

Einen WLAN-Accesspoint auf Raspberry Pi 3 (oder Pi Zero W) aufsetzen mit hostapd

Hier auch mit WPA-Enterprise (EAP) und Authentifikationsserver, so dass jeder Schüler einen eigenen Zugang bekommt.

Mit OpenWRT: https://wiki.openwrt.org/toh/raspberry_pi_foundation/raspberry_pi

Manuell:

Hostap-Teil: Anleitung analog <https://frillip.com/using-your-raspberry-pi-3-as-a-wifi-access-point-with-hostapd/>

1. Aktuelles Raspbian aufsetzen. Hier im Test verwende ich die Methode mit qemu-Emulator, statt mich auf Raspberry Pi einzuloggen.
2.

```
sudo apt install hostapd dnsmasq
sudo systemctl unmask hostapd
sudo systemctl enable hostapd
in die /etc/default/hostapd
HOSTAPD_CONFIG=/etc/hostapd/hostapd.conf
```

3.

```
sudo nano /etc/dhcpd.conf
```

, dort am Ende eintragen:

```
denyinterfaces wlan0
```

Hierdurch soll verhindert werden, dass der Raspi versucht, sich eine IP-Adresse per DHCP auf das Interface zu holen. Es muss statisch konfiguriert werden! Eigentlich sollte es genügen, in die *etcnetwork/interfaces* einzutragen, dass das Interface statisch ist.

4. In */etc/network/interfaces* den statischen Eintrag für wlan0 anlegen:

```
allow-hotplug wlan0

iface wlan0 inet static
    address 10.10.10.1
    netmask 255.255.255.0
    network 10.10.10.0
    broadcast 10.10.10.255
```

5. Nun die hostapd-Konfiguration anpassen, ein Beispiel findet sich im doc-Verzeichnis von hostapd:

```
cat /usr/share/doc/hostapd/examples/hostapd.conf | \
sudo dd of=/etc/hostapd/hostapd.conf
sudo nano /etc/hostapd/hostapd.conf
```

Dort sind folgende Einträge zu ändern:

```
driver=nl80211
ssid=seminar.lan2
hw_mode=g (steht schon da)
channel=0 # Automatisch Channel suchen
ieee80211n=1 (N Protokoll unterstützen)
```

Die einfache Variante mit WPA-Preshared-Key (WPA-PSK):

```
wpa=2 (NUR WPA2 zulassen, kein WPA-V1)
wpa_key_mgmt=WPA-PSK
wpa_passphrase=xxxxxxxxxx
```

6. Die Enterprise-Variante (jeder Teilnehmer muss sich mit eigenem Passwort+Login authentifizieren), zusätzlich kann man AUCH WPA-PSK erlauben. Frei nach <https://gist.github.com/noahwilliamsson/f2714e63e5959ffa9c92>

```
wpa_key_mgmt=WPA-PSK WPA-EAP
ieee8021x=1
eapol_version=2
eap_message=ping-from-hostapd
eap_server=1
# ca_cert=/etc/hostapd/hostapd.ca.pem
# dh_file=/etc/hostapd/hostapd.dh.pem
server_cert=/etc/hostapd/hostapd.cert.pem
private_key=/etc/hostapd/hostapd.key.pem
eap_user_file=/etc/hostapd/hostapd.eap_user
```

Mindestens das Server-Zertifikat (Public Key) und Server-Key (Private Key) müssen mit openssl erzeugt werden:

```
openssl req -new -x509 -days 3500 -nodes \
            -out /etc/hostapd/hostapd.cert.pem \
            -keyout /etc/hostapd/hostapd.key.pem
```

openssl fragt dabei interaktiv die Daten ab, die im Zertifikat stehen sollen. Als „common name“ sollte der Server – Hostname oder seine IP angegeben werden, optional mit einer Mailadresse dazu.

hostapd.eap.user:

Ausführliches Beispiel mit Einträgen für Testuser unter http://rpc.one.pl/pliki/openwrt/backfire/10.03.x/atheros/hostapd/dokumentacja/hostapd.eap_user

7. Jetzt muss noch der DHCP- und Nameserver konfiguriert werden:

```
sudo nano /etc/dnsmasq.conf
```

Dort eintragen:

```
interface=wlan0
listen-address=10.10.10.1
bind-interfaces
server=9.9.9.9          # Forward DNS requests to Google DNS
domain-needed          # Don't forward short names
```

```
bogus-priv          # Never forward addresses in the non-  
routed address spaces.  
dhcp-range=10.10.10.50,10.10.10.150,12h
```

8. IP-Forwarding und Masquerading (einfache Network Address Translation):

```
sudo nano /etc/sysctl.conf  
Dort eintragen:  
net.ipv4.ip_forward=1
```

Beim Neustart sollte ein Skript laufen, das mit iptables das Masquerading aktiviert:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE  
iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT  
iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
```

Hinweis von Herbert: Die letzten beiden Zeilen sind bei den aktuellen Raspbian-Versionen schon standardmäßig gesetzt.

Dies kann z.B. in die Datei `/etc/rc.local` geschrieben werden.