

# Beispielkonfigurationen für MikroTik-Geräte / Stand Juli 2020

Bevor man diese Konfigurationen importieren kann, muss der Spiegel zurückgesetzt werden und die MikroTik-Default-Configuration darf NICHT geladen werden! Danach dann mit WinBox die Datei importieren oder das Script mittels SSH ausführen. Eine ausführliche Anleitung zur Vorgehensweise wird folgen.

In neueren Versionen vom RouterOS (Firmware des Mikrotik) gibt es auch direkt im Browser ein Terminal.

## Erklärung für manuelle Einrichtung

### Allgemein

#### 2025-04-30 by DC8LZ:

Der Spiegel geht über das WLAN Interface in das Hamnet mit ssid=„HAMNET DB0FRG“ und erhält dort via DHCP eine HAMNET-IP. Es gibt kein Passwort für dieses HAMNET-WLAN.

Dem Ethernet-Interface geben wir irgend eine private IP Adresse. Auf diesem Interface lassen wir einen DHCP Server laufen und jener vergibt den lokalen Geräten eine IP. Per NAT werden diese dann über/in das HAMNET angebunden.

Damit unsere Endgeräte wissen, dass die HAMNET-IPs über dieses Interface laufen sollen, setzen wir über den DHCP Server auf dem Ethernetinterface noch entsprechende Routen.

Anleitung und Infos zu Mikrotik, siehe [hier](#).

[Infos zum LHG 5 Spiegel](#).

Hörensagen: Man solle nur die letztes 6er RouterOS verwenden. Getestet hier ist bis zur f7.18.2 für HAMNET. Infos zu [mikrotik Software Webseite hier](#).

**Todo: Achtung: Die folgende Konfiguration ist noch nicht getestet... (tested siehe weiter unten, von 2020)**

```
##### CALLSIGN #####  
#  
# Hier zwei mal CALLSIGN ersetzten!  
# Der Rest unten passt idR. und muss meist  
# nicht angepasst werden.  
#  
/system identity set name=DC8LZ  
  
/interface wireless  
set [ find default-name=wlan1 ] disabled=no band=5ghz-a/n channel-
```

```
width=10mhz \  
  country=no_country_set disconnect-timeout=15s frequency=5705 frequency-  
mode=superchannel \  
  hw-retries=15 scan-list=5705 mode=station ssid="HAMNET DB0FRG" \  
  radio-name=DC8LZ  
  
##### unspezifisches... #####  
#  
/ipv6 settings  
  set disable-ipv6=yes max-neighbor-entries=8192  
  
##### HAMNET/WLAN #####  
#  
/interface wireless security-profiles  
  set [ find default=yes ] supplicant-identity=MikroTik  
  
/ip dhcp-client  
  add dhcp-options=hostname,clientid disabled=no interface=wlan1  
  
##### Ethernet #####  
# Spiegel hat 10.11.10.1/32  
/ip address  
  add address=10.11.10.1/24 interface=ether1 network=10.11.10.0  
##### DHCPD auf eth #####  
# DHCP Vergabe von 10.11.10.10-10.11.10.200  
/ip pool  
  add name=dhcp_pool0 ranges=10.11.10.10-10.11.10.250  
  
/ip dhcp-server  
  add address-pool=dhcp_pool0 disabled=no interface=ether1 name=dhcp1  
  
# code=121 ist eine statische  
# der Value beinhaltet gw IP 10.11.10.1 (s.o.) und Netz  
# see also  
https://help.mikrotik.com/docs/spaces/R0S/pages/24805500/DHCP#DHCP-DHCP0ptions.1  
# Calculator von hier wurde benutzt:  
# https://medo64.com/posts/configuring-classless-static-route-option  
#  
/ip dhcp-server option  
  add code=121 name="Hamnet" comment="44.0.0.0/9 44.128.0.0/10"  
0x092C000A0B0A010A2C800A0B0A01  
# mit def route und den zwei anderen:  
0x000A0B0A01092C000A0B0A010A2C800A0B0A01  
  
/ip dhcp-server network  
  add address=10.11.10.1/24 dhcp-option="Hamnet" ntp-server=44.148.224.123  
  
##### DNS, NTP... #####  
#  
/ip dns set allow-remote-requests=yes
```

```
/system clock set time-zone-name=Europe/Berlin

/system ntp client set enabled=yes

/system ntp client servers
  add address=44.148.224.123

##### Services auf Mikrotik #####
#
# Todo: Was/wann/wofür/warum ist api und api-ssl?
/ip service
  set telnet disabled=yes
  set ftp disabled=yes
# set api disabled=yes
# set api-ssl disabled=yes

##### Firewall/NAT #####
#
# ...ein paar Zeilen Unsinn sind auskommentiert, jene
# dann ggf interessant, wenn man noch einen wireguard Tunnel einrichtet...
/ip firewall connection tracking
  set udp-timeout=10s
/ip firewall filter
  add action=accept chain=input comment="defconf: accept
  established,related,untracked" connection-
  state=established,related,untracked
  add action=accept chain=input comment="wg in" in-interface=wireguard1 src-
  address-list="" disabled=yes
  add action=accept chain=input comment="wg udp in" disabled=yes in-
  interface=wireguard1 protocol=udp src-port="" disabled=yes
  add action=accept chain=forward comment="wg forward" disabled=yes in-
  interface=wireguard1 protocol=tcp disabled=yes
  add action=accept chain=forward comment="wg forward" in-interface=all-
  ethernet disabled=yes
  add action=drop chain=input comment="defconf: drop invalid" connection-
  state=invalid
  add action=accept chain=input comment="defconf: accept ICMP" protocol=icmp
  add action=accept chain=input comment="defconf: accept to local loopback
  (for CAPsMAN)" dst-address=127.0.0.1
  add action=drop chain=input comment="defconf: drop all not coming from LAN"
  in-interface-list=!LAN
  add action=accept chain=forward comment="defconf: accept in ipsec policy"
  ipsec-policy=in,ipsec
  add action=accept chain=forward comment="defconf: accept out ipsec policy"
  ipsec-policy=out,ipsec
  add action=fasttrack-connection chain=forward comment="defconf: fasttrack"
  connection-state=established,related disabled=yes hw-offload=yes
  add action=accept chain=forward comment="defconf: accept
  established,related, untracked" connection-
  state=established,related,untracked
  add action=drop chain=forward comment="defconf: drop invalid" connection-
```

```
state=invalid
add action=drop chain=forward comment="defconf: drop all from WAN not
DSTNATed" connection-nat-state=!dstnat connection-state=new in-interface-
list=WAN
/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade" ipsec-
policy=out,none out-interface-list=WAN
```

# Beispielkonfigurationen für MikroTik-Geräte / Stand Juli 2020

Bevor man diese Konfigurationen importieren kann, muss der Spiegel zurückgesetzt werden und die MikroTik-Default-Configuration darf NICHT geladen werden! Danach dann mit WinBox die Datei importieren oder das Script mittels SSH ausführen. Eine ausführliche Anleitung zur Vorgehensweise wird folgen.

## Portabel-Konfiguration

Zuerst mal eine Portabel-Konfiguration, die für den Einsatz auf Wiesen, Feldern etc. geeignet ist oder auch für den Einsatz zuhause, wenn man den Spiegel nicht in das Heimnetz integrieren möchte.

### Datei

[Download hier:](#)

db0frg-portabel.rsc

**ACHTUNG!** In der Datei gibt es an zwei Stellen (5. Zeile von oben und 3. Zeile von unten) das Wort **CALLSIGN**. Diese bitte durch das eigene Rufzeichen ersetzen indem man die Datei z.B. mit [Notepad++](#) öffnet. Alternativ einfach das Script unten kopieren, in einer Text Datei speichern und dann auf die Endung .rsc umbenennen

### Script

**ACHTUNG!** Im Script gibt es an zwei Stellen (5. Zeile von oben und 3. Zeile von unten) das Wort **CALLSIGN**. Diese bitte durch das eigene Rufzeichen ersetzen

```
/interface wireless
set [ find default-name=wlan1 ] band=5ghz-a/n channel-width=10mhz country=\
no_country_set disabled=no disconnect-timeout=15s frequency=5705 \
frequency-mode=superchannel hw-retries=15 mode=station-bridge radio-
```

```
name=\
    CALLSIGN scan-list=5705 ssid="HAMNET DB0FRG"
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip dhcp-server option
add code=121 name="Route 44.0.0.0/8" value=0x082cc0a80801
/ip pool
add name=dhcp_pool0 ranges=192.168.8.2-192.168.8.14
/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface=ether1 name=dhcp1
/ip address
add address=192.168.8.1/28 interface=ether1 network=192.168.8.0
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=wlan1
/ip dhcp-server network
add address=192.168.8.0/28 dhcp-option="Route 44.0.0.0/8" dns-server=\
    192.168.8.1 domain=Mikro.Tik ntp-server=\
    44.148.224.123
/ip dns
set allow-remote-requests=yes
/ip firewall filter
add action=reject chain=input comment=\
    "Web GUI vor Zugriff aus Hamnet schuetzen" dst-port=80 in-
interface=wlan1 \
    protocol=tcp reject-with=icmp-admin-prohibited
add action=reject chain=input comment=\
    "Winbox vor Zugriff aus Hamnet schuetzen" dst-port=8291 in-interface=\
wlan1 protocol=tcp reject-with=icmp-admin-prohibited
add action=reject chain=input comment=\
    "SSH vor Zugriff aus dem Hamnet schuetzen" dst-port=22 in-
interface=wlan1 \
    protocol=tcp reject-with=icmp-admin-prohibited
/ip firewall nat
add action=dst-nat chain=dstnat comment="Beispiel Portweiterleitung" \
    disabled=yes dst-port=80 in-interface=wlan1 protocol=tcp to-addresses=\
    192.168.8.14
add action=masquerade chain=srcnat comment=\
    "Restliches lokales Netz verstecken" out-interface=wlan1
/ip service
set telnet disabled=yes
set ftp disabled=yes
set api disabled=yes
set api-ssl disabled=yes
/system clock
set time-zone-name=Europe/Berlin
/system identity
set name=CALLSIGN
/system ntp client
set enabled=yes primary-ntp=44.148.224.123
```

# Heimnetz-Konfiguration

Hier noch die Konfiguration für eine feste Installation zuhause und Integration in das heimische Netzwerk. Es müssen dann noch Router zwei statische Routen auf die IP des Spiegels gesetzt werden: 44.0.0.0/9 und 44.128.0.0/10 jeweils zur IP des Spiegels.

## Datei

[Download hier:](#)

db0frg-portabel.rsc

**ACHTUNG!** In der Datei gibt es an zwei Stellen (5. Zeile von oben und 3. Zeile von unten) das Wort **CALLSIGN**. Diese bitte durch das eigene Rufzeichen ersetzen indem man die Datei z.B. mit [Notepad++](#) öffnet. Alternativ einfach das Script unten kopieren, in einer Text Datei speichern und dann auf die Endung .rsc umbenennen

## Script

**ACHTUNG!** Im Script gibt es an zwei Stellen (5. Zeile von oben und 3. Zeile von unten) das Wort **CALLSIGN**. Diese bitte durch das eigene Rufzeichen ersetzen

```
/interface wireless
set [ find default-name=wlan1 ] band=5ghz-a/n channel-width=10mhz country=\
no_country_set disabled=no disconnect-timeout=15s frequency=5705 \
frequency-mode=superchannel hw-retries=15 mode=station-bridge radio-
name=\
CALLSIGN scan-list=5705 ssid="HAMNET DB0FRG"
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip dhcp-server option
add code=121 name="Route 44.0.0.0/8" value=0x082cc0a80801
/ip pool
add name=dhcp_pool0 ranges=192.168.8.2-192.168.8.14
/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface=ether1 name=dhcp1
/ip address
add address=192.168.8.1/28 interface=ether1 network=192.168.8.0
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=wlan1
/ip dhcp-server network
add address=192.168.8.0/28 dhcp-option="Route 44.0.0.0/8" dns-server=\
192.168.8.1 domain=Mikro.Tik ntp-server=\
44.148.224.123
/ip dns
set allow-remote-requests=yes
```

```
/ip firewall filter
add action=reject chain=input comment=\
    "Web GUI vor Zugriff aus Hamnet schuetzen" dst-port=80 in-
interface=wlan1 \
    protocol=tcp reject-with=icmp-admin-prohibited
add action=reject chain=input comment=\
    "Winbox vor Zugriff aus Hamnet schuetzen" dst-port=8291 in-interface=\
wlan1 protocol=tcp reject-with=icmp-admin-prohibited
add action=reject chain=input comment=\
    "SSH vor Zugriff aus dem Hamnet schuetzen" dst-port=22 in-
interface=wlan1 \
    protocol=tcp reject-with=icmp-admin-prohibited
/ip firewall nat
add action=dst-nat chain=dstnat comment="Beispiel Portweiterleitung" \
    disabled=yes dst-port=80 in-interface=wlan1 protocol=tcp to-addresses=\
    192.168.8.14
add action=masquerade chain=srcnat comment=\
    "Restliches lokales Netz verstecken" out-interface=wlan1
/ip service
set telnet disabled=yes
set ftp disabled=yes
set api disabled=yes
set api-ssl disabled=yes
/system clock
set time-zone-name=Europe/Berlin
/system identity
set name=CALLSIGN
/system ntp client
set enabled=yes primary-ntp=44.148.224.123
```

## Heimnetz-Konfiguration

Hier noch die Konfiguration für eine feste Installation zuhause und Integration in das heimische Netzwerk. Es müssen dann noch Router zwei statische Routen auf die IP des Spiegels gesetzt werden: 44.0.0.0/9 und 44.128.0.0/10 jeweils zur IP des Spiegels.

### Datei

[Download hier:](#)

db0frg-heimnetz.rsc

**ACHTUNG!** In der Datei gibt es an zwei Stellen (5. Zeile von oben und 3. Zeile von unten) das Wort **CALLSIGN**. Diese bitte durch das eigene Rufzeichen ersetzen indem man die Datei z.B. mit [Notepad++](#) öffnet. Alternativ einfach das Script unten kopieren, in einer Text Datei speichern und dann auf die Endung .rsc umbenennen

## Script

**ACHTUNG!** Im Script gibt es an zwei Stellen (5. Zeile von oben und 3. Zeile von unten) das Wort **CALLSIGN**. Diese bitte durch das eigene Rufzeichen ersetzen

```
/interface wireless
set [ find default-name=wlan1 ] band=5ghz-a/n channel-width=10mhz country=\
    no_country_set disabled=no disconnect-timeout=15s frequency=5705 \
    frequency-mode=superchannel hw-retries=15 mode=station-bridge radio-
name=\
    CALLSIGN scan-list=5705 ssid="HAMNET DB0FRG"
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool0 ranges=192.168.8.2-192.168.8.14
/ip address
add address=192.168.8.1/28 interface=ether1 network=192.168.8.0
/ip dhcp-client
add dhcp-options=hostname,clientid disabled=no interface=wlan1
add dhcp-options=hostname,clientid disabled=no interface=ether1
/ip dns
set allow-remote-requests=yes
/ip firewall filter
add action=reject chain=input comment=\
    "Web GUI vor Zugriff aus Hamnet schuetzen" dst-port=80 in-
interface=wlan1 \
    protocol=tcp reject-with=icmp-admin-prohibited
add action=reject chain=input comment=\
    "Winbox vor Zugriff aus Hamnet schuetzen" dst-port=8291 in-interface=\
wlan1 protocol=tcp reject-with=icmp-admin-prohibited
add action=reject chain=input comment=\
    "SSH vor Zugriff aus dem Hamnet schuetzen" dst-port=22 in-
interface=wlan1 \
    protocol=tcp reject-with=icmp-admin-prohibited
/ip firewall nat
add action=dst-nat chain=dstnat comment="Beispiel Portweiterleitung" \
    disabled=yes dst-port=80 in-interface=wlan1 protocol=tcp to-addresses=\
    192.168.8.14
add action=masquerade chain=srcnat comment=\
    "Restliches lokales Netz verstecken" out-interface=wlan1
/ip service
set telnet disabled=yes
set ftp disabled=yes
set api disabled=yes
set api-ssl disabled=yes
/system clock
set time-zone-name=Europe/Berlin
/system identity
set name=CALLSIGN
/system ntp client
```

```
set enabled=yes primary-ntp=44.148.224.123
```

From:

<https://radio.feindas.de/> - **radio.feindas.de**

Permanent link:

<https://radio.feindas.de/hamnet:beispielkonfigurationen?rev=1746476568>

Last update: **2025/05/05 20:22**

