Motivation

- Als Digital Botschafter kann es angebracht werden die Bedienung des Smartphone zu Zeigen, wenn ein Beamer zur Verfügung steht, ist es kein Problem.
- In Fremde Nezten ändern sich die Adressen.
    - Eingabe sind notwendig.
- Der ein eigene Hotspot kann so eingestellt werden, dass die Adresse konstant bleibt und eine Anzeige auf den Beamer per Knopfdruck erfolgen kann.
- Darüberhinaus, sollte ein WLAN-Verkehr auf das Haupt-Kanal nich störend sein (nutzbare Bandbreite).
- Viele Hostspots lassen ein Datenverkehr zwischen den angemeldete Systeme nicht zu. Mit ein eigenen Hotspot kann es umgegangen werden.
    - Beispiel Steuerung der Präsentation mittels ein Smartphone.

Mögliche Komponenten

- Mit NetworkManager
- Mit Hostapd

Das Aufsetzen einem Hotspot mit den Networkmanager klingt gut, unglücklicherweise fehlt es an einige Einstellungsmöglichkeiten, der Betrieb und geziehlten Ein- Ausschalten erfordet die Verwendung einem Script, der von Hand aufgerufen werden muss.

Wenn ein Script erhalten muss, kann auch hostapd verwendung finden. Es ist der Weh der gegangen wird.

Was zu beachten ist.

- **NetworkManager:** Netwerkschnittstellen Verwaltung
    - nmcli (Netwerkschnittstelle vom NetworkManager Zuständigkeit entfernen)
- **firewall:**
    - Übergeordnete Firewall Systeme
        - firewall-cmd
        - ufw
    - Unterste Schicht
        - iptables(-legacy)
        - nftables
            - iptables-nft (übersetzt iptanbles nach nftables).

Haupt Zutaten

- hostapd
- dnsmasq (nur DHCP Server)
- ip
- iptables* / nftables
- sh, grep, cut, sed, awk, ... (nichts Besonderes).
- ein externe WLAN-USB Gerät

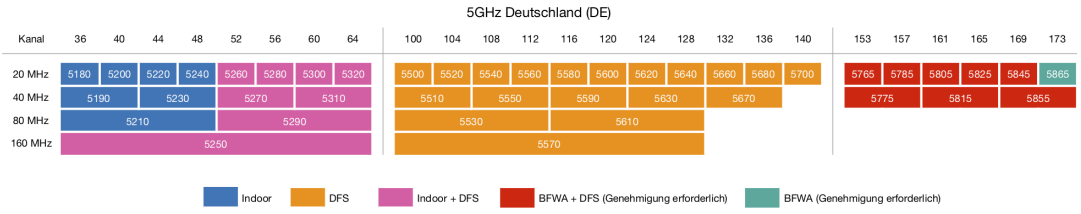
Wahl des Frequenzbereiches

- 2,4 Ghz geht normalerweise problemlos.
- 5 GHz ist sehr problematisch, viele Adapter unterstützen es unzureichend.
    - Die Regulierung in der EU bzw. Deutschland erlauben sehr wenig (Kanäle 36 bist 48).

Wahl des Kanals, 2.4 GHz

- Die alte Angabe Kanal 1, 6 oder 11 ist veraltet
- Bei 4 nutzbare Bereiche a 20 MHz im 2,4 GHz Bereich
    - Kanäle 1, 5, 9 und 13
- Bei 2 Nuzbare Bereiche a 40 MHz im 2,4 GHz Bereich
    - Kanäle 3 und 11
- Quellen:
    - https://wiki.freifunk-franken.de/w/WLAN_Frequenzen

Wahl des Kanals, 5GHz

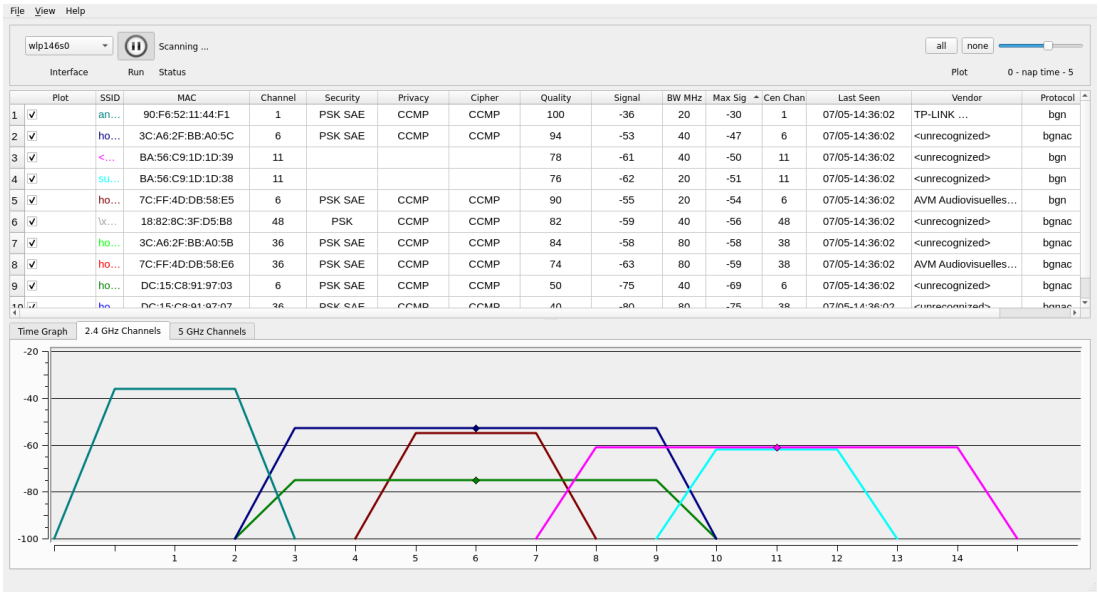


Kanäle 5GHz, Quelle: freifunk-franken.de

Tools zur Ermittlung der freie Kanäle

- Android
    - Wifi Analyzer
- Linux
    - linssid (Nicht für alle Distributionen vorhanden).
    - Kommando: *nmcli dev wifi*

Linssid



Linssid

Hotspot Sicherheit

- Open
    - Keine Sicherheit
- WEP
    - Veraltet, schnell knackbar
- WPA (TKIP)
    - Veraltet, schnell knackbar
- WPA2 (CCMP)
    - Kann geknackt werden.
- WPA3
    - Momentan das beste Verfahren,
    - Wird nicht von jede System und Adapter unterstüzt
- WPA2/WPA3
    - Kompatibilitätsmodus

Wahl des USB-WLAN- Adapter

- Die Suche einen geeignete Adapter kann, wenn 5GHz unterstüzt sein sollte sich als sehr schwierig erweisen
- Hilfe ist unter https://github.com/morrownr/USB-WiFi uu finden.

Mögliche Betriebsarten

- Repeater Betrieb
  - Fertige Repeater verwenden.
- Bridged Hotspot
  - Setzt ein Ethernetanschluss voraus!
- **Autarktes Hotspot**
  - DHCP notwendig
  - hostapd notwendig
  - NAT notwendig (iptables, nfttables)
  - flexibel

SoftAP

- Viele Adapter ermöglichen es eine virtuelle Netwerk Schnittstelle anzulegen.
  - Normalerweise kann **kein** anderen Frequenbereich verwendet werden.
  - Bestenfalls als ein Art Repeater einsetzbar.

IPv6 or not IPv6 ? That’s the question

- IPv6 Adressen sind kompliziert / unhandlich
- IPv6 ist schneller als IPv4 (eigene Erfahrungen)
- IPv4 + IPv6 gleichzeitig ist die Lösung
  - Damit IPv6 sich entfalten kann müssen die Adressen routbar sein!
  - Link Lokale Adressen (Bereich fd00::/8 sind ungeeignet)
  - Lösung: eine nicht vergebene Adresse 4000::/32 oder besser
  - 2001:2::/48 (Reserviert für Benchmarking)
- IPv4 darf nicht mit der Hauptadresse kollidieren
  - Lösung: 198.18.0.0/15 (Für Tests reserviert).

NetworkManager Hürde überwinden

- Das NetworkManager ist bei viele Distributionen installiert
  - Er kümmert sich um die Verwaltung der Netwerkschnittstellen
  - Es muss. für unseren Hotspot-Schnittstelle, abgeschaltet werden
  - Kommando: *nmcli device $HotSpotDev managed no*

Forwarding einschalten

```
sysctl net.ipv4.conf.all.forwarding=1
sysctl net.ipv6.conf.all.forwarding=1
```

IPv6 Schnittstellenkonfiguration

```
sysctl net.ipv6.conf.$wlan1.addr_gen_mode=0
sysctl net.ipv6.conf.$WLANDEV.use_tempaddr=0
sysctl net.ipv6.conf.$WLANDEV.accept_ra=0
```

Sicherstellen des Zugriffes auf der Netzwerkschnittstelle

```
ip link set down $wlan1
ip link set up $wlan1
```

Network Address Translation

Die für das Hotspot verwendete Adressen können nicht im Internet verwendet werden. Mit den Adressen können die externe Router nichts anfangen,

- Einsatz von Firewall Regeln.
- INPUT muss auf ACCEPT gestellt werden,
- FORWARDING ebenfalls.
- nat POSTROUTING soll Masquerading, SNAT oder DNAT vornehmen.
    - Die Adressen der Clients werden durch die Adressen der Schnittstelle zum Internet (Server) umgesetzt.

NAT Regeln

```
iptables -t nat -A POSTROUTING -s 198.18.0.0/24 -o $wlan0  -j MASQUERADE
```

oder

```
nft add rule ip nat POSTROUTING oifname "$wlan0" ip saddr 198.18.0.0/24 counter masquera
```

Server von Zufriffe schützen

```
# Kein Verkehr zu unseren Rechner
iptables -A INPUT -s 198.18.0.0/24 -d 192.168.0.23  -j DROP
# mDNS zur Clients abschalten
iptables -A OUTPUT -o $wlan1 -p udp --dport 5353 -j DROP
```

oder

```
nft add rule ip filter INPUT ip saddr 198.18.0.0/24 ip daddr 192.168.0.23 counter drop
nft add rule ip filter OUTPUT oifname $wlan1 udp dport 5353 counter drop
```

Hostapd Konfiguration - allgemein

```
ctrl_interface=/var/run/hostapd
ctrl_interface_group=wheel
country_code=DE
macaddr_acl=0
ignore_broadcast_ssid=0
ieee80211n=1
preamble=1
wmm_enabled=1
ieee80211d=1
ignore_broadcast_ssid=0
interface=$wlan1
hw_mode=g
channel=1
ssid=meinHotspot
```

Hostapd Konfiguration - Autorisierung

```
# Autorisierung
auth_algs=1
wpa=2
wpa_passphrase=$PASS
rsn_pairwise=CCMP
wpa_key_mgmt=WPA-PSK

# Für WPA2/WPA3
#ieee80211w=2
#wpa_key_mgmt=SAE WPA-PSK
```

Hostapd Konfiguration - Bandbreite

```
# 20 MHz Kanäle (N150, bis 72 Mbps)
ht_capab=[HT20][SHORT-GI-20]

# 40 MHz Kanäle (N300, bis 144 Mbps)
#ht_capab=[HT20][SHORT-GI-20][HT40-][HT40+][SHORT-GI-40]
```

Dnsmasq Konfiguration

```
interface=$wlan1
# DNS-Server = Quad9 (Schweiz)
server=2620:fe::9
server=9.9.9.9
Server=2620:fe::fe
server=149.112.112.112

bind-dynamic
domain=hotspot
local=/hotspot/
except-interface=lo
dhcp-authoritative
dhcp-rapid-commit
dhcp-leasefile=/tmp/dnsmasq.lease
dhcp-range=198.18.0.2,198.18.0.254,360
dhcp-option=option:dns-server,198.18.0.1.1
dhcp-range=::,constructor:$wlan1,ra-names,ra-advrouter
dhcp-option=option6:dns-server,[2001:2::1]
enable-ra
```

Besonderheit für Firewalld

Die Netzwerkschnittstelle muss eine passende Zone zugeordnet werden

```
zone=$(firewall-cmd --get-zone-of-interface=$wlan1 2>/dev/null)
if [ "$zone" = "trusted" ]; then
    return;
fi
if [ "$zone" != "" ]; then
    firewall-cmd --zone=$zone --remove-interface=$wlan1
fi
firewall-cmd --zone=trusted --add-interface=$wlan1
```

Hostspot Starten

```
Parameter_ermitteln              # /bin/sh Skript
Konfigurationsdateien_erzeugen   # hostapod.conf dnsmasq.conf
Setze_Schnittstelle_unmanaged    # nmcli
Forwarding_einstellen            # sysctl
Adapter_für_IPv6_konfigurieren   # sysctl
Schnittstelle_Down_Up            # ip
Zone_setzen                      # falls notwendig, firewallcmd, ...
Hostapd_starten                  # hodtapd
Dnsmasq_starten                  # dnsmasq
Ip_Adressen_und_Routen_setzen    # ip
```

Betrieb mit eigene Hardware

- D-Link DWA-192, Treiber 8814AU (selbst kompiliert):
    - 2,4 GHz Bereich. Nur 20 MHz Bereiche verwendbar.
    - 5 GHz. Kanäle 36 bis 48 verwendbar.
- Notebook mit Intel Chips:
    - 5 GHz nicht möglich.
    - Gemischt 2,4 GHz (AP), 5 GHz (Internet, nicht immer möglich).
- TP-Link Adapter: (Atheros ath9k bzw. Realtek rtl8192CU.
    - Nur 2,4 GHz Band. Funktion OK.