-speed USB device number 6 using dwc_otg
[2934611.814306] usb 1-1.5.2: New USB device found, idVendor=12d1, idProduct=14fe
[2934611.814331] usb 1-1.5.2: New USB device: Mfr=2, Product=1, SerialNumber=0
[2934611.814349] usb 1-1.5.2: Product: HUAWEI Mobile
[2934611.814365] usb 1-1.5.2: Manufacturer: HUAWEI
[2934611.816789] usb-storage 1-1.5.2:1.0: USB Mass Storage device detected
[2934611.818962] scsi host1: usb-storage 1-1.5.2:1.0
[2934611.819840] usb-storage 1-1.5.2:1.1: USB Mass Storage device detected
[2934611.820235] scsi host2: usb-storage 1-1.5.2:1.1
[2934612.497513] usb 1-1.5.2: USB disconnect, device number 6
[2934618.113327] usb 1-1.5.2: new high-speed USB device number 7 using dwc_otg
[2934618.214538] usb 1-1.5.2: New USB device found, idVendor=12d1, idProduct=1506
[2934618.214564] usb 1-1.5.2: New USB device strings: Mfr=3, Product=2 …
[2934618.214582] usb 1-1.5.2: Product: HUAWEI Mobile
[2934618.214597] usb 1-1.5.2: Manufacturer: HUAWEI
[2934618.218759] usb-storage 1-1.5.2:1.4: USB Mass Storage device detected
[2934618.219301] scsi host3: usb-storage 1-1.5.2:1.4
[2934618.220157] usb-storage 1-1.5.2:1.5: USB Mass Storage device detected
[2934618.220558] scsi host4: usb-storage 1-1.5.2:1.5
[2934618.265855] usbcore: registered new interface driver usbserial
[2934618.266054] usbcore: registered new interface driver usbserial_generic
[2934618.266242] usbserial: USB Serial support registered for generic
[2934618.269213] usbcore: registered new interface driver cdc_ncm
[2934618.275659] usbcore: registered new interface driver cdc_wdm
[2934618.286789] usbcore: registered new interface driver option
[2934618.286983] usbserial: USB Serial support registered for GSM modem (1-port)
[2934618.287328] huawei_cdc_ncm 1-1.5.2:1.1: MAC-Address: 58:2c:80:13:92:63
[2934618.287357] huawei_cdc_ncm 1-1.5.2:1.1: setting rx_max = 16384
[2934618.287755] huawei_cdc_ncm 1-1.5.2:1.1: setting tx_max = 16384
[2934618.288436] huawei_cdc_ncm 1-1.5.2:1.1: cdc-wdm0: USB WDM device
[2934618.290042] huawei_cdc_ncm 1-1.5.2:1.1 wwan0: register 'huawei_cdc_ncm' at \
       usb-3f980000.usb-1.5.2, Huawei CDC NCM device, 58:2c:80:13:92:63
[2934618.290335] option 1-1.5.2:1.0: GSM modem (1-port) converter detected
[2934618.290402] usbcore: registered new interface driver huawei_cdc_ncm
```

```
[2934618.290895] usb 1-1.5.2: GSM modem (1-port) converter attached to ttyUSB0
[2934618.291214] option 1-1.5.2:1.2: GSM modem (1-port) converter detected
[2934618.292108] usb 1-1.5.2: GSM modem (1-port) converter attached to ttyUSB1
[2934618.292291] option 1-1.5.2:1.3: GSM modem (1-port) converter detected
[2934618.292824] usb 1-1.5.2: GSM modem (1-port) converter attached to ttyUSB2
[2934618.414538] huawei_cdc_ncm 1-1.5.2:1.1 wwan0: kevent 12 ..dropped
[2934619.214405] scsi 4:0:0:0: Direct-Access     HUAWEI   SD Storage \
       2.31 PQ: 0 ANSI: 2
[2934619.215258] scsi 3:0:0:0: CD-ROM            HUAWEI   Mass Storage \
       2.31 PQ: 0 ANSI: 2
```

14.5. wvdial

The next step in the old fashioned way is setting up wvdial.

```
sudo apt-get install wvdial
```

There are other alternatives to access the modem, but his one just works fine for me. If you don't like it, maybe have a look at http://www.sakis3g.com/.

wvdial is responsible for communicating with the modem hardware. After connection, work is handed over to pppd.

wvdial uses the configuration at /etc/wvdial.conf. It has also a builtin feature to create a basic default configuration for the currently detected modem. So, as a first step insert the stick and run

```
sudo wvdialconf /etc/wvdial.conf
```

No edit the /etc/wvdial.conf and add a section for the provider you want to dial up at the end. Here's my example

```
[Dialer Defaults]
Init1 = ATZ
Init2 = ATQ0 V1 E1 S0=0 &C1 &D2
Modem Type = Analog Modem
ISDN = 0
Baud = 9600

[Dialer pin]
Modem = /dev/gsmmodem
Init3 = AT+CFUN=1,1
Init4 = AT+CPIN="1234"

[Dialer myprovider]
Modem = /dev/gsmmodem
Init4 = AT+CGDCONT=1,"IP","internet.partner"
Phone = *99#
Username = " "
Password = " "
```

The first section was created initially by the wvdialconf call, I have just removed garbage.

The next section defines the things wvdial should do when I want to set the pin or talk to "unitymedia".

Parameter	Meaning
Modem	The device we are talking to. You can derive this from the messages that you get via dmesg after inserting the stick. Here you see that a ttyUSB0, ttyUSB1 and ttyUSB2 is automatically created.

	The interesting information is that usb-modeswitch additionally installs automatically a device link /dev/gsmmodem So unless this link to the correct tty* is not available, use /dev/gsmmodem. If for some reason this does not work (there seem to be strange conditions in the USB jungle causing this), just try ttyUSB0.
Init<n>	The init strings that are sent to the modem. The first section one unlocks the SIM – you can omit this if your SIM is not PIN protected. While in theory you can include this command within the dial sequence itself, for me it was not possible because a second attempt to authenticate the PIN (when already authenticated) resulted in a modem error. As the PIN is not reset until power off, it was not possible to bounce a connection. Setting the PIN within the wvdial init sequence is one of many options, you can also • remove the PIN from the card • set the pin via a pre-up script. This is a hook within the network configuration that allows you to call scripts before a network adapter is started. The second one identifies and initialized the APN. Setting the correct APN is crucial. Setting the wrong APN not only can lead to malfunction, but can select an endpoint that is not compatible to your data plan and lead to extreme costs!
Username	The username for authentication with your provider. If you need no username it's a little tricky: wvdial does not accept an empty entry. Just adding a dummy entry " " (including the blank) should work.
Password	The password for authentication with your provider. If you need no password, set to " " (including the blank).
Phone	The number to dial. In most cases this will be *99#. See your respective provider manuals.

Setting "Baud" is unnecessary, as the real network speed is negotiated on the PPP level later on.

Depending on your provider you may need to set still other parameters. See the wvdial man page for more.

Running (the "&" is important – the console is not available otherwise after calling)

```
sudo wvdial myprovider &
```

will hopefully result in

```
[ pi@wbbase ~ $ --> WvDial: Internet dialer version 1.61
--> Initializing modem.
--> Sending: ATZ
ATZ
OK
--> Sending: ATQ0 V1 E1 S0=0 &C1 &D2
```

```
ATQ0 V1 E1 S0=0 &C1 &D2
OK
--> Sending: AT+CGDCONT=1,"IP","<APN>"
AT+CGDCONT=1,"IP","<APN>"
OK
--> Modem initialized.
--> Sending: ATDT*99#
--> Waiting for carrier.
ATDT*99#
CONNECT
--> Carrier detected.  Waiting for prompt.
--> Don't know what to do!  Starting pppd and hoping for the best.
--> Starting pppd at Sun Jan 10 16:22:57 2016
--> Pid of pppd: 2808
--> Using interface ppp0
--> local  IP address 10.148.172.74
--> remote IP address 10.64.64.64
--> primary   DNS address 193.189.244.225
--> secondary DNS address 193.189.244.206
```

Don’t worry if you have lines like

```
--> pppd: ð±ôvPÐ[01][08]ï[01][03]
--> pppd: ð±ôvPÐ[01][08]ï[01][03]
```

between, just ignore them.

If everything goes well, ifconfig will show after this a network interface ppp0.

```
ppp0      Link encap:Punkt-zu-Punkt-Verbindung
          inet Adresse:x.x.x.x  P-z-P:x.x.x.x  Maske:255.255.255.255
          UP PUNKTZUPUNKT RUNNING NOARP MULTICAST  MTU:1440  Metrik:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
          Kollisionen:0 SendewarteschlangenlÃ¤nge:3
          RX bytes:458 (458.0 B)  TX bytes:521 (521.0 B)
```

This interface is created by the pppd after getting control from wvdial and negotiating the parameters with the provider.

Do not forget to

```
sudo killall wvdial
```

to end the connection.

If you fail, you will get an error, look it up for further investigation. A typical error (well, hmm, my error) is “error 11” – the SIM is PIN protected. Read the next chapter.

```
--> Sending: AT+CGDCONT=1,"IP","internet.partner"
AT+CGDCONT=1,"IP","internet.partner"
+CME ERROR: 11
--> Bad init string.
```

14.6. SIM PIN

14.6.1. Keep the PIN

If you absolutely want to keep the SIM PIN you have to go the extra mile.

On one hand, I didn’t manage adding the modem PIN command to the wvdial.conf. The second time the PIN authentication is executed the modem will return an error and wvdial will fail. As there is no such thing as an optional wvdial entry, you must enter the

PIN separately. The best bet is here to add it in the /etc/network/interfaces as an pre-up hook script, saved in /opt/admin/setupPIN.sh.

```
#!/bin/bash
echo "AT+CPIN=1234\n\r" > /dev/gsmmodem
```

Then you add to the /etc/network/interfaces in the ppp0 section the last line. Before uping the adapter the PIN will be set.

```
auto ppp0
iface ppp0 inet wvdial
provider myprovider
pre-up /usr/local/bin/setPIN.sh
```

To ease manual PIN unlocking add this section to the wvdial.conf

```
[Dialer pin]
Modem = /dev/gsmmodem
Init1 = AT+CPIN="1234"
```

Now you can manually unlock with

```
sudo wvdial pin
```

14.6.2. Unlock the SIM

The easiest way is to put the SIM in a handy and interactively remove the PIN.

As an alternative you can use “minicom” and send

```
// check
AT+CPIN?
→ +CPIN: PIN

// unlock
AT+CPIN=”<your PIN>”
→ OK

// remove PIN
AT+CLCK=”SC”, 0, “<your PIN>”
→ OK
```

14.7. pppd

PPP (Point to Point Protocol) is a high level protocol between peers (your Pi and the provider endpoint). It has mechanisms to negotiate connection parameters and the IP address.

At the heart of the protocol implementation is pppd - this is called after the modem is connected to the provider by wvdial. wvdial is more of a wrapper for pppd here.

You can configure pppd options when started via wvdial in the /etc/ppp/peers/wvdial config file.

Important options

- defaultroute
  Add a default route for this connection
- replacedefaultroute
  Option to “defaultroute”, replace an already existing defaultroute

- persist
  Do not exit after a connection is terminated; instead try to reopen the connection.
- usepeerdns
  Use the DNS information from the connected server
- holdoff 10
  How many seconds to wait before re-initiating the connection

14.8. Network config

14.8.1. /etc/network/interfaces

```
auto ppp0
iface ppp0 inet wvdial
provider myprovider
pre-up /bin/sleep 30
pre-up /opt/admin/setPIN.sh
```

This configuration launches the “myprovider” entry via wdial upon startup. Before starting the adapter, we wait 30 seconds, then the script setPIN.sh is executed.

14.8.2. Manual shutdown and startup

To manually startup ppp0

```
sudo ifup ppp0
```

An here the shutdown

```
sudo ifdown ppp0
```

14.8.3. The routing table after successful connection

Now lets have a look at the current routing information with “netstat –r”

```
Kernel-IP-Routentabelle
Ziel            Router          Genmask         Flags   MSS Fenster irtt Iface
default         *               0.0.0.0         U         0 0          0 ppp0
10.64.64.64     *               255.255.255.255 UH        0 0          0 ppp0
192.168.42.0    *               255.255.255.0   U         0 0          0 eth0
```

As far as i understood the network mechanics this means that traffic to the network segment 192.18.42.* is routed via the Ethernet card, the rest is sent to the WAN interface. That's ’t.

14.8.4. Provide internet access for all other nodes

Now that our basement server is online, we’d like to share this access throughout our network. It will become a breeze to maintain and update the other network nodes, we will be able to access internet services (let our heating send mails, then…) – pretty much features regarding that this is none of an effort now.

Two things must happen to provide seamless internet access:

- Defining a default gateway for all nodes
- Support NATing the requests from other nodes on the default gateway

a Setting the default gateway

For all other nodes in your network that should have internet access you must add the GSM enabled station as the default gateway, ensuring you have internet everywhere.

This is an additional entry in the /etc/network/interfaces

```
gateway 192.168.41.1
dns-nameservers 8.8.8.8
```

The routing table on the satellites should look like this.

```
Kernel-IP-Routentabelle
Ziel            Router          Genmask         Flags Metric Ref    Use Iface
default         wbbase          0.0.0.0         UG    0      0        0 eth0
192.168.42.0    *               255.255.255.0   U     0      0        0 eth0
```

b Configuring NAT on the default gateway

Now that the other clients have a default gateway, they simply send all IP packets with addresses that do not lie in the local network to the default gateway. And we must tell the gateway what it should do with all the IP packets it will receive – forward to its own default gateway at the internet provider.

First, we have to enable ip forwarding for the system at all. This is done by adding the following line to /etc/sysctl.conf

```
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
net.ipv4.ip_forward=1
```

Then we must add routing rules with the “iptables” command.

```
# add NAT masquerading to output via ppp0
sudo iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
# allow explicitly packet forwarding from eth0 to ppp0
sudo iptables -A FORWARD -i eth0 -o ppp0 -j ACCEPT
# allow packet forwarding from ppp0 to eth0 only if originated from here
sudo iptables -A FORWARD -i ppp0 -o eth0 -m state --state RELATED,ESTABLISHED\
 -j ACCEPT
```

These rules are transient, you have to reenter them after reboot. To make them permanent you should follow these steps

```
sudo iptables-save > ./iptables.dump
sudo mv iptables.dump /opt/admin/iptables.dump
```

This saves the current (all!) settings to a dump file. To restore these settings we create a script that will be executed every time the network comes up.

```
sudo nano /etc/network/if-pre-up.d/iptables-restore
```

This creates a script file “iptables-restore”. Add the following content

```
#!/bin/bash

iptables-restore < /opt/admin/iptables.dump
exit 0
```

This will restore the content of the backup. In order to make it an executable script, you have to make it executable for sure.

```
sudo chmod 755 /etc/network/if-pre-up.d/iptables-restore
```

14.9. Keep alive

While ppd has builtin features to monitor the connection, there seem to be enough scenarios where you should have another check. The following script monitors the existence of an internet connection purely from a client point of view.

Edit and save as /opt/admin/internetMonitor.sh. As always, make the script file executable..

```
#!/bin/bash
    #
    # Restart network interfaces
    # if ppp0 connection is down

    PING="/bin/ping -q -c1 -W 10 -I ppp0"
    HOST=8.8.8.8

    ${PING} ${HOST}
    if [ $? -ne 0 ]; then
            echo "ppp0 is down, try reconnect…"
        /sbin/ifdown --force ppp0
        sleep 10
        /sbin/ifup --force ppp0
        sleep 10
    fi
```

Use crontab to run this script on a regular base – you can lookup the chapter below to find more information on crontab itself.

```
sudo crontab –e
```

This line will run the script every 10 minutes

```
*/10 * * * * /opt/admin/internetMonitor.sh
```

14.10. Auto disconnect

Some providers disconnect your modem on a regular base (every 24h). It may be helpful to automatically restart the connection using a cron script.

14.11. Security

For some providers the Pi now gets a (temporary) public IP address. Be prepared to be visible from the outside world immediately. There are strange guys out there that scan for open SSH ports to login. With a “standard” Pi configuration with active SSH, user “pi” and password “raspberry” it’s a matter of time until you fall prey to one of these – and this is only one of the many attack scenarios.

Securing a server in the internet is really out of scope for this book, only the most important tips:

- Disable all unneeded servers
- Change the default password to strong ones
- If you need SSH, use a public/private key scenario
- Set up a firewall on the Pi. The iptables rules from above are a start, but I don’t know if its enough!

If you see an address in the private IP ranges (e.g. 10.*.*.* like mine), you are not visible from the “outside” (At least for the guys from outside your providers private network. But

the bad guys may be nearby…). This reduces the possibilities of an attack, but now you have serious challenges when you want to remote access your system. More on this later.

14.12. Issues

14.12.1. Modem not detected

Some bloggers have experienced timing problems, so after a reboot the device may not be available for the USB modeswitch. For me this was not a problem so I cannot give advice. These guys tried with a script that restart all devices.

For example (from https://nicovddussen.wordpress.com/2014/11/12/setting-up-your-raspberry-pi-to-work-with-a-3g-dongle/)

```
#!/bin/bash
sleep 1m
udevadm trigger
sleep 1m
Wvdial
```

14.12.2. Network to fast

Another type of problem is the network is up before the device is provided by the kernel (different from above where modeswitch was not able to reconfigure the device). pppd will fail if the modem device is not available. Solution is in this case to wait for the device to appear.

The “wait” script

```
#!/bin/bash
    #INTERFACE="/dev/$(head -1 /etc/ppp/options-mobile)"
    INTERFACE="/dev/$1"
    MAX_SECONDS_TIMEOUT=$2

    dsec=$((${MAX_SECONDS_TIMEOUT} * 10))
    for ((retry=0; retry < ${dsec}; retry++))
    do
        if [ -c ${INTERFACE} ]; then
            echo "$0: OK existing required device ${INTERFACE} (in $((retry /
10)).$((100 * (retry % 10) / 10)) seconds)"
            logger "$0: OK existing required device ${INTERFACE} (in $((retry
/ 10)).$((100 * (retry % 10) / 10)) seconds)"
            break
        else
            sleep 0.1
        fi
    done
    if [ ! -c ${INTERFACE} ]; then
        echo "$0: ERROR timeout waiting for required device ${INTERFACE}"
        logger "$0: ERROR timeout waiting for required device ${INTERFACE}"
        exit 1
    fi
```

The /etc/network/interfaces

```
auto ppp0
iface ppp0 inet wvdial
 provider vodafone
 pre-up /etc/ppp/wait-dialup-hardware gsmmodem 20
```

14.13. More …

The following links have more detailed information on the highly complex (subtopic) of WAN networking.

https://www.debian.org/doc/manuals/debian-reference/ch05.en.html

http://www.tldp.org/HOWTO/PPP-HOWTO/index.html

15. Remote Control

One particularly important topic is remote control. At least in my project, the installation is headless and you have to work with a remote console (if you don't want to run through the house all day and connect your keyboard to another Pi).

So, even when not remote accessing from the internet, access from the LAN is highly recommended. The workhorse of all this is "ssh".

15.1. SSH

15.1.1. Install ssh

Before you can remote connect to your Pi, you must ensure that the ssh daemon is up and running, and correctly configured. In current distributions, ssh should be installed and only has to be activated in the Raspberry initial configuration menu. To restart the configuration use

```
sudo raspi-config
```

A manual install is not hard, though

```
sudo apt-get install ssh
```

Now you can start the ssh server with

```
sudo /etc/init.d/ssh start
```

It is important to add the ssh server to the autostart to have it available after reboot.

```
sudo update-rc.d ssh defaults
```

15.1.2. Basic usage

ssh is the single most important tool to control a standalone, console-less Pi.

You use it primarily to work on the commandline of the "remote" systems. To connect remotely to your Pi you type

```
ssh <host>
```

which will connect you to the target host using the same user as locally.

If you do this for the first time, a prompt will ask you to approve the connection to a still unknown machine. The "fingerprint" is then saved, so you won't be prompted again. Take the prompt for serious, especially if you think that you have established the connection before but suddenly the fingerprint has changed – someone may play dirty tricks on you.

Finally you will have to enter the password for the user on the remote machine.

15.1.3. Important options

Option	Description
-l (lowercase L)	The user on the target host
-p	The port on the target host

15.1.4. Public/Private key

The best way to use ssh is based on public/private key authentication instead of password based authentication. While the procedure seems awkward at first, you will get through it very fast.

First, we create a key pair on (each) Pi and each client that wants to access remotely.

```
ssh-keygen
```

If you answer all questions with a return, this will create a default 2048 bit RSA based key pair in the file /home/<user>/.ssh/id_rsa (which is the private key) and /home/<user>/.ssh/id_rsa.pub (the public key).

Now, whatever way you prefer to do so, you must add the public key you just created to the list of authorized keys in the ssh configuration on the server.

- lookup the .ssh directory in the home directory of the target user on the server (in this case /home/pi/.ssh). If it does not exist, create it (it **must** have the permission set to 0700, owner **must** be the user to which the directory belongs).

```
mkdir .ssh
chmod 0700 .ssh
```

- Here you open the file "authorized_keys" (or create it, permissions **must** be 0600, owner **must** be the user to which the directory belongs)

```
touch authorized_keys
chmod 0600 authorized_keys
```

and simply add the content of the public key file from the client that should be allowed to access to the end.

I've done this for every account in this matrix – this eases life considerably.

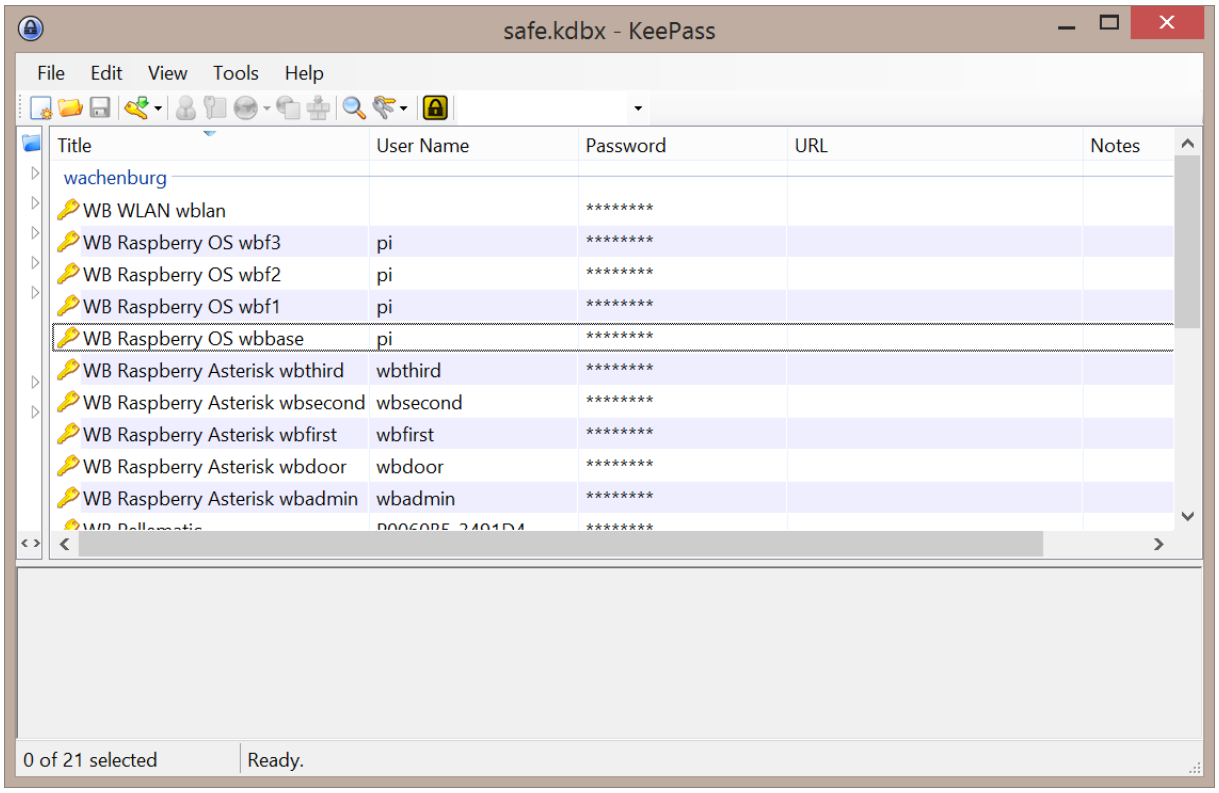
Local \ Remote	wbbase	wbf1	wbf2	wbf3
WinSCP	*	*	*	*
Connect Bot	*	*	*	*
wbbase		*	*	*

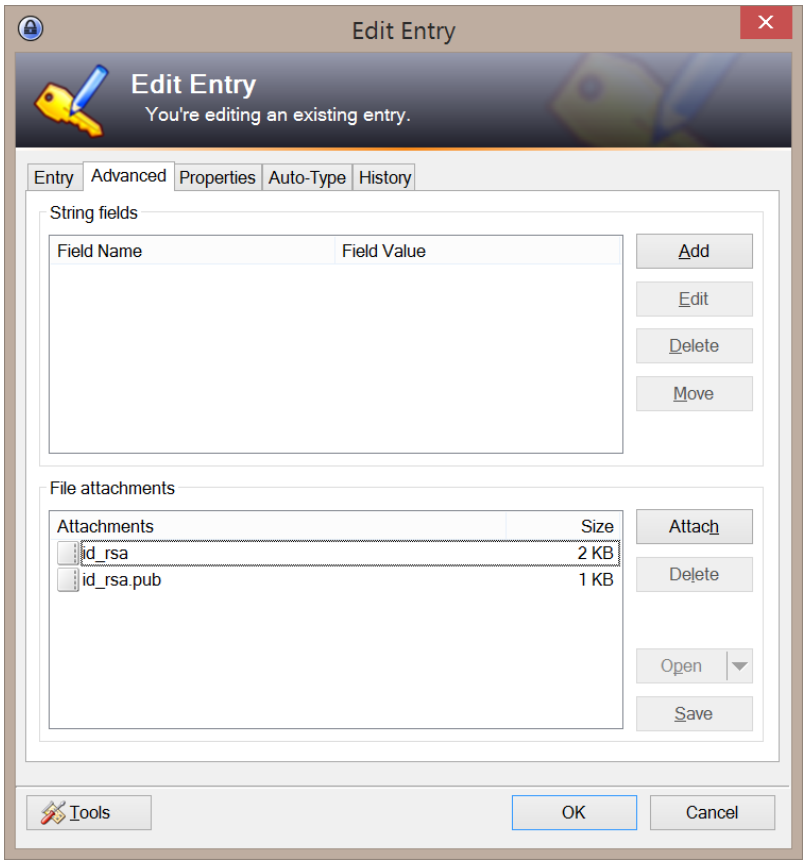
This way I can access any Pi in the house from a console (ssh client) on the machines listed on the left.

To ease later administration, I copy the public key to the samba share for each machine

```
cp /home/pi/.ssh/id_rsa.pub /media/remote/wbdisk/private/admin
```

I recommend to copy the private key, too, and save it a secure place like the Keepass vault.





15.1.5. *SSH daemon*

/etc/ssh/sshd_config

Its considered best practice to disable the ssh login for user “root”.

```
PermitRootLogin no
```

Some guys recommend to change the SSH port from the default 22 to something an intruder might not try to connect to.

```
Port 222
```

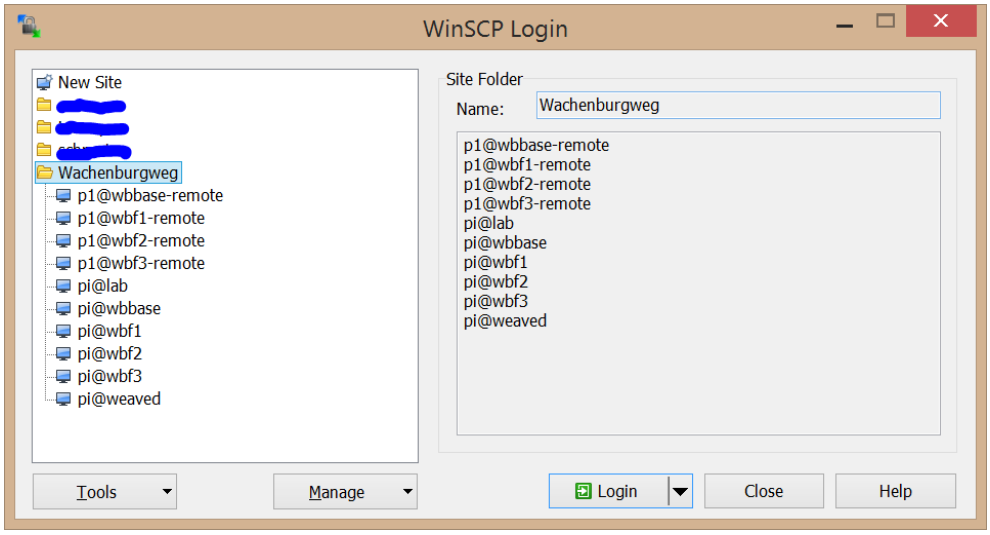
Upon saving you must restart the server.

```
sudo service ssh restart
```

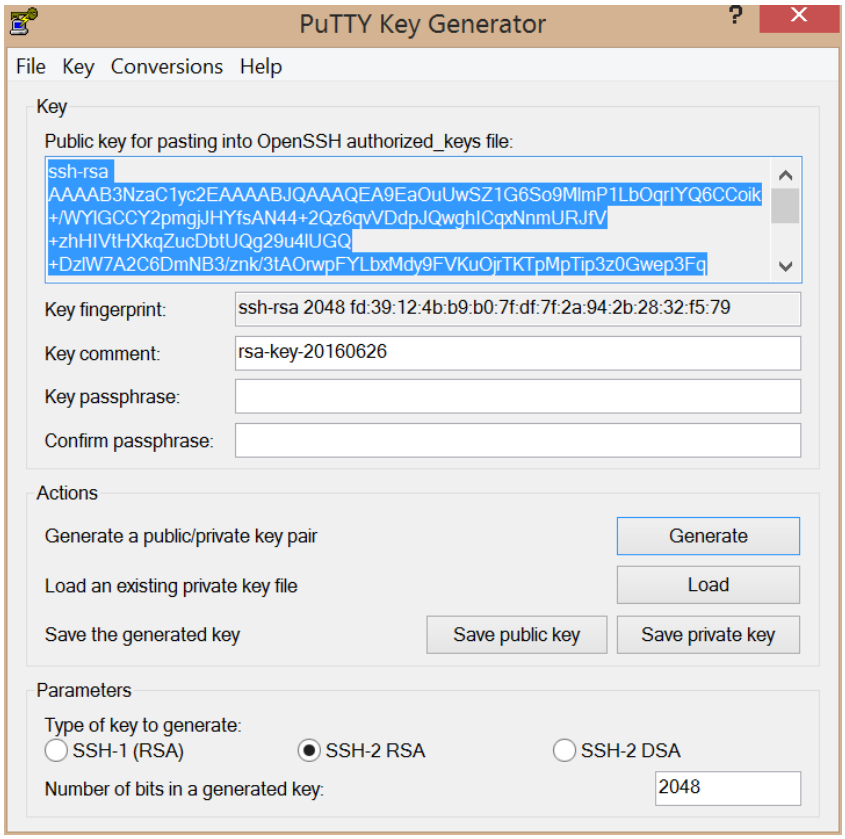
15.1.6. *WinSCP*

If you're using ssh and Windows I can recommend very much Win SCP, a remote "explorer" onto your machine. Combined with "putty", a remote console you have everything you need to efficiently manage your Pi's.

Included with WinSCP is a simle way to create a key pair for installation on your target machines.

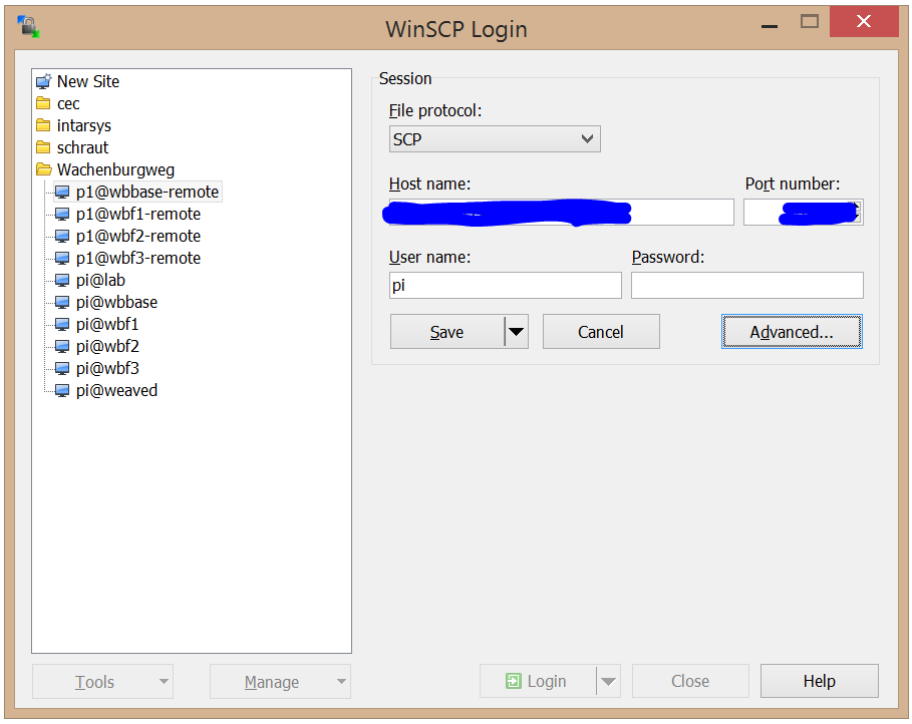


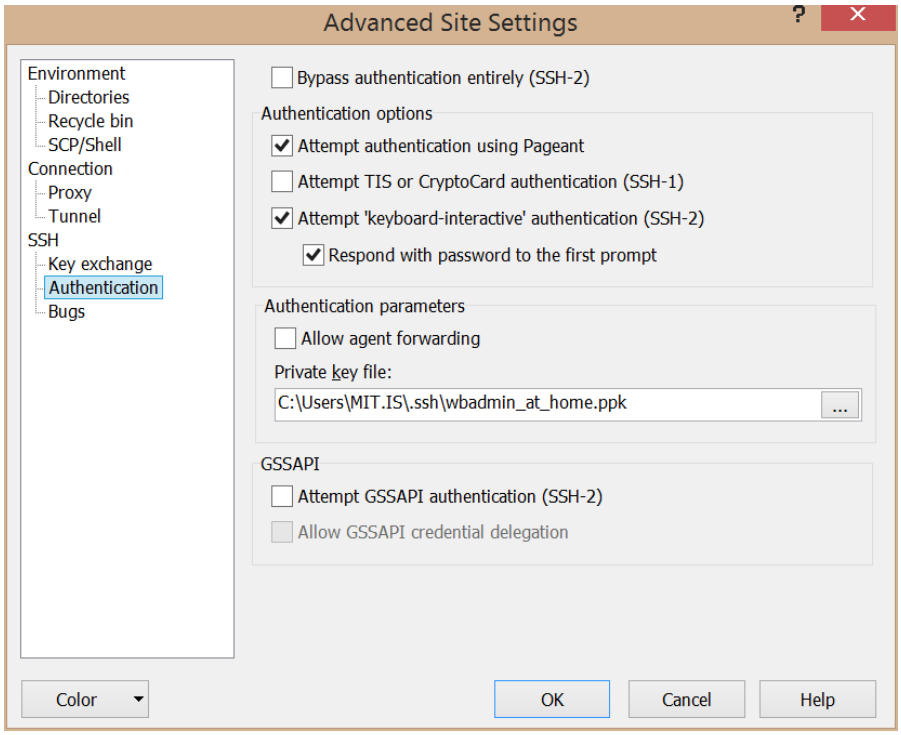
Using the button "Tools", you can start "Puttygen", a simple tools for key generation.



I'd recommend using 208 bit keys, then press "Generate". Save the keys and transport them to the respective clients.

You can configure a configuration by adding a "New Site". Under "Advanced…" you can enter your private key.





Now you are ready to connect to you site using WinSCP and PPK.

15.1.7. ConnectBot

A great additional feature is provided by “ConnectBot”, an SSH client for Android.

Following this easy steps you will get remote control in the palm of your hands

- Install ConnectBot
- Create a key with a meaningful name
- Copy the public key and send it via mail to an account where you can manage the Pi’s authorized keys
- Add the public key to each /home/pi/.ssh/authorized_keys
- Connect via Android…

15.1.8. fail2ban

If your account is in any way visible in the internet you will most certainly encounter malicious login attempts. A very good and simple tool is “fail2ban” in addition to strong passwords and/or ssh via PPK.

Fail2ban will effectively slow down machines trying to break into your account using brute force.

15.2. DynDNS

The next problem you will encounter is the fact that the IP address of your gateway is not static – every time you provider considers a change to be useful, your client receives a new address.

In this case, you can setup “dynamic DNS”. At a DNS service you can register a name (like “www.mydomain.de”) along with an IP address, so any client can find your server using the name only. Dynamic DNS in addition has an API to change the IP address for the name, well, dynamically. Old bindings are not cached. There are a lot of such services

around, the classical one being “dyndns.org”. As they serve no longer accounts for free, you may have to look around for some other. I’m actually using “changeip.com”.

In addition you will have to install a client that will call the service upon a change of the IP address. I cannot recommend any special as I have not installed any.

The problem is: In the case of our WAN connection, life is even more restrictive. Most surfsticks will never ever have a “real” IP address. They have addresses local in a private address range setup by the provider (such as “10.10.10.*”).

You simply cannot reach this components from the internet! To circumvent this, you have to setup more delicate techniques.

15.3. Reverse tunneling

15.3.1. Intro

“Reverse tunneling” is the option in case like our WAN connection or restrictive firewalls around our service.

Instead of calling in the network to machine A, we call out to some external machine B. On B we open a listener that, when contacted, forwards the request to A. In other words, I SSH to a special port on B who will transparently forward to A, tunneled through the already existing connection initiated by A. For my client B is not visible, so I use for example the same PPK credentials like I’d use in a direct connection.

We have a look at two different “reverse scenarios”.

15.3.2. Weaved

I stumbled over “weaved” by hazard. If you’re not into heavy configuration or do not have a server at hand that is under your control and visible in the internet, this is a really useful service.

You can register an account for free and after installation of the Weaved client on your raspberry, you can setup a SSH remote console very easily.

I will not go into details here, but this is really fine for initial steps or under the above mentioned conditions. The service was stable - to be honest, more stable than my own reverse tunnel configuration until today. I do not know what the additional mile is they did go for it…

15.4. SSH Tunneling

15.4.1. Straight tunnel

You use a “straight” tunnel, if you have some services behind a known, reachable gateway that only provides SSH services. Using an SSH tunnel you can access another server and its service through the SSH tunnel.

Using this tunnel you could for example forward a HTTP protocol through the SS service of your Pi to reach some HTTP server (your heating!) in the network.

Option	Description
-f	Go into the background
-N	Don’t execute command on the target machine
-L <localport>:<host>:<port>	when connecting to localport on the local machine ssh will create a tunnel to

	remote host:port service. host is the name of the target known on the ssh server side!

15.4.2. Reverse SSH

In some occasions we want to connect to a service behind some firewall or (in our case of surfstick based WAN connection) behind some NATing box.

```
ssh -fNR *:10122:wbf1:22 tunnel@myserver.com
```

This command will create a port 10122 on the machine myserver.com. When connecting to this port, the connection is forwarded to wbf1:22 as seen from the machine issuing the command.

Option	Description
-f	Go into the background
-N	Don't execute command on the target machine
-R [bind:]<remoteport>:<host>:<port>	when connecting to remoteport on the remote machine ssh will create a tunnel to a local host:port service. host is the name of the machine known on the local ssh side!

15.4.3. autossh

There's a wrapper implementation for ssh that will keep track of your connections itself. First, install autossh

```
sudo apt-get install autossh
```

15.4.4. Add to crontab

Most probably you want to open the tunnels upon every restart, so best is to put the call in the crontab and execute on every reboot.

```
crontab -e
```

Be sure to use the correct crontab – depending on the user you setup your keys for (pi or root) you must execute the script (with "pi" or "root" respectively) which again implies "crontab" or "sudo crontab".

```
@reboot /opt/admin/ssh-tunnel-ssh.sh > /dev/null
```

15.4.5. SSH daemon

By default a forwarded port can only be accessed via "localhost". This means if you have a reverse tunnel opened to your gateway, you can access the service on your gateway, but not from another machine via your gateway. To allow SSH to publish the port to all interfaces, you need to set GatewayPorts=yes in your /etc/ssh/sshd_config

```
GatewayPorts yes
```

The ssh server automatically disconnects a client if no data is transmitted. In the case of our tunnels this is quite annoying – you must restart the tunnels from the console. But

you can't, as you can no longer access the console… You should instruct the server to send keep alive messages to the client to ensure it's still there

```
ClientAliveInterval 30
ClientAliveCountMax 10
```

This will send messages to your client every 60 seconds. If 5 messages are unanswered, the server disconnects.

There's a similar option for the client, too

/etc/ssh/ssh_config

```
ServerAliveInterval 30
ServerAliveCountMax 10
```

After any changes on the sshd_config file, you should restart the service

```
sudo service sshd restart
```

16. Thou shalt not write…

A weak spot of the raspberry (at least regarding stability) is the SD card. Chances are good that after a certain time the card is simply no longer working. From spurious failures to non booting Pi's – everything is possible.

The best bet is to write as few as possible in everyday work, prolonging SD card life.

16.1. Do not write at all

Double check the log level of the components installed. Some of them produce incredible amount of data.

Especially with openHAB check the decision to support historic data.

16.2. Use temporary file system

If you do not want to write to SD, well either do not write at all or do write only to ram.

To do so, you can add entries in /etc/fstab. This entry for example creates a "redirection" for /var/log to the temporary file system of maximum size 1 MB.

Again, consider disabling logging completely if your data will be lost anyway for post mortem analysis. Information on the topic of "sustainable SD card use" you will find in the respective configuration sections of the software components.

And consider that a tmpfs may run out of space, too.

```
none        /var/log        tmpfs   size=1M,noatime         00
none        /var/run        tmpfs   size=1M,noatime         00
```

"noatime" is an important flag for other file systems, too. It simply says "do not record time of last file access".

Be ware that logging to RAM will loose information from subsystems like apt, too, that record the installation history from your system.

You will find more on the topic of log optimization in a later chapter.

16.3. Disable swap

```
sudo dphys-swapfile swapoff
sudo dphys-swapfile uninstall
sudo update-rc.d dphys-swapfile remove
```

16.4. Reduce system logging

Replace log management with busybox one

apt-get install busybox-syslogd; dpkg --purge rsyslog

This will put log into circular memory buffer, you will able to see log using logread command

17. Tweak Raspbian

17.1. Install minicom

```
sudo apt-get install minicom
```

- ttyUSB0 locked

17.2. Install screen

```
sudo apt-get install screen
```

Strg-a ?	help	Zeigt den eingebauten Hilfebildschirm
Strg-a 0..9	select	Schaltet zum Bildschirm 0..9
Strg-a A	title	Erlaubt dem User, dem aktuellen Bildschirm einen Namen zu geben.
Strg-a c	create	erzeugt einen neuen von Screen verwalteten Bildschirm
Strg-a d	detach	Beendet den screen prozess, der die Session und das Terminal verbindet
Strg-a "	windowlist -b	Listet alle Fenster der aktuellen Session
Ctrl-a" "H"		Log session

```
screen -ls

Liste der laufenden screens

screen -r

Reattach to a screen
```

17.3. Hostname

```
sudo hostname -b {NEUERNAME}
```

Unter Umständen ist es damit allerdings nicht getan. Man sollte noch einen Blick in die hosts-Datei werfen.

cat /etc/hosts

Wenn dort noch der alte Hostname drin steht, dann muss man den in dieser Datei auch noch ändern.

sudo nano /etc/hosts

17.4. Disable root login

sudo passwd -d root ???

17.5. Memory

Die einfachste Art und Weise, die Speicherverteilung zu ändern, ist der Weg über "raspi-config". Hier gibt es einen dafür vorgesehenen Menüpunkt.

sudo raspi-config

In den "Advanced Options" gibt es den Menüpunkt "Memory Split". Dort kann man die Speichergröße für die GPU einstellen. Der geringstmögliche Wert ist "16" MByte.

Damit die Änderung Wirkung zeigt, muss der Raspberry Pi neu gestartet werden.

17.6. Move root file system

If you really have extreme requirements, you even can move the root file system. I will not go into detail here, some good tutorials are around.

17.7. Watchdog

The Pi CPU has a builtin “watchdog”. You can use this feature to automatically reboot the Pi if chances are good that it is stale anyway.

To understand the feature and its implications you must be aware that we talk of different parts

- The watchdog itself
  This is a hardware feature on the chip, accessible via /dev/watchdog after installation of the kernel module
- The watchdog activation
  Writing to /dev/watchdog wakes the dog and it will wait for more food on this device. If it gets none, it will reset.
  On the Pi the maximum hardware delay is about 16 sec. I did not find any information on how to set the hardware timer, so I just use the defaults.
- The watchdog daemon
  The watchdog is not particularly picky about who is feeding him. You can write a tool that satisfies your logic and do it yourself. Good news is that there’s a generic watchdog daemon available that should handle most of the tasks. It follows your instructions and writes to /dev/watchdog

In conclusion take care of the following before activating the watchdog or its daemon:

- Be sure you can feed the dog in a timely manner after the first write. If e.g. launching the “feeder” takes too long, your Pi may stuck in reboot.
- Be sure the conditions in the watchdog daemon can be fulfilled
  This is especially true for network devices (that may not yet be up at this moment) and file monitoring (because the owning processes are not yet up). Take care of your launch sequence.
- Be sure you can handle the watchdog if your Pi is under service. If your watchdog is on and you stop and start e.g. “openHAB” after configuration change, it’s easy to see your Pi restart because of log inactivity.

Activate watchdog and install daemon

```
sudo modprobe bcm2708_wdog
echo "bcm2708_wdog" | sudo tee -a /etc/modules
sudo apt-get install watchdog
sudo update-rc.d watchdog defaults
```

Change config in /etc/watchdog.conf, remove at least “#” hashmark from the following entries

```
watchdog-device        = /dev/watchdog
max-load-1             = 24
```

If the load goes over “24 raspberrys” over 1 minute (this means that you would have needed more than 24 Raspberry Pis to complete that task in 1 minute) the watchdog will reset the Pi.

For more information see

```
http://linux.die.net/man/5/watchdog.conf
```

The first time start

```
sudo /etc/init.d/watchdog restart
```

You can do a lot of things more with the watchdog daemon, especially it can have a look at files that get touched within a certain period. Tuning the dog is beyond this paper.

18. What time is it?

18.1. Network Time

```
sudo apt-get install ntp
```

update-rc.d ntp defaults

```
pi@wbbase ~ $ sudo service ntp start
[ ok ] Starting NTP server: ntpd.
pi@wbbase ~ $ date
Do 14. Jan 02:18:11 CET 2016
```

and shortly after…

```
pi@wbbase ~ $ date
Mo 18. Jan 21:09:48 CET 2016
```

Reducing traffic

```
server 0.debian.pool.ntp.org iburst minpoll 9 maxpoll 11
server 1.debian.pool.ntp.org iburst minpoll 9 maxpoll 11
# server 2.debian.pool.ntp.org iburst
# server 3.debian.pool.ntp.org iburst
```

```
tinker panic 0
```

```
server 192.168.42.1
```

monitor ntp

```
ntpq -pn
```

19. Improve logging

19.1. Log to temporary file system

```
tmpfs     /var/log        tmpfs   size=1M,noatime,nodiratime,mode=0755    00
```

19.2. Log to external disk

Now we have some prerequisites to improve the logging still further and we move the important logs simply to the private share on the harddisk.

To be flexible we provide a complete directory on the private Samba share that will receive “working stuff” from the clients. Add this to /etc/fstab after creating the directory /var/remote locally.

```
# mount a directory for working stuff that can be moved to the server
/media/remote/wbdisk/private/var  /var/remote  none  _netdev,bind  0  0
```

When the Samba share is available, all data should be written to the hard disk. It’s important to add the “_netdev” flag in order to wait for the network is up.

Now add another subdirectory “log” to /var/remote after mounting. We will use this as a new base directory for all subsystems whose log is large and/or in some way interesting.

To check if everything was alright, you can

```
touch /var/remote/log/test
```

The file “test” should have been created on the harddisk at “srv/wbf1/var/log” (if you have made this experiment from the wbf1 machine).

any service that wants to log to samba share must add dependency to `$remote_fs`

19.3. Tweak logrotate

Logrotate is the little tool that monitors log files on a regular base and rotates them according to the rules defined in /etc/logrotate.conf and the included rule sets in /etc/logrotate.d/*

For this project the constraints are:

- I want to log on a temporary file system to avoid SD wear out.
- To avoid overflow on the tmpfs, we must logrotate early
- Rotated files are moved immediately to an attic folder, again to preserver tmpfs space
- Where possible, logs are created on a Samba share from the start

From the requirements results this default configuration

```
daily
rotate 1
dateext
dateformat .%Y%m%d.back.log
ifemtpy
missingok
create
```

After rotating I want to transfer the now rotated files to the attic on the Samba share. This could be done using a cron job, but I include it in the “postrotate” section to have the log related config in one place. “postrotate” must be defined on a per log file definition, not in the default. So I include with every log file I want to backup

```
postrotate
 mv /var/log/<optional path>/*.back.log /var/remote/log/<optional path>
endscript
```

You should then go through /etc/logrotate.d/* and adapt any setting that should follow this convention.

In addition I removed most of the redundant logs from rsyslog.conf. Having everything in syslog is fine with me

```
#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                    /var/log/auth.log
*.*;auth,authpriv.none             -/var/log/syslog
#cron.*                     /var/log/cron.log
#daemon.*                   -/var/log/daemon.log
#kern.*                     -/var/log/kern.log
#lpr.*                      -/var/log/lpr.log
#mail.*                     -/var/log/mail.log
#user.*                     -/var/log/user.log
```

To force logrotate to evaluate the definitions immediately you can call

```
logrotate --force /etc/logrotate.conf
```

which will rotate every log file (regardless of rule evaluation).

19.4. Move logs

19.4.1. rsyslog

We tweak the postrotate a little bit here to get all rotated logs to /var/remote

```
/var/log/syslog
{
 postrotate
        invoke-rc.d rsyslog rotate > /dev/null
        mv /var/log/*.back.log /var/remote/log
 endscript
}

/var/log/mail.info
/var/log/mail.warn
/var/log/mail.err
/var/log/mail.log
/var/log/daemon.log
/var/log/kern.log
/var/log/auth.log
/var/log/user.log
/var/log/lpr.log
/var/log/cron.log
/var/log/debug
/var/log/messages
{
 sharedscripts
 postrotate
        invoke-rc.d rsyslog rotate > /dev/null
        mv /var/log/*.back.log /var/remote/log
 endscript
```

```
}
```

19.4.2. apt

```
/var/log/apt/*.log {
 postrotate
        mv /var/log/apt/*.back.log /var/remote/log/apt
 endscript
}
```

Don't forget to create /var/remote/log/apt

19.4.3. dpkg

```
/var/log/dpkg.log {
 create 644 root root
 postrotate
        mv /var/log/*.back.log /var/remote/log
    endscript
}
/var/log/alternatives.log {
 create 644 root root
 postrotate
        mv /var/log/*.back.log /var/remote/log
    endscript
}
```

19.4.4. ppp

```
/var/log/ppp-connect-errors {
 nocreate
 postrotate
        mv /var/log/*.back.log /var/remote/log
 endscript
}
```

19.4.5. samba

```
/var/log/samba/log.smbd {
 postrotate
        /etc/init.d/samba reload > /dev/null
        mv /var/log/samba/*.back.log /var/remote/log/samba
 endscript
}

/var/log/samba/log.nmbd {
 postrotate
        [ ! -f /var/run/samba/nmbd.pid ] || kill -HUP `cat
/var/run/samba/nmbd.pid`
        mv /var/log/samba/*.back.log /var/remote/log/samba
 endscript
}
```

Don't forget to create /var/remote/log/samba

???does not work ???

19.4.6. msmtp

First we move the logfile to the remote location right from the start and edit /etc/msmtprc

```
logfile /var/remote/log/msmtp.log
```

Then we change the logrotate.d configuration

```
/var/remote/log/msmtp.log {
 su root root
 rotate 7
 copytruncate
}
```

19.4.7. *asterisk*

Asterisk logging is quite complex and offers a lot of alternatives. To stick with a simple one use the same look&feel as our other components, we simply switch the asterisk log to the samba share and have a look at the logrotate instructions.

Asterisk's log directory is determined in /etc/asterisk/asterisk.conf. We simply change the astlogdir

```
…
astlogdir => /var/remote/log/asterisk
…
```

We want the log to reside on the samba share from the start.

B.t.w. log contents are configured in /etc/asterisk/logger.conf. We leave it alone.

```
/var/remote/log/asterisk/debug /var/remote/log/asterisk/messages
/var/remote/log/asterisk/full /var/remote/log/asterisk/*_log {
 su root root
 daily
 missingok
 rotate 7
 sharedscripts
 postrotate
              /usr/sbin/invoke-rc.d asterisk logger-reload > /dev/null 2>
/dev/null
 endscript
}
```

The logrotate instructions should look like this. As we are already on the samba share, you may only want to switch to, lets say, 1 week of logs. Note the "remote/" subdirectory!

19.4.8. *hmland*

We tweak the init-d script to switch the log directory

```
 chrt 50 /opt/hmcfgusb/hmland -r 0 -d -I -P -l 127.0.0.1 -p $port 2>&1 | perl
-ne '$|=1; print localtime . ": [hmland] $_"' >> /var/remote/log/hmland.log &
```

logrotate??

19.4.9. *homegear*

To keep the log files in production small, we reduce the log level. It's not directly documented, but according to some forum threads, lowering the level means less detail.

/etc/homegear/main.conf

```
# Default: debugLevel = 3
# higher values means more details
```

```
debugLevel = 2
…
logfilePath = /var/remote/log/homegear
```

A nasty detail with homegear: in the init.d script there's also a reference to the log file path, so you have to change it twice.

/etc/init.d/homegear

```
CONFIGPATH=/etc/homegear
DAEMON=/usr/bin/homegear
PIDPATH=/var/run/homegear
PIDFILE=$PIDPATH/homegear.pid
DBPATH=/var/lib/homegear
LOGPATH=/var/remote/log/homegear
```

And, be sure to try it twice: homegear does not start when the log directory is not present, create the "homegear" subdirectory in /var/remote/log !!! My tenant knows, he's rooms have been getting quite cold..

Now have a look at the logrotate instructions at /etc/logrotate.d/homegear. Again, as we are already on the samba share, we do not need to think about space restrictions as much, so we stick with a 1 week rolling behavior, too. Keep in mind that all defaults are in place.

```
/var/remote/log/homegear/*.log /var/remote/log/homegear/*.err {
 su root root
 rotate 7
 sharedscripts
 postrotate
        /etc/init.d/homegear reload > /dev/null
 endscript
}
```

Take care of the "remote/" subdirectory. Be sure to have "homegear" created.

19.4.10. openHAB

openHAB is (as always?) the exception to the rule. With its platform independent character it comes along with its own builtin rotation strategy.

Here, too we want to minimize log file writing.

First step is to edit "<openhab>/configurations/logback.xml. For me I will start a single, simple log at "INFO" level, rotating every day and keeping a history of 2 days. It looks like this

```
<configuration scan="true">

 <appender name="FILE"
class="ch.qos.logback.core.rolling.RollingFileAppender">
        <file>/var/log/remote/openhab/openhab.log</file>
        <rollingPolicy
class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
               <!-- weekly rollover and archiving -->
               <fileNamePattern>/var/log/remote/openhab/openhab-%d{yyyy-MM-
dd}.log.zip</fileNamePattern>
               <!-- maximum number of archive files to keep -->
               <maxHistory>2</maxHistory>
        </rollingPolicy>
        <encoder>
```

```
                <pattern>%d{yyyy-MM-dd HH:mm:ss.SSS} [%-5level] [%-20.20logger]
- %msg%n</pattern>
        </encoder>
  </appender>

  <logger name="javax.jmdns" level="OFF"/>
  <logger name="OSGi" level="OFF" />
  <logger name="org.atmosphere.cpr.AtmosphereFramework" level="OFF" />
  <logger name="org.atmosphere.cpr.DefaultAnnotationProcessor" level="OFF"/>

  <root level="INFO">
        <appender-ref ref="FILE" />
  </root>

</configuration>
```

You can do a lot of additional things with logback that may be interesting in this use case, e.g.

- Change log level
- Change log file
- Write to syslog
- Network logging
- Change rolling strategy and history

You should refer to the logback web site for detailed information.

The second source of logging events stems from jetty. It logs each and every request to a web resource (which may be much…). I don't need this in production, so I switch it off completely.

See <openhab>/etc/jetty.xml

```
  ...
    <Set name="handler">
      <New id="Handlers"
class="org.eclipse.jetty.server.handler.HandlerCollection">
        <Set name="handlers">
         <Array type="org.eclipse.jetty.server.Handler">
           <Item>
             <Ref id="Rewrite" />
           </Item>
           <Item>
             <New id="Contexts"
class="org.eclipse.jetty.server.handler.ContextHandlerCollection"/>
           </Item>
           <Item>
             <New id="DefaultHandler"
class="org.eclipse.jetty.server.handler.DefaultHandler"/>
           </Item>
           <!-- disable request log
           <Item>
             <New id="RequestLog"
class="org.eclipse.jetty.server.handler.RequestLogHandler"/>
           </Item>
           -->
         </Array>
        </Set>
      </New>
    </Set>
  …
```

In addition you **must** comment out the section with the “Ref” to “RequestLog”, as this is now no longer a valid reference.

logrotate

```
/var/remote/log/openhab.log {
 su root root
 rotate 7
 copytruncate
}
```

20. Network monitoring

Now, having attached a surfstick and doing all kind of traffic, you may be interested in some details regarding the connection. The tool of choice is here “vnstat”, a simple console tool that allows to monitor your network interfaces.

If you’re into sophisticated user interfaces, charts and the like, you should go for tools like “ntop”. For my project vnstat is just the right size.

As always install from the repo

```
sudo apt-get install vnstat
```

With regard to the “SD less” system, you should tweak the configuration file at /etc/vnstat.conf. Change the following entries

```
DatabaseDir "/var/remote/lib/vnstat"
???
```

Do not forget that you must create the directory you referenced above. After this you bounce the service

```
sudo service vnstat restart
```

Now you can create a new database for collecting the information

```
sudo vnstat -u -i ppp0
```

As we want to monitor the WAN traffic, ppp0 is used as the target interface.

20.1. Show statistics

After a while you can start reading useful output with daily, weekly and monthly statistics using the –d, -w and –m option

```
vnstat -i ppp0 -m
```

There are some other options, so play around. For the visual types you can even create images using “vnstati”.

20.2. Send statistics

A interesting option is an automatic notification mail about the traffic at the end of the month. Just combine the “vnstat” command and “mail” in a crontab entry.

This is the script you create that is finally called by crontab ((opt/admin/notifyVnstat.sh)

```
#!/bin/bash
(echo "Subject: ppp0 network statistics"; vnstat -i ppp0 -w) | msmtp pi
```

The output of “echo” and “vnstat” is combined to a valid SMTP message content and piped to msmtp, which we installed earlier.

Now we add to crontab, calling

```
sudo crontab -e
```

This line will call the notify once a week.

```
0 0 * * 0 /opt/admin/notifyVnstat.sh > /dev/null
```

21. Data logging

21.1. Data sources

21.1.1. Pi data

21.1.2. openHAB data

openHAB has a well documented REST interface. It allows reading and writing item data and sending commands. While a push interface is available, this is out of scope here.

The main url or the rest API is

```
http://<host>:8080/rest
```

where host is one of ma wbf1, wbf2 or wbf3 hosts with openHAB.

You can select the content, I'm using JSON, so adding the header

```
Accept: application/json
```

Service	
	/rest/items
Method	
	GET
Request Data	
Response Data	
	Array of items • type • name • state

Service	
	/rest/items/<item name>/state
Method	
	GET
Request Data	
Response Data	
	item state string

Service	
	/rest/items/<item name>/state
Method	
	PUT
Request Data	
	New item state as string
Response Data	

```
curl \
  http://wbf1:8080/rest/items/wbf1_kitchen_therm0_tempAct/state  \
  --verbose
```

21.1.3. *Heating data (Ökofen pellematic)*

A very interesting feature is integration of heating sensor data. Most modern systems have some kind of API for home automation integration, most of them plain Web forms or REST services.

My system, an Ökofen pellematic, has a “hybrid” web interface that combines a web page for login and Ajax based services for providing the data.

Such a system can be very easily integrated by emulating the browser protocol, the browser protocol can easily be reverse engineered by using a modern browser, in my case Chrome. Open the developer tools and record the requests. With Chrome a very interesting feature is to save a request in “curl” format. curl is a commandline HTTP client and is the perfect tool for this task.

Lets look at the examples first. We add the –verbose flag, so you can insepct the protocol information in more detail. Here's the logon, saving the session cookies in a jar using the “—cookie-jar” argument…

```
curl
 http://192.168.42.2:8080/index.cgi
 --verbose
 --cookie-jar pellematic
 --data "username=<user>&password=<password>&language=en&submit="
```

Now we are authenticated, the cookies are injected in the following requests using the “—cookie” argument. Now we can request the sensor information.

```
curl
 'http://192.168.42.2:8080/?action=get&attr=1'
 --verbose
 --cookie pellematic
 -H 'Content-Type: application/x-www-form-urlencoded'
 -H 'Accept: application/json, text/javascript, */*; q=0.01'
 -H 'Connection: keep-alive'
 --data '[
        "CAPPL:LOCAL.L_aussentemperatur_ist",
        …,
        "CAPPL:LOCAL.L_zaehler_fehler"
 ]'
```

And this is the result.


```
[
{
"formatTexts":"",
"shortText":"???",
"unitText":"°C",
"lowerLimit":"???",
"upperLimit":"???",
"name":"CAPPL:LOCAL.L_aussentemperatur_ist",
"value":"16",
"divisor":"10",
"status":"OK",
"unitTextImperial":"°F"
},
{
"formatTexts":"Dauerlauf|Start|Zuendung|…|Aus",
"shortText":"???",
"unitText":"???",
"lowerLimit":"",
```

```
"upperLimit":"",
"name":"CAPPL:FA[0].L_kesselstatus",
"value":"99",
"divisor":"",
"status":"OK",
"unitTextImperial":"???"
},
…
]
```

Let's analyze this in detail.

You request data points using a list of their names in JSON format (lets ignore the fact, that the Content-type is wrong ☺)

Service	
	/?action=get&attr=1'
Method	
	POST
Request Data	
	Array of data points names in JSON format
Response Data	
	Array of data point result objects. We will read the following object properties • name • value • divisor • status

You can set, data points, too

…

21.1.4. Internet data

21.2. Data sinks

21.2.1. Plain RRD

rrdTool is a de facto standard when it comes to collection data, so it's a piece of cake to get it up and running. Just kidding…

To be honest, as always in the hackers world the tools are fragmented and you have to collect the pieces together… at least in the windows world.

Get the epoch

http://www.epochconverter.com/

perl -e "print time"

If you want to estimate the size of the resulting database, you may use the online calculator at http://eccentric.slavery.cx/misc/rrdcalc.html.

install rrd

sudo apt-get install rrdtool python-rrdtool

check last update

rrdtool lastupdate filename

show database info

rrdtool info filename

fetch information

rrdtool fetch filename

21.2.2. *Outside temperature*

For the outside, I store one value per hour, only the average over 6 data points. I keep this for 2 years. I plan to push a new value every 10 minutes and allow for one missing data point.

```
rrdtool create /media/remote/wbdisk/shared/rrd/environment.rrd
  --start now-1h
  --step 600
  DS:temp_outside:GAUGE:1200:-30:50
  RRA:AVERAGE:0.5:6:17520
```

21.2.3. *Heating*

The heating provides many data points to control its effectiveness.

4320 = 1measure/[10 min] * 6 * 24 *30

17520 = measure/[1h] * 24 * 365 * 2

```
rrdtool create /media/remote/wbdisk/shared/rrd/heating.rrd
  --start now-1h
  --step 600
  DS:count_burner_start:COUNTER:1200:U:U
  DS:temp_burner_act:GAUGE:1200:-30:500
  DS:temp_floor_act:GAUGE:1200:-30:500
  DS:temp_floor_nom:GAUGE:1200:-30:500
  DS:temp_water_act:GAUGE:1200:-30:500
  DS:temp_pump_off_act:GAUGE:1200:-30:500
  DS:temp_pump_on_act:GAUGE:1200:-30:500
  RRA:AVERAGE:0.5:1:4320
  RRA:AVERAGE:0.5:6:17520
```

21.2.4. *Room data*

10080 = 1measure/[1 min] * 60 * 24 *7

17520 = 1 measure/[1h] * 24 * 365 * 2

```
rrdtool create /media/remote/wbdisk/shared/rrd/wbf1_roomR.rrd \
  --start now-1h \
  --step 60 \
  DS:humidity:GAUGE:300:0:100 \
  DS:temp_act:GAUGE:300:-30:500 \
  DS:temp_set:GAUGE:300:-30:500 \
  DS:valve:GAUGE:300:0:1 \
  RRA:AVERAGE:0.5:1:10080 \
  RRA:AVERAGE:0.5:60:17520
```

21.2.5. rrdtool graphing

```
#!/bin/bash
#

rrdtool graph environment.png \
-w 600 -h 400 -a PNG \
--slope-mode \
--start -86400 --end now \
--font DEFAULT:7: \
--title "Heating" \
--vertical-label "Temperature" \
--lower-limit -10 \
--x-grid MINUTE:10:HOUR:1:MINUTE:120:0:%R \
--alt-y-grid --rigid \
DEF:temp_outside=/media/remote/wbdisk/shared/rrd/environment.rrd:temp_outside:
AVERAGE \
LINE1:temp_outside#0000FF:"Aussen"
```

21.2.6. openHAB persistence

21.2.7. Hosted cloud services

21.2.8. Own services

21.3. Data visualization

22. Event notifications

22.1. Sending eMail

Still the most important channel (well, for me) is email, so we set up this one first.

As always in this project, mailing is a really complex component and you have many software packages around. To give a rough (and maybe a bit simplifying overview):

- you create a mail using a mail user agent (MUA)
- the mail is sent to a mail submission agent (MSA)
- the MSA calls the mail transfer agent (MTA) and asks him to send the mail to its final or intermediate destination at a mail server (a remote MTA)
- the mail server acts either as a relay and still forwards to another server or is the final destination. In this case the mail is put in the target box by the mail delivery agent (MDA)
- now a user can use her mail client to access the post box.

The protocol used for sending the mail is SMTP, the protocols to read mail via the mail client are usually POP3 or IMAP. The different roles in this game can be implemented by only a single large software component or by different specialized ones.

In theory you could connect to your target mail host directly and “push” your mail. Too bad that in the meantime sending spam is a real plague and most servers will no longer accept mail from you directly. It may get quite complicated to setup a MTA with direct internet access and keep it online – believe me, I’ve been there.

I don’t need server or relay features and no local postboxes. I just want to

- send mails from the Pi world to the outside
- receive the Pi “local” mails (e.g. mail to from crontab to root) in my regular mail infrastructure

To achieve this you don’t need to install full blown MTA like Postfix or Exim, you need a tool that can send all your mail messages to a friendly server that takes care of forwarding them to whomever may be concerned. These servers or relays are often called smarthosts.

One such smarthost is provided by Google and in the next steps a Google account is provided as example. The same scheme applies to other providers.

Most tutorials I found install “ssmtp” a quite small tool that worked without much hassle. Here are the basic steps to do so.

Install the MTA “light”

```
sudo apt-get install ssmtp
```

Install the MUA

```
sudo apt-get install mailutils
```

Now we edit the configuration file at /etc/ssmtp/ssmtp.conf

```
root=<mail address to receive system mails>
mailhub=smtp.gmail.com:587
hostname=wbbase
```

```
AuthUser=<yourname>@gmail.com
AuthPass=<yourpassword>
UseSTARTTLS=YES
```

If you use a Gmail account as a smarthost, be sure to enable the setting “Allow less secure applications” in your account setting, your mail will not be delivered otherwise.

Again, there are some additional features that you can explore in some spare time…

```
echo “Test text” | mail -s “Test Mail” targetperson@example.com
```

```
Change the 'From' text by editing /etc/passwd to receive mail from 'root at
myhost' instead of just 'root'.
# chfn -f 'root at myhost' root
# chfn -f 'mainuser at myhost' mainuser
```

Now that you have mail set up on your Pi, you may find out that there’s a mail for each cron job.

```
>/dev/null 2>&1
```

If you want to change the name of the sender when mailing on behalf of a system user, you can do this by setting the user’s name:

1

2

sudo chfn -f root.homeserver root

sudo chfn -f myuser.homeserver myuser

Failed messages are placed in dead.letter in the sender's home directory.

22.1.1. *msmtp*

/etc/msmtprc

```
defaults
auth on
tls on
tls_trust_file /etc/ssl/certs/ca-certificates.crt
logfile /var/remote/log/msmtp.log
aliases /etc/aliases

# gmail
account gmail
host smtp.gmail.com
port 587
from foo@gmail.com
user foo@gmail.com
password 1234

account default : gmail
```

Part IV

This is the part about dreaming. What could we add to make this a real reference installation. I hope many of the following topics will make it to part III one fine day.

23. More event notifications…

23.1. Sending SMS

23.2. Twitter

23.3. Push message platforms

24. Adding a UI device

25. Alternate actor technology

26. Access control

27. Irrigation control

28. RTC

Part V

These are the appendices, a bunch of information added for reference purposes.

29. Troubleshooting

- have a backup around
- fstab tmp too small
- update-rc.d –f ntp remove
- touch definition files
-

30. Abbreviations

Abbreviation	Meaning
HA	Home Automation
SBC	Single Board Computer

31. *nix 101

31.1. Package management

31.2. mount

To reload after changes

```
mount -a
```

31.3. shebang

The first line of a script file can be used as special marker to identify the interpreter context to execute the file content.

```
#!/bin/sh
```

This will for example execute as a plain shell script.

History explains this as a concatenation of sharp (the '#' sign) and bang (the unix slang for the '!').

31.4. python

sudo apt-get install python-pip

sudo pip install requests

```
#!/usr/bin/python
```

make executable!

31.5. Users & Passwords

31.5.1. Change password

You can change your password using

```
passwd
```

You'll be prompted to enter your current password, then asked for a new passwordand a confirmation. Once your new password is verified, you'll be shown a success message and it will be immediately in effect.

31.5.2. Remove password

In certain occasions you may want to remove a users password (wich means he can not login), especially you may want to remove the possibility for the user "root" to login interactively.

```
sudo passwd root -d
```

31.5.3. Create a user

To create an additional user "foo" you can

```
sudo adduser foo
```

This will add a new user after prompting for a new password.

31.5.4. Remove a user

If you want to get rid of a user, type

```
sudo userdel -r foo
```

The “-r” option will remove the home folder, too.

31.6. Service Management

Deactivate

```
sudo service {dienst} stop
sudo update-rc.d -f {DIENST} remove
```

Activate

```
sudo update-rc.d {DIENST} defaults
```

31.7. Send command to background

&

31.8. Concatenatign output

`( command1 ; command2 ; command3 ) | cat`

31.9. whoami

31.10. groups

31.11. rm

rm removes a file or directory

Safety belt

rm –I

Prompt once if you’re about to delete recursively or a lot of files.

-r recursive delete. To delete directories you must always explicitly use -r

31.12. File system magic

31.12.1. Show file system of a file

```
df -T /else/where
```

31.13. Networking

31.13.1. netstat

Now lets have a look at the current routing information with “netstat –r”

```
Kernel-IP-Routentabelle
Ziel            Router          Genmask         Flags   MSS Fenster irtt Iface
default         *               0.0.0.0         U         0 0          0 ppp0
10.64.64.64     *               255.255.255.255 UH        0 0          0 ppp0
192.168.42.0    *               255.255.255.0   U         0 0          0 eth0
```

31.14. crontab

To edit a crontab entry call

```
sudo crontab -e
```

or

```
crontab -e
```

depending on if you want to edit the root or current user specific crontab. The crontab definitions are stored in /var/spool/cron/crontabs, but you should not edit the crontab definitions directly.

Here a short summary of crontab syntax.

```
*     *     *     *     *  <user> <command>
-     -     -     -     -
|     |     |     |     |
|     |     |     |     +----- day of week (0 is sunday)
|     |     |     +------- month (1 - 12)
|     |     +--------- day (1 - 31)
|     +----------- hour (0 - 23)
+------------- minute (0 - 59),

*/n every n unit
x-y from unit x to unit y
```

Short forms

Short form	Meaning	cron synax
@reboot	once upon start	
@daily	once per day	0 0 * * *
@hourly	one per hour	0 * * * *
@weekly	once per week	0 0 * * 0
@monthly	once per month	0 0 1 * *
@yearly	once per year	0 0 1 1 *

To list the crontab for the current user

```
crontab -l
```

32. Tools

32.1. Connecting

WinSCP

Putty

32.2. Some network tools

32.2.1. wget

commandline HTTP client.

32.2.2. NMAP

Simple host discovery

```
sudo apt-get install nmap
```

```
nmap -sP 192.168.2.1/24
```

32.2.3. netcat

The net swiss army knife

```
sudo apt-get install ncat
```

33. File listings

33.1. /etc/fstab