

Projektarbeit
in der Fakultät
Informatik

Access Point und Router mit embedded Board Banana Pi R1

Referent : Dr. Jiri Spale

Vorgelegt am : ??.??.2017

Vorgelegt von : Bastian
Elias
Jakob
Jonas
Tom

Abstract

English Abstract

Diese Dokumentation ist Teil des Projektes "Access Point und Router mit embedded Board Banana Pi R1", welches im Sommersemester 2017 an der Hochschule Furtwangen durchgeführt wird. Das Projekt besteht daraus, das Vorgängerprojekt mit eigenen Implementierungen zu erweitern. Projektziele sind das Testen passender Betriebssysteme, sowie die Implementierung verschiedener Funktionen wie VPN, Radius, Samba, einem Mailserver und einer Displaystatusanzeige.

Inhaltsverzeichnis

Abstract	i
Inhaltsverzeichnis	iv
Abbildungsverzeichnis	v
Abkürzungsverzeichnis	vii
1 Projektübersicht	1
1.1 Kontext	1
1.2 Ziel	1
2 Betriebssystemeübersicht	3
2.1 OpenWRT	3
2.2 Bananian	3
2.3 IPFire	3
2.4 Armbian	3
3 Implementierung	5
3.1 Backup und Wiederherstellung des Betriebssystems	6
3.1.1 dd	6
3.1.2 rsync	8
3.1.3 tar	8
3.1.4 Automatisierung mittels Bash-Skript	9
3.2 Update des Banana Pi	10
3.3 Implementierung einer Displaystatusanzeige	11

3.4	Mail-Server	12
3.5	Samba	14
3.6	DDNS	16
3.6.1	Einrichtung No-IP	16
3.6.2	Einrichtung Custom-Domain	19
3.7	Radius	21
3.7.1	Allgemein	21
3.7.2	Funktionsweise	21
3.7.3	FreeRADIUS	22
3.8	Captive Portal	24
3.8.1	Algemeines	24
3.8.2	Funktionsweise	24
3.8.3	CoovaChilli	25
4	Benutzeranleitung BananaPi	27
4.1	Pi Hoch- und Herunterfahren	27
4.2	Verbindung über SSH	27
4.3	Lan, Wlan und Vlans	29
4.4	Samba	30
4.5	Mailserver	30
4.6	Domainverwaltung	31
4.7	Backup und Restore	33
4.8	Statusanzeige	33
5	Projektbewertung	35
6	Teilnehmer und Rollenverteilung	37
7	Ausblick	39
	Literaturverzeichnis	41

Eidesstattliche Erklärung	43
-------------------------------------	----

Abbildungsverzeichnis

Abbildung 1: Vorhandene Dateisysteme	6
Abbildung 2: Laufender Backupprozess mit Statusanzeige	7
Abbildung 3: Laufender Wiederherstellungsprozess mit Statusanzeige	7
Abbildung 4: Ausführung wöchentliches Backup	9
Abbildung 5: Verwendung von Tmux mit 'htop' und 'iftop'	11
Abbildung 6: noip Domain	16
Abbildung 7: noip Konfiguration	17
Abbildung 8: freenom Domain	19
Abbildung 9: freenom Nameserver	19
Abbildung 10: Cloudflare DNS	20
Abbildung 11: Radius Funktionsweise	21
Abbildung 12: Radius Test	23
Abbildung 13: CoovaChilli Funktionsweise	25
Abbildung 14: Eingabe des Hostnamens	28
Abbildung 15: Die SSID des AP	29
Abbildung 16: No-IP Startseite	31
Abbildung 17: Freenom Domainverwaltung	32
Abbildung 18: Cloudflare DNS	32

Abkürzungsverzeichnis

1 Projektübersicht

1.1 Kontext

Das Projekt mit dem Titel Router mit embedded Board Banana Pi R1 wird als Semesterprojekt im Sommersemester 2017 an der Hochschule Furtwangen durchgeführt. Das Projekt wurde von Dr. Jiri Spale ins Leben gerufen und wird intern, ohne die Kooperation mit einem Unternehmen durchgeführt. Die Anzahl der studentischen Projektteilnehmer beträgt fünf.

1.2 Ziel

Das primäre Ziel des Projektes ist es, das bestehende Router-Projekt weiterzuentwickeln. Folgende Funktionalitäten sollen implementiert werden:

- Implementierung eines RADIUS-Servers zur zentralen Authentifizierung von Anwendern
- Implementierung eines Voucher-Systems
- Installation des Betriebssystems IP Fire
- Mehrere WLAN Access Points auf einem WLAN-Chip
- Mail-Server zum Statusbericht der Backups
- SAMBA/NFS Server
- Automatische Aktualisierung von Programmpaketen des Systems
- Implementierung einer Display-Statusanzeige

Die Funktionen sollen auf dem Betriebssystem "Bananian", einem auf das Banana Pi zugeschnittenen Debian, implementiert werden.

2 Betriebssystemeübersicht

2.1 OpenWRT

2.2 Bananian

2.3 IPFire

2.4 Armbian

3 Implementierung

3.1 Backup und Wiederherstellung des Betriebssystems

Um die Implementationen und Konfigurationen des Pi's abzusichern, wird eine Backup Lösung eingesetzt. Die Sicherung relevanter Daten soll hierbei einem möglichen Defekt oder Inkompatibilität durch Updates o.ä. entgegenwirken.

'FauBackup' und 'gitbac' bieten hierbei eine Lösung mittels externer Programme an. Debian bietet jedoch bereits standardmäßig einige Aufrufe welche zur Anlegung von Backups verwendet werden können. Diese wurden im Folgenden in Ubuntu anhand eines Bash Skripts zur Automatisierung getestet und implementiert.

3.1.1 dd

Als erste Ausführung wurde der Aufruf 'dd' verwendet. Hierbei wird der Inhalt der gesamten SD Karte als Image Datei abgespeichert.

Schritt 1:

Übersicht der vorhandenen Dateisysteme mittels des Terminalaufrufs 'df'

```

bastian@bastian-VirtualBox:~$ df
Dateisystem    1K-Blöcke  Benutzt Verfügbar Verw% Eingehängt auf
udev           497668      4    497664   1% /dev
tmpfs          101768     900    100868   1% /run
/dev/sda1      9156984  5217368   3451424  61% /
none            4          0         4   0% /sys/fs/cgroup
none           5120          0     5120   0% /run/lock
none          508832     76    508756   1% /run/shm
none          102400     56    102344   1% /run/user
none          455712764 373044796  82667968  82% /media/sf_OrdnerWindows
bastian@bastian-VirtualBox:~$

```

Abbildung 1: Vorhandene Dateisysteme

Schritt 2:

Terminalaufruf für den Backupprozess

```
sudo dd if=INPUTPARTITION of=OUTPUTFILE
```

- sudo -> Backupprozess benötigt root-Rechte
- dd -> bit-genaues Kopieren der Dateien
- if=FILE -> Die Datei oder Partition welche integriert wird
- of=FILE -> Die Output Datei welche angelegt wird

Schritt 3:

Optionale Nutzung von Terminalaufruf 'pv' um den Fortschritt des Backup Prozesses zu sehen. Die mögliche Restzeit lässt sich nur durch das Hinterlegen der Größe der Partition anzeigen.

```
sudo dd if=INPUTPARTITION |pv| sudo dd of=OUTPUTFILE
```

```
bastian@bastian-VirtualBox:~$ sudo dd if=/dev/sda1 |pv| sudo dd of=/media/sf_OrdnerWindows/Backup.iso  
31,4MB 0:00:06 [5,28MB/s] [ <=> ]
```

Abbildung 2: Laufender Backupprozess mit Statusanzeige

Schritt 4:

Wiederherstellen eines hinterlegten Backups läuft ähnlich wie der ursprüngliche Prozess ab.

```
sudo dd if=OUTPUTFILE |pv| of=INPUTPARTITION
```

```
bastian@bastian-VirtualBox:~$ sudo dd if=/media/sf_OrdnerWindows/Backup.iso |pv -s 10G| sudo dd of=/dev/sda1 bs=4096  
56,8MB 0:00:12 [5,23MB/s] [> ] 0% ETA 0:35:52
```

Abbildung 3: Laufender Wiederherstellungsprozess mit Statusanzeige

Quelle: [1]

3.1.2 rsync

Da der Vorgang mittels 'dd' als suboptimal angesehen wird, wurde alternativ der Aufruf 'rsync' verwendet. Dieser bietet die Möglichkeit eines inkrementellen Backups wodurch die Dauer des Prozesses erheblich reduziert werden kann. Hierbei werden die Größe und die Änderungszeit der Dateien in Quelle und Ziel miteinander verglichen. Eine Aktualisierung findet demnach nur statt, wenn Unterschiede vorzufinden sind.

```
rsync -aAXv --delete --exclude={"/dev/*","/proc/*","/sys*  
/*","/tmp/*","/run/*","/mnt/*","/media/*","/lost+found*  
"} / /path/to/backup/folder
```

- rsync -> Kopieren der Dateien
- aAX -> Übertragung im Archiv Modus wodurch alle symbolischen Verweise beibehalten werden
- delete -> Dateien die im Ursprungsverzeichnis nicht mehr existieren werden im Zielverzeichnis ebenfalls gelöscht
- exclude -> Dateien werden ausgelassen

Wiederherstellen des Rsync Backups durch folgenden Befehl:

```
rsync -aAXv /path/to/backup/location/* /mount/point/of/ ↵  
new/install/ --exclude={"/dev/*,/proc/*,/sys/*,/tmp/*,/ ↵  
run/*,/mnt/*,/media/*,/lost+found,/home/*}
```

Quelle: [2]

3.1.3 tar

Eine weitere Anwendungsmöglichkeit bietet die 'tar' Archivierung. Vorteil dieses Aufrufs ist, dass durch Angabe von Parametern die Berechtigungen aller zu sichernden Daten ebenfalls beibehalten werden und die Archivierung Speicherplatz spart.

Wechsel in das Backupverzeichnis dann:

```
tar -cpzf Backup.tar ORDNER
```

- tar -> Archivieren von Daten
- c -> Archiv wird erzeugt (create)
- p -> Berechtigungen beibehalten (privilege)
- z -> Zusätzliche Komprimierung mit gzip
- f -> Archiv in Datei schreiben (finish)

Quelle: [3]

3.1.4 Automatisierung mittels Bash-Skript

Damit der Nutzer die Aufrufe nicht händisch zu bestimmten Zeiten ausführen muss, wurden zwei Bash-Skripte zur Automatisierung geschrieben. Es gibt ein monatliches Backup mittels (tar) und wöchentliche inkrementelle Backups (rsync) auf die zurückgegangen werden kann.

Um das Zeitintervall der Backups einzustellen wird der 'Cron' Dienst verwendet. Hiermit können Skripte und Programme zu festgelegten Zeiten gestartet werden. Wenn ein hinterlegter Job täglich zu einer bestimmten Uhrzeit ausgeführt wird muss allerdings auch der Rechner zu dem Zeitpunkt aktiv sein. Ist dies nicht der Fall, startet der Prozess nicht. Um dies zu umgehen wird 'Anacron' verwendet. Durch ablegen des Skripts in eines der entsprechenden Verzeichnisse wird der Prozess entsprechend ausgeführt. [4]

- /etc/cron.hourly/ - Stündlich ausführen
- /etc/cron.daily/ - Täglich ausführen
- /etc/cron.weekly/ - Wöchentlich ausführen
- /etc/cron.monthly/ - Monatlich ausführen

```
Woechentliches Backup wird ausgeführt. Diesen Vorgang bitte nicht abbrechen!  
sending incremental file list  
deleting security.update.log  
rsync: symlink "/media/sf_OrdnerWindows/Backup/initrd.img" -> "boot/initrd.img-3.13.0-119-generic" failed: Read-only file system (30)  
rsync: symlink "/media/sf_OrdnerWindows/Backup/initrd.img.old" -> "boot/initrd.img-3.13.0-117-generic" failed: Read-only file system (30)  
rsync: symlink "/media/sf_OrdnerWindows/Backup/vmlinuz" -> "boot/vmlinuz-3.13.0-119-generic" failed: Read-only file system (30)  
rsync: symlink "/media/sf_OrdnerWindows/Backup/vmlinuz.old" -> "boot/vmlinuz-3.13.0-117-generic" failed: Read-only file system (30)  
./
```

Abbildung 4: Ausführung wöchentliches Backup

3.2 Update des Banana Pi

Ziel war es das Betriebssystem und alle Programme immer auf dem aktuellsten Stand zu halten. Hierbei kann es jedoch zu Inkompatibilität bestimmter Funktionen oder Konfigurationen kommen. Daher wurde die Umsetzung auf die relevantesten Updates (Sicherheitsupdates) reduziert. Im Normalfall können mittels des Konsolenaufrufs 'apt-get update' die Updateliste und mit 'apt-get upgrade' die Programm Pakete selbst aktualisiert werden. Durch Nutzung des Aufrufs 'unattended-upgrade' wird auf Sicherheitsupdates des Systems überprüft und diese anschließend installiert.

Durch 'unattended-upgrade --dry-run -d' wird auf Verfügbarkeit von Updates geprüft ohne anschließende Installation. Nach jedem Durchgang wird eine Logdatei in /var/log/unattended-upgrades/ angelegt welche genauere Informationen zu den aktualisierten Dateien liefert. [5]

3.3 Implementierung einer Displaystatusanzeige

Zur besseren Übersicht des Netzwerktraffics als auch der Ressourcen des Banana Pi sollte eine Displaystatusanzeige implementiert werden. Der Aufruf 'htop' bietet eine Übersicht aller laufenden Prozesse und deren Ressourcennutzung. 'iftop' zeigt die Netzwerkinterfaces und die eingehende und ausgehende Kommunikationen. Da das Terminal jedoch nur einen der Befehle zu einem Zeitpunkt ausüben kann wird ein Terminal-Multiplexer verwendet. Zur Auswahl stehen hierbei 'Terminator', 'screen', und 'Tmux'. Aufgrund der geringen Einarbeitungszeit und einfachen Anwendbarkeit wurde letzteres zur Implementation ausgewählt. Alle Multiplexer bieten die Möglichkeit Sitzungen zu erstellen. Leider kann dies nicht zur Implementierung der Displaystatusanzeige verwendet werden, da die Sitzung beim Herunterfahren des Betriebssystems gelöscht wird. Daher wird zum Systemstart ein Bash-Skript eingesetzt, welches automatisch die benötigten Fenster zur Überwachung anlegt. [6]

```

bastian@bastian-VirtualBox:~/Dokumente/Studium_HFU/ProjektSS2017/BackupRestoreUpdate/Fertige_Skripte/Ubuntu$

```

The screenshot shows a Tmux terminal window with two panes. The top pane displays the output of the 'htop' command, showing system statistics and a list of running processes. The bottom pane displays the output of the 'iftop' command, showing network interface statistics.

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Comm
2176	bastian	20	0	1389M	63908	15240	S	4.7	6.3	0:30.17	comp
1057	root	20	0	455M	90016	8088	S	3.3	8.8	0:28.12	/usr
3574	root	20	0	31440	1984	1400	R	2.7	0.2	0:00.43	htop
2492	bastian	20	0	638M	16612	5504	S	0.7	1.6	0:07.57	gnom
1096	mysql	20	0	609M	50116	900	S	0.7	4.9	0:05.85	/usr
1320	root	20	0	235M	1072	664	S	0.7	0.1	0:02.25	/usr
2230	bastian	20	0	857M	26360	13044	S	0.0	2.6	0:04.08	naut

TX: cum: 0B pearates: 0b 0b 0b 0b
RX: 0B 0b 0b 0b 0b
TOTAL: 0B 0b 0b 0b 0b

iftop: eth0: 12,5kb 25,0kb 37,5kb 50,0kb 62,5kb

Abbildung 5: Verwendung von Tmux mit 'htop' und 'iftop'

3.4 Mail-Server

Um Statusbenachrichtigungen zu erhalten, wurde ein Mail-Server auf dem Pi eingerichtet, welcher als Relay über Google Mail fungiert. Dazu wurde ein Google Mail Konto eingerichtet, auf welches Post Fix zugreift und Mails verschickt.

Alle System Mails werden Über das Google-Konto weitergeleitet, dazu gehören auch Statusmeldungen des Backup-Skripts.

Dieser Weg wurde wegen des geringen Aufwands gewählt. Ohne Relay würde man eine eigene Domain und sehr viel mehr Konfiguration benötigen. Da ein Google Mail Konto nie verfällt, war dies die beste und pflegeleichteste Möglichkeit.

Weiterhin können die Mails auch an jede beliebige Adresse verschickt werden, dies ist im Mail-Server frei konfigurierbar. Die Mails gehen momentan an die Google Mail Adresse.

Einrichtung:

Voraussetzungen:

- Internetzugriff
- Google Mail-Konto
- Texteditor (Nano)
- SSH/Physikalischen Zugriff

1. Post Fix installieren:

```
apt-get update  
apt-get install postfix libsasl2-modules bsd-mailx
```

2. Das Konfigurationsfenster öffnet sich.

3. TLS/SSL aktivieren:

```
nano /etc/postfix/main.cf
```

3.1 Folgendes Einfügen:

```
mtp_sasl_auth_enable = yes  
smtp_sasl_security_options = noanonymous  
smtp_sasl_password_maps = hash:/etc/postfix/sasl_password  
# verschluesselung einschalten  
smtp_tls_security_level = may
```


4. Nutzerdaten des Google Mail-Kontos hinterlegen:

```
nano /etc/postfix/sasl_password  
smtp.gmail.com Bananapihfu:<Password>
```

5. Datei nur für root lesbar machen, da Klartext:

```
chmod 600 /etc/postfix/sasl_password
```

6. Postfix lookup Tabelle erstellen:

```
postmap hash:/etc/postfix/sasl_password
```

7. Postfix neustarten:

```
/etc/init.d/postfix restart
```

8. Für Weiterleitung der Systemnachrichten aliases bearbeiten:

```
nano /etc/aliases  
root: bananapihfu@gmail.com
```

Oder Wunschemail an welche Systemnachrichten gesendet werden

9. Änderungen an Aliases wirksam machen:

```
Newaliases
```

Quelle: [7]

3.5 Samba

Um den Dateizugriff zu erleichtern, wurde ein Samba-Server auf dem Pi implementiert.

Samba ermöglicht es von nahezu jedem Gerät auf ein Freigegebenes Verzeichnis auf dem Server zuzugreifen. Voraussetzung ist, dass das Client Betriebssystem das SMB-Protokoll unterstützt.

Die meisten modernen Betriebssysteme, wie Windows, MacOS und andere Unixoiden besitzen Samba Funktionalität.

Einrichtung

Voraussetzungen:

- Internetzugriff
- Texteditor (Nano)
- SSH/Physikalischen Zugriff

1. Samba installieren:

```
sudo apt-get update  
sudo apt-get install samba
```

2. Benutzer für Samba erstellen (Hat keinen Shell-Zugriff):

```
useradd sambaur --shell /bin/false
```

3. Passwort für den Benutzer in Samba setzen:

```
smbpasswd -a <user_name>
```

4. Verzeichnis im Home erstellen:

```
mkdir /home/sambaur  
mkdir /home/sambaur/samba
```

5. Berechtigungen setzen:

```
chown sambaur:sambaur /home/sambaur/  
chown sambaur:sambaur /home/sambaur/samba/
```

6. Backup der Samba Konfiguration im Homeverzeichnis machen:

```
cp /etc/samba/smb.conf ~
```

7. Config bearbeiten:

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

7.1 folgendes am Ende der Konfiguration Einfügen:

```
[samba]  
path = /home/sambausr/samba  
valid users = sambausr  
read only = no
```

8. Service neustarten:

```
service smbd restart
```

9. Config testen:

```
testparm
```

Quelle: [8]

3.6 DDNS

Um immer die aktuelle IP-Adresse des Pi zur Hand zu haben, wurde ein DynDNS-Client von no-ip implementiert, bei jedem Systemstart wird die bei der DNS hinterlegte IP-Adresse aktualisiert.

Nachteil hierbei ist jedoch, dass man alle 30 Tage diese Domain aktivieren muss, da diese sonst verfällt.

Um dies zu umgehen wurde die Kostenfreie Domain bananapihf.tk gebucht. Von Vorteil ist hier, dass diese Domain eine Laufzeit von einem Jahr hat und nach Ablauf auch ohne Mehrkosten verlängert werden kann.

Diese Domain wird bei Cloudflare verwaltet, da hier auch eine API angeboten wird, mit welcher man Theoretisch komplett auf eine Dynamische DNS bei No-IP verzichten kann.

3.6.1 Einrichtung No-IP

Voraussetzungen:

- Internetzugriff
- SSH/Physikalischen Zugriff
- NoIP.com Account

1. NoIP Hostnamen anlegen:

Man muss in No-IP den gewünschten Hostnamen einrichten, welcher später auf die aktuelle IP-Adresse verweist.

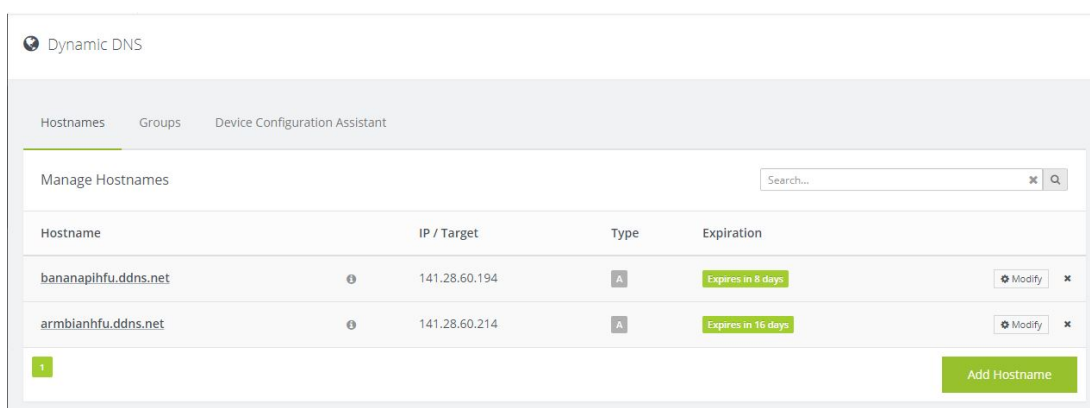


Abbildung 6: noip Domain

2. Verzeichnis für DDNS im Homeverzeichnis erstellen und wechseln:

```
mkdir DDNS
cd DDNS
```

3. NoIP-Client von NoIP.com beziehen:

```
wget https://www.noip.com/client/linux/noip-duc-linux.tar.gz
```

4. Das Archiv entpacken:

```
tar xvf noip-duc-linux.tar.gz
```

5. In den Entpackten Ordner wechseln:

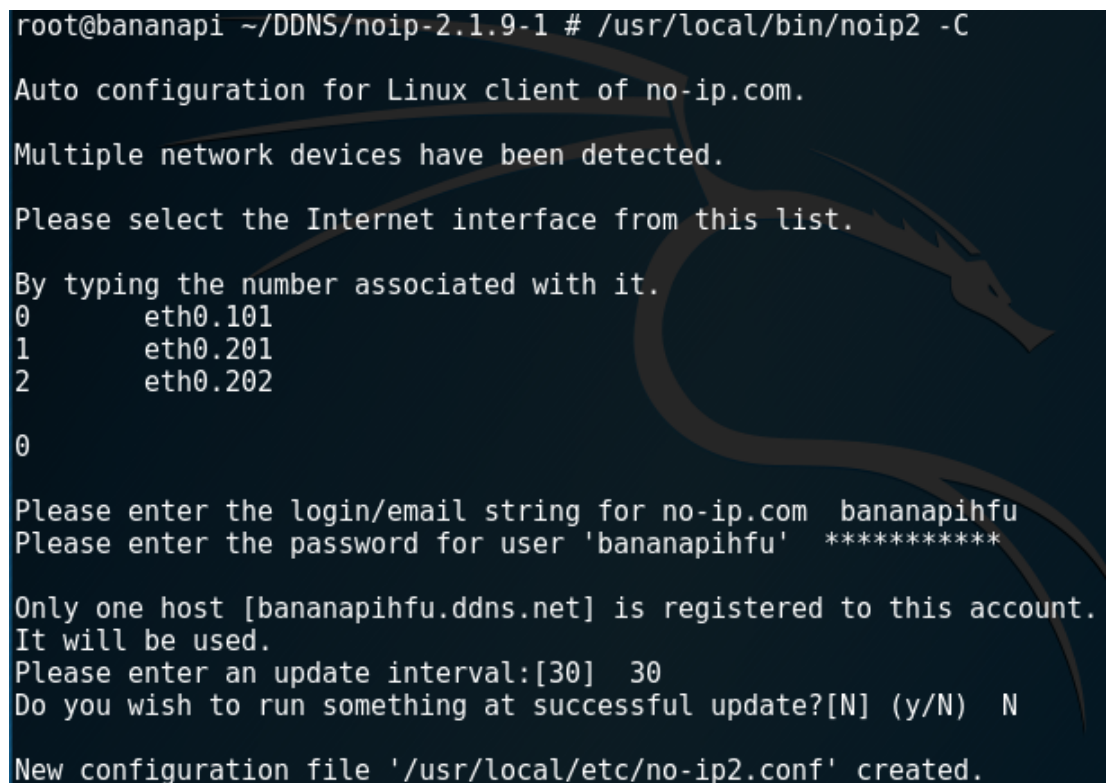
cd noip eingeben und mit TAB vervollständigen

```
cd noip-x.x.x-x
```

6. Client bauen und installieren:

```
make && make install
```

7. Konfiguration wird gestartet:



```
root@bananapi ~/DDNS/noip-2.1.9-1 # /usr/local/bin/noip2 -C
Auto configuration for Linux client of no-ip.com.
Multiple network devices have been detected.
Please select the Internet interface from this list.
By typing the number associated with it.
0      eth0.101
1      eth0.201
2      eth0.202
0

Please enter the login/email string for no-ip.com  bananapihfufu
Please enter the password for user 'bananapihfufu'  *****

Only one host [bananapihfufu.ddns.net] is registered to this account.
It will be used.
Please enter an update interval:[30]  30
Do you wish to run something at successful update?[N] (y/N)  N

New configuration file '/usr/local/etc/no-ip2.conf' created.
```

Abbildung 7: noip Konfiguration

Um den Daemon automatisch bei Systemstart zu starten muss noch folgende Konfiguration vorgenommen werden:

1. Startscript unter `/etc/init.d/noip2` ablegen:

```
vim /etc/init.d/noip2
```

2. Script "noip2" kopieren und einfügen:

Verweis auf Anhang

3. Script ausführbar machen:

```
chmod a+rx /etc/init.d/noip2
```

Quelle: [9]

3.6.2 Einrichtung Custom-Domain

Voraussetzungen:

- Account bei Cloudflare

1. Domain bei Freenom.com aussuchen:

Hier gibt es jede Menge kostenfreie Domains

2. Wunsch-Domain registrieren

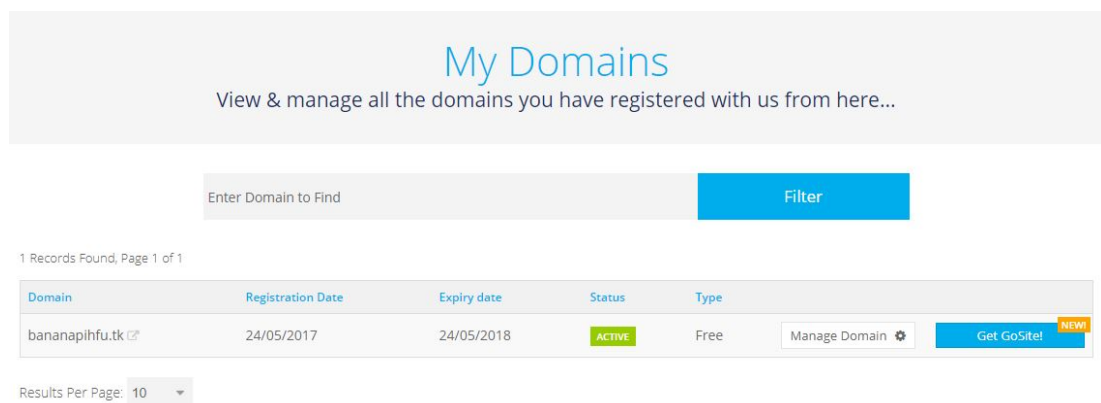


Abbildung 8: freenom Domain

3. Nameserver bei Freenom ändern:

Um die Domain bei Cloudflare zu verwalten, müssen die Nameserver angepasst werden. Diese erhält man, wenn man sich bei Cloudflare anmeldet.

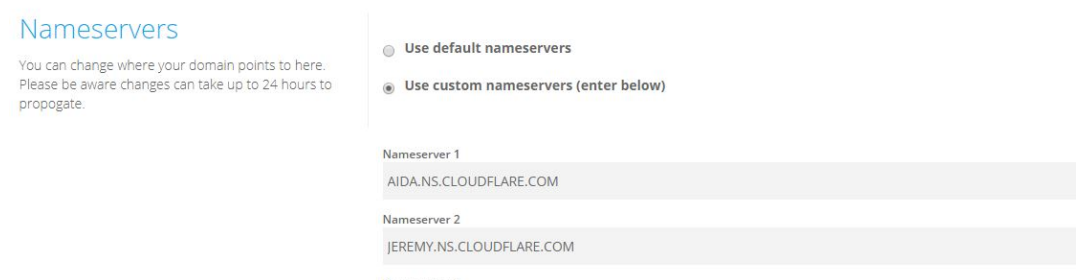


Abbildung 9: freenom Nameserver

3. CNAME Weiterleitung auf No-Ip einrichten

DNS

Manage your Domain Name System (DNS) settings.


DNS Records

A, AAAA, and CNAME records can have their traffic routed through the Cloudflare system. Add more records using this form, and click the cloud next to each record to toggle Cloudflare on or off.





- ⚠ An A, AAAA or CNAME record was not found for the **www** subdomain. The **www.bananapihf.tk** subdomain will not resolve.
- ⚠ An A, AAAA or CNAME record was not found pointing to the root domain. The **bananapihf.tk** domain will not resolve.
- ⚠ An MX record was not found for your root domain. An MX record is required for mail to reach **@bananapihf.tk** addresses.

A

Automatic TTL



Add Record

Type	Name	Value	TTL	Status
CNAME	armbian	is an alias of armbianhf.ddns.net	Automatic	 
CNAME	bananian	is an alias of bananapihf.ddns.net	Automatic	 

[Advanced](#) [API](#) [Help](#)

Abbildung 10: Cloudflare DNS

3.7 Radius

3.7.1 Allgemein

Der Remote Authentication Dial-In User Service (RADIUS, deutsch Authentifizierungsdienst für sich einwählende Benutzer) ist ein Protokoll zwischen Benutzer und Server, das für die 3 A's (dem sogenannten Tripple-A-System), also der Authentifizierung, Autorisierung und das Accounting zuständig ist. Laut Internetquellen ist es der „De-facto Standard bei der zentralen Authentifizierung von Einwahlverbindungen über Modem, ISDN, VPN, WLAN (IEEE 802.1X) und DSL“. [10]

3.7.2 Funktionsweise

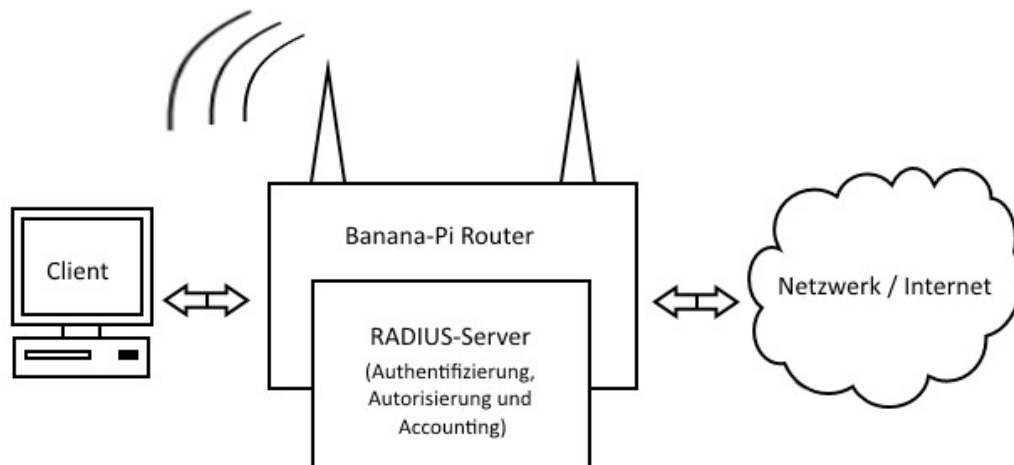


Abbildung 11: Radius Funktionsweise

Anhand der obenstehenden Abbildung lässt sich gut erkennen wie der Aufbau ist. Der Client (Smartphone, PC, etc.) kann sich wahlweise per WLAN oder LAN mit dem Banana-Pi Router verbinden, dabei sendet er eine Authentifizierungsanfrage an diesen, welche der Router an den Radius-Server, welcher auf dem Banana-Pi läuft, weiterleitet. Dieser verarbeitet nun die Anfrage indem er, je nach Konfiguration, in unserem Fall über eine SQL-Datenbank überprüft ob der Client berechtigt ist dem Netzwerk beizutreten. Zusätzlich kann diese Verbindung dann auch limitiert werden (Volumen-Limit, Bandbreiten-Drosselung, beschränkter Zugriff auf Subnetze/VLANs).

3.7.3 FreeRADIUS

FreeRADIUS ist wie der Name schon vermuten lässt eine freie und kostenlose Implementierung des RADIUS-Protokolls und unter der GNU General Public License, version 2 lizenziert. Es ist laut eigenen Angaben der weltweit am meisten eingesetzte RADIUS-Server und wird von den meisten Internetdiensteanbietern (Providern) sowie den 500 umsatzstärksten Unternehmen der Welt benutzt. [11]

Es findet außerdem auch in der Hochschule sowie im akademischen Forschungsnetzwerk Eduroam Einsatz. Es unterstützt den meistverbreiteten Authentifizierungsstandard EAP, auf deutsch etwa „Erweiterbares Authentifizierungsprotokoll“ [12], der ca. 40 verschiedene Verfahren anbietet, welche heutzutage unter anderem in den Sicherheitsimplementationen WPA und WPA2 Verwendung finden.

Installation:

FreeRADIUS ist auch in den offiziellen Paket-Quellen von Debian enthalten und kann somit ganz einfach über den Debian-Paketmanager apt-get installiert werden. Als erstes stellen wir sicher dass das System up-to-date ist und die aktuellen Paketquellen besitzt. [13]

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get freeradius freeradius-utils freeradius-mysql >
mysql-server
```

Bei der Installation des MySQL-Servers wird man gebeten das Passwort für den Root-User zu setzen und zu bestätigen (in unserem Fall ist dies bananapi). Im nächsten Schritt wird eine Datenbank für RADIUS angelegt.

```
q! -uroot -p
```

```
CREATE DATABASE radius;
GRANT ALL PRIVILEGES ON radius.* TO root@localhost >
    IDENTIFIED BY "bananapi";
flush privileges;
exit
```

Danach noch die SQL Schemas in die Datenbank laden: [14]

```
mysql -uroot -p radius < /etc/freeradius/sql/main/mysql/ >
    schema.sql
mysql -uroot -p radius < /etc/freeradius/sql/main/mysql/ >
    setup.sql
```

Zukünftig können nun Benutzer mit folgendem MySQL-Befehl angelegt werden:

```
insert into radcheck (username, attribute, op, value) values
("USERNAME", "Cleartext-Password", ":", "PASSWORD");
```

Nun muss RADIUS dafür konfiguriert werden, das SQL-Modul zu benutzen, dafür editiert man die Datei `/etc/freeradius/sql.conf` und trägt im Bereich `#Connection` info die korrekten Login-Daten ein. Desweiteren muss man in der Datei `radius.conf` die Zeile `$INCLUDE sql.conf`, sowie in der Datei `/etc/freeradius/sites-available/default` zwei mal `sql` in den Sektionen `authorize` und `accounting` ein kommentieren.

Testen:

Um die Konfiguration zu überprüfen kann der RADIUS-Server im Debugging-Modus gestartet werden. Dazu sollte der RADIUS-Dienst erst beendet werden:

```
service freeradius stop
freeradius -X
```

Danach kann in einem zweiten Terminal (oder ggf. mit Terminal-Multiplexer) das Programm `radtest` verwendet werden um Authentifizierungsanfragen an den RADIUS-Server zu senden: [15]

```
radtest USERNAME PASSWORD 127.0.0.1 0 mysecret
```

Eine typische Ausgabe einer erfolgreichen Anfrage sollte wie folgt aussehen:

```
root@bananapi ~ # radtest mysqluser1 "testpass" localhost 1812 testing123
Sending Access-Request of id 140 to 127.0.0.1 port 1812
  User-Name = "mysqluser1"
  User-Password = "testpass"
  NAS-IP-Address = 141.28.60.191
  NAS-Port = 1812
  Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=140, length=20
```

Abbildung 12: Radius Test

3.8 Captive Portal

3.8.1 Allgemeines

Als Captive Portal (zu deutsch etwa „Umleitung auf ein Web-Portal“) wird eine Webseite bezeichnet, die dafür verwendet wird Authentifizierungen durchzuführen, meistens findet sie in WLANs Einsatz. In unserem Fall dient sie dem Login auf einer HTTP-Seite um sich beim RADIUS-Server einzuloggen. [16]

3.8.2 Funktionsweise

Prinzipiell ist die Funktionsweise relativ simpel. Man benötigt lediglich einen Webserver und eine Firewall, in unserem Fall Apache2 und iptables. Wenn nun ein Benutzer in ein WLAN-Netzwerk möchte, wird erst einmal der komplette Netzwerkverkehr ignoriert, bis er einen Browser öffnet. Dieser Zugriff wird immer auf das Captive Portal weitergeleitet, sodass der Benutzer immer zu der Login-Seite kommt. Je nach Anwendungsfall können dort dann auch Bezahlungssysteme implementiert werden oder Nutzungsbedingungen die akzeptiert werden müssen.

Es gibt verschiedene Möglichkeiten wie die Umleitung von Statten gehen kann, durchgesetzt hat sich aufgrund verschiedener sicherheitstechnischer Aspekte die Umleitung via HTTP (direkte IP- sowie DNS-Umleitungen sind aufgrund des dann nicht mehr gültigen DNSSEC-Zertifikats nicht möglich). [17]

3.8.3 CoovaChilli

Allgemeines:

CoovaChilli ist ein open-source Tool das unter der GNU General Public License 3 veröffentlicht wurde und frei zugänglich ist. Es bietet eine Zugriffskontrolle als Captive Portal und liefert die dafür benötigten HTML/CSS/Javascript Dateien. Es basiert auf dem mittlerweile nicht mehr unterstützten Projekt CoovaSpot und funktioniert mit dem RADIUS-Protokoll.

Funktionsweise:

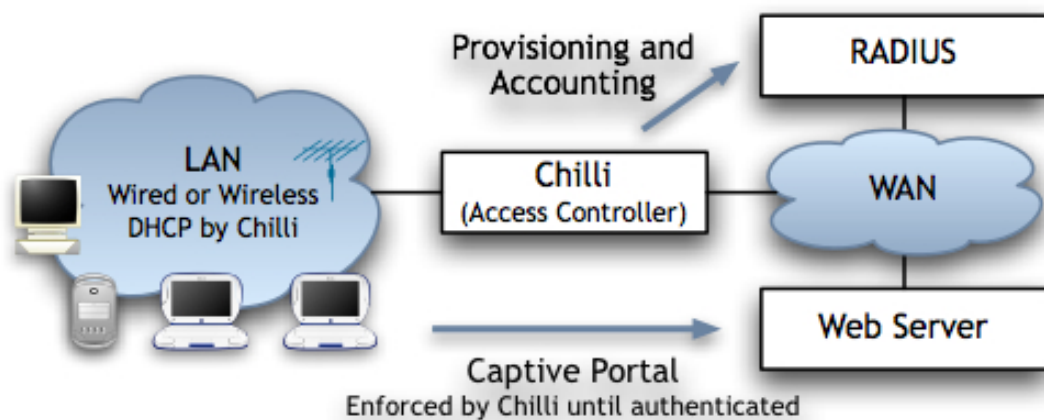


Abbildung 13: CoovaChilli Funktionsweise

Quelle: [18]

Wie in der Abbildung oberhalb zu erkennen bildet CoovaChilli die Instanz zwischen dem Access- Point des Netzwerks und der Netzwerkinfrastruktur dahinter (in unserem Fall laufen Netzwerk- Access-Server, also dem WLAN-AP, CoovaChilli und der RADIUS-Server auf der gleichen Maschine). Will ein Benutzer nun ins Internet verbindet er sich wahlweise per LAN oder WLAN mit dem AP, ruft den Browser auf und wird auf das Captive Portal auf dem Webserver weitergeleitet. Beim Login kommuniziert CoovaChilli mit dem RADIUS-Server, bei erfolgreichem Login wird der Internetzugang für den Benutzer freigegeben.

Installation:

4 Benutzeranleitung BananaPi

4.1 Pi Hoch- und Herunterfahren

Um den Pi Hochzufahren, muss lediglich das Netzteil eingesteckt werden:

1. Netzteil in Steckdose einstecken
2. Micro-USB Port an den äußeren Port des Pis anschließen. Der andere Port ist nur für OTG!

Um den Pi Herunterzufahren muss benötigt man Zugriff auf die Kommandozeile

1. Pi an Tastatur und Bildschirm anschließen || SSH-Verbindung zum Pi aufbauen
2. Anmelden (User: root / Passwort: bananapi)
3. shutdown -h 0 eingeben und mit ENTER bestätigen

4.2 Verbindung über SSH

Um eine Verbindung über SSH aufzubauen wird folgendes benötigt:

- Putty (Windows)
- ssh-Packet (Linux)
- Netzwerkverbindung

Um eine Verbindung aufzubauen muss der Pi hochgefahren sein und über den Wan-Port an ein Netzwerk angeschlossen sein.

Windows:

1. Putty öffnen
2. Hostnamen armbian.bananapihf.tk angeben 3. Durch Klick auf „Open“ Verbindung

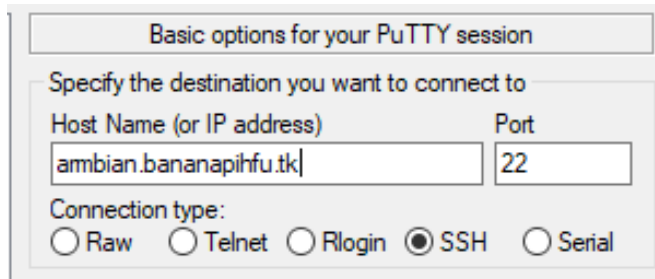


Abbildung 14: Eingabe des Hostnamens

aufbauen -> Terminal öffnet sich

```
login as: root
password: bananapi
```

4. Verbindung erfolgreich!

Linux:

1. Terminal öffnen
2. Folgenden Befehl eingeben:

```
ssh root@armbian.bananapihf.tk
```

3. Passwort eingeben:

```
password: bananapi
```

4. Verbindung erfolgreich!

4.3 Lan, Wlan und Vlans

Übersicht Vlans:

Der Pi besitzt 4 Lan Ports und einen Wlan Access-Point.

Vlan 1:

- Internetzugriff
- Lan 1 + Lan 2
- Gateway:192.168.1.1

Vlan 2:

- Kein Internetzugriff
- Lan 3 + Lan 4
- Gateway:192.168.2.1

Vlan 3:

- Internetzugriff
- WLAN AP
- Gateway:192.168.3.1

Wlan:

Der Pi besitzt einen Wlan-AP, über welchen eine Internetverbindung möglich ist. Lokal ist jedoch nur Zugriff auf Geräte im Vlan 3 möglich. Um eine Verbindung zum AP

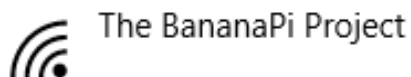


Abbildung 15: Die SSID des AP

herzustellen muss folgendermaßen Vorgegangen werden:

1. Wlan Übersicht am Client Gerät öffnen und nach APs suchen
 - a. The BananaPi Project auswählen
 - b. WPA/WPA2 PSK auswählen
 - c. Passwort: bananapi
2. Verbindung hergestellt

Lan:

Der Pi besitzt insgesamt 5 Lan-Ports. Einer davon ist der WAN-Port, welcher an ein externes Netzwerk angeschlossen wird. Die vier restlichen Ports werden über den Pi geroutet und sind in Vlans unterteilt (siehe Übersicht Vlans).

4.4 Samba

Verbindung aufbauen

Mit Samba können Dateien zwischen dem Pi und einem anderen Gerät ausgetauscht werden.

Um den Samba-Share im am eigenen PC einzubinden muss folgendes gemacht werden:

Windows:

1. Ausführen-Dialog aufrufen mit Win + R
2. \\armbian.bananapihf.tk\samba eingeben und mit ENTER bestätigen
3. Login Fenster öffnet sich
 - a. Login: sambausr
 - b. Passwort: bananapi

Linux:

1. smbclient installieren:
 - a. sudo apt-get update
 - b. sudo apt-get install smbclient
2. Verbindung aufbauen:
 - a. smbclient \\armbian.bananapihf.tk /samba -U sambausr
 - b. Passwort eingeben: bananapi

MacOSX:

1. Im Finder mit Server verbinden (Command + K)
2. Serveradresse angeben:
 - a. smb://armbian.bananapihf.tk/samba
3. Verbinden als Registrierter Nutzer:
 - a. Name: sambausr
 - b. Passwort: bananapi

4.5 Mailserver

Um auf die Mails zuzugreifen, muss man <https://www.google.com/gmail> besuchen und sich mit folgenden Benutzerdaten anmelden:

- Email: bananapihf
- Passwort: 63!gr&8FJZdd

Um die Emails über einen Mail-Client aufzurufen, kann die Anleitung von Google zur Hand genommen werden:

<https://support.google.com/mail/answer/7126229?hl=en>

4.6 Domainverwaltung

Ni-IP

Um die Dynamische DNS bei No-IP zu verwalten muss no-ip.com besucht werden: -

Login: bananapihf

- Passwort: BananaPhone

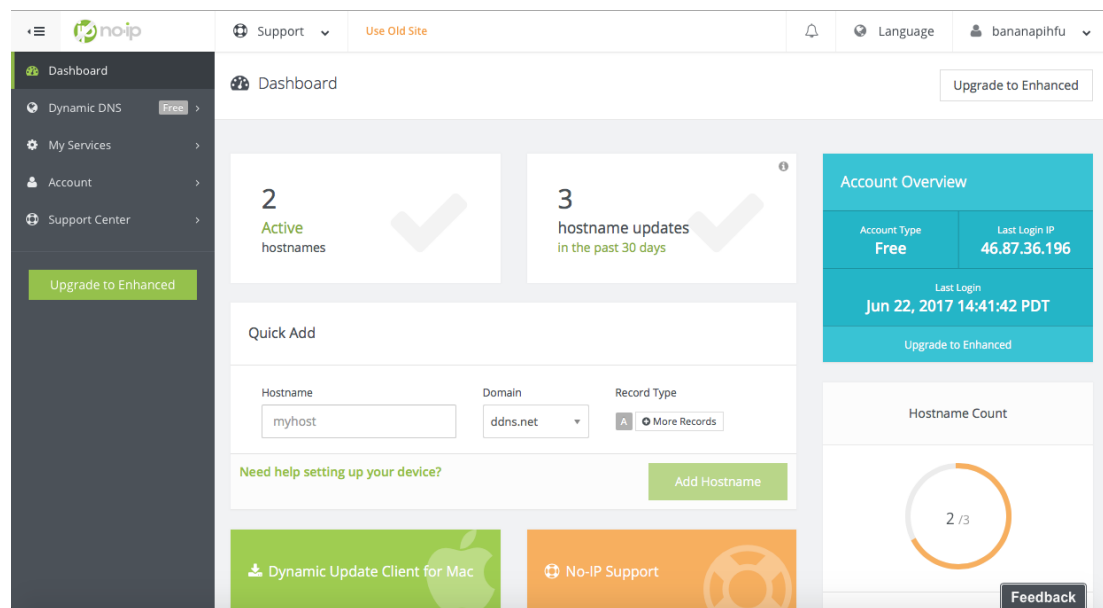


Abbildung 16: No-IP Startseite

Freenom.com

Über Freenom wurde die kostenfreie Domain bananapihf.tk gebucht.

Login: bananapihf@gmail.com

Passwort: bananapi

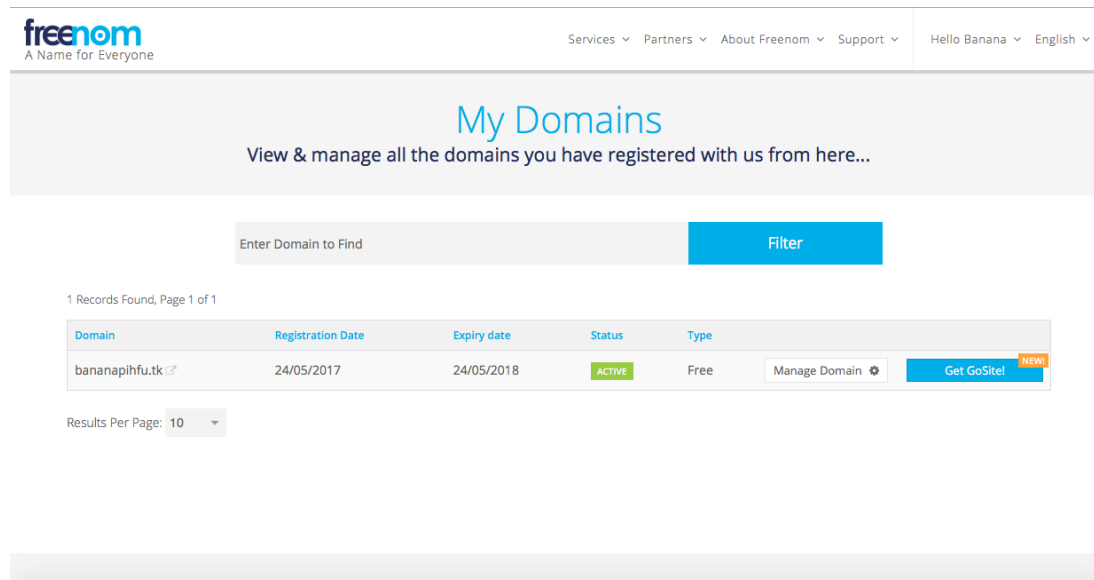


Abbildung 17: Freenom Domainverwaltung

CloudFlare

Über CloudFlare werden die DNS-Einträge der Domain verwaltet:

Login: bananapihf@gmail.com

Passwort: k%KKx!HkNW23

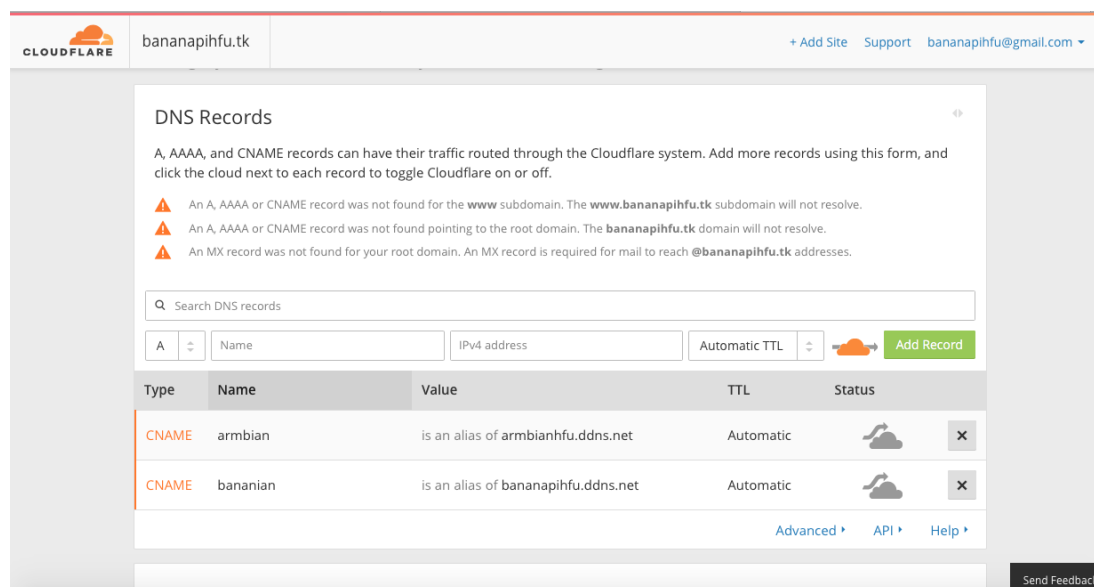


Abbildung 18: Cloudflare DNS

4.7 Backup und Restore

Das Backup wird über zwei Skripte gestartet, welche in den Verzeichnissen `/etc/-cron.weekly/` und `/etc/cron.monthly/` liegen. Das Backup wird somit regelmäßig ausgeführt.

Manuelles Backup

Sollte man ein aktuelles Backup benötigen, kann man das Backup-Script manuell ausführen:

```
bash /etc/cron.weekly/Backup_Weekly
```

Hierbei wird das Backup unter `/mnt/SSD/Backup_Weekly` gespeichert.

Zur Archivierung des Backups, kann auch das `Backup_Monthly` aufgerufen werden:

```
bash /etc/cron.monthly/Backup_Monthly
```

Dieses Skript speichert dann das Wöchentliche Backup unter `/mnt/SSD/Backup_Monthly` als tar-Archiv.

4.8 Statusanzeige

Die Statusanzeige wird bei Systemstart geöffnet, da das Skript für diese unter `/etc/init.d/` abgelegt ist. Das Skript baut eine `tmux`-Session auf, welche mit folgendem Befehl aufgerufen werden kann:

```
tmux attach
```

Beendet wird die Session mit folgender Tastenkombination:

```
CTRL + D
```


5 Projektbewertung

Die technischen Herausforderungen des Projekts waren für alle Teilnehmer eine spannende und lehrreiche Erfahrung. Durch die Umsetzung der verschiedenen Implementationsziele auf der gegebenen eingebetteten Plattform können alle Projektteilnehmer einen großen Zugewinn an fachspezifischen Wissen verzeichnen.

Mit den wöchentlichen Projekttreffen war es möglich, frühzeitig auf aktuelle Probleme zu reagieren und Lösungsansätze gemeinsam zu erörtern.

Aufgrund des Wechsels von Bananian auf Armbian wurde der Zeitplan des Projekts teils weit zurückgeworfen. Weniger vorweisbare Projekt-Ergebnisse und kleinere Entwicklungsschritte waren die Folge, da Kernfunktionen wie die Switcharchitektur des Banana Pi komplett neu entwickelt werden mussten. Zudem wirkten sich Updates des Betriebssystems teils deutlich auf die Verlässlichkeit und Bedienbarkeit des Geräts aus, was mutmaßlich dem noch unausgereiften Betriebssystem geschuldet ist, das sich zum Zeitpunkt des Projekts in einer sehr aktiven Entwicklungsphase befindet.

6 Teilnehmer und Rollenverteilung

Die Rollen der studentischen Projektteilnehmer wurden wie folgt aufgeteilt:

Name	Hauptrolle
Bastian	<ul style="list-style-type: none">- Projektleiter- Entwicklung Backup Skripte- Entwicklung Displaystatusanzeige
Jonas	<ul style="list-style-type: none">- Implementierung Mail-Server- Implementierung Samba-Server- Implementierung DDNS
Tom	<ul style="list-style-type: none">- Implementierung einer WLAN-Benutzerverwaltung- Implementierung eines RADIUS-Server mittels CoovaChilli
Jakob	<ul style="list-style-type: none">- Erstellung der Dokumentation- Untersuchung von IP-Fire als Alternatives Betriebssystem
Elias	<ul style="list-style-type: none">- Überprüfung des WLAN-Chips in Bananian- Integration des WLAN und VLAN in Armbian

Die Verteilung der Rollen und mancher Aufgabengebiete änderte sich im Verlauf des Projekts. Die hier dargestellte Unterteilung bezieht sich auf den Stand zum Semesterende.

7 Ausblick

Literaturverzeichnis

- [1] <https://wiki.ubuntuusers.de/dd/>.
- [2] <https://wiki.ubuntuusers.de/rsync/>.
- [3] <https://wiki.ubuntuusers.de/tar/>.
- [4] <https://wiki.ubuntuusers.de/Cron/>.
- [5] <https://wiki.debian.org/UnattendedUpgrades>.
- [6] <https://wiki.ubuntuusers.de/tmux/>.
- [7] <http://my5cent.spdns.de/allgemein/banana-pi-postfix-installieren-und-einrichten.html>.
- [8] https://help.ubuntu.com/community/How%20to%20Create%20a%20Network%20Share%20Via%20Samba%20Via%20CLI%20%28Command-line%20interface/Linux%20Terminal%29%20-%20Uncomplicated%2C%20Simple%20and%20Brief%20Way%21#About_This_Guide.
- [9] https://www.togaware.com/linux/survivor/No_IP_Manual.html.
- [10] http://i.techrepublic.com/downloads/PDF/SolutionBase_RADIUS_deployment_scenarios.pdf.
- [11] <http://freeradius.org/>.
- [12] <https://www.heise.de/glossar/entry/Extensible-Authentication-Protocol-397255.html>.
- [13] <https://www.vultr.com/docs/install-freeradius-on-debian-7>.
- [14] <https://wiki.freeradius.org/guide/SQL-HOWTO-for-freeradius-3.x-on-Debian-Ubuntu>.
- [15] <https://extremeshok.com/5486/debian-7-freeradius-server-mysql-authentication/>.
- [16] <https://andrewwippler.com/2016/03/11/wifi-captive-portal/>.
- [17] https://en.wikipedia.org/wiki/Captive_portal.
- [18] https://coova.github.io/img/Chilli_2.jpg.

Eidesstattliche Erklärung

Ich versichere, dass ich die vorstehende Arbeit selbständig verfasst und hierzu keine anderen als die angegebenen Hilfsmittel verwendet habe. Alle Stellen der Arbeit die wörtlich oder sinngemäß aus fremden Quellen entnommen wurden, sind als solche kenntlich gemacht.

Die Arbeit wurde bisher in gleicher oder ähnlicher Form in keinem anderen Studiengang als Prüfungsleistung vorgelegt oder an anderer Stelle veröffentlicht.

Ich bin mir bewusst, dass eine falsche Erklärung rechtliche Folgen haben kann.

Furtwangen, den ??.???.2017