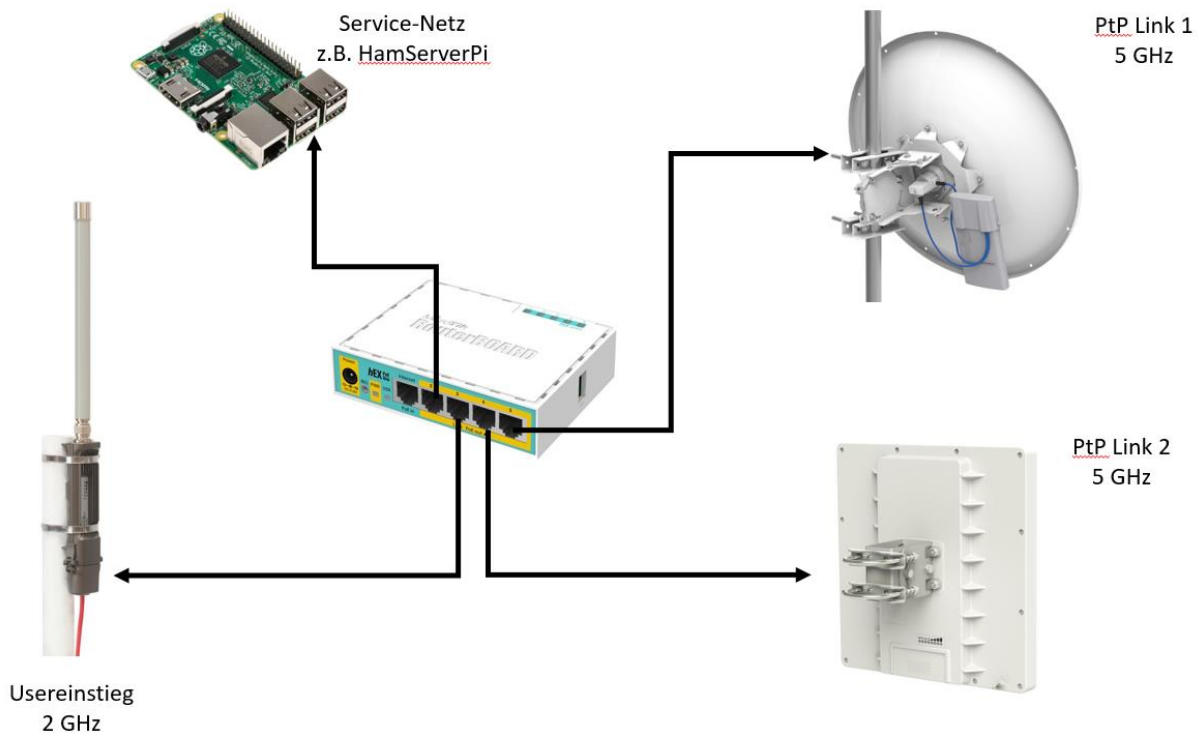


Konfiguration eines Hamnet Knoten mit Mikrotik RouterOS



Erstellt von Attila Kocis, DL1NUX (dl1nux@darc.de)

Stand: 23.07.2020

Bitte stets nach einer aktuellen Version umschauen auf www.dl1nux.de

Konfiguration eines Hamnet Knoten mit Mikrotik RouterOS	1
1. Allgemeines zum Thema Hamnet	4
2. Mikrotik RouterOS Vorbereitungen	5
2.1. Arbeiten mit WinBox und RouterOS	5
2.1.1. Aufgabe und Download von winbox.exe.....	5
2.1.2. Anschluss der Hardware.....	5
2.1.3. Spannungsversorgung der Router.....	5
2.1.4. Login mit WinBox über die Mac-Adresse	6
2.1.5. Erste Schritte mit WinBox	7
2.2. RouterOS Upgrade (offline).....	8
2.3. RouterOS Upgrade (online)	9
2.4. Mikrotik-RouterOS Upgrade Mirror im Hamnet	10
2.5. Firmware Upgrade.....	11
2.6. Konfiguration des Routers zurücksetzen.....	11
3. Allgemeines zur Konfiguration	13
3.1. Grundsätzliches zum IP-technischen Aufbau eines HAMNET Knotens:.....	13
3.2. To-Do Liste vor der Konfiguration	14
3.3. Aufbau des Beispielknotens DBODAH	15
4. Konfiguration der Linkstrecke zu DBOZKA.....	17
4.1. Einrichten der IP-Parameter in der Außeneinheit.....	17
4.2. Einrichten der HF-Parameter für die WLAN Verbindung	23
5. Konfiguration der Linkstrecke zu DBOTVM.....	25
5.1 Einrichten der IP-Parameter in der Außeneinheit (analog zum DBOZKA Link).....	25
5.2. Einrichten der HF-Parameter für die WLAN-Verbindung.....	26
5.3. Weitere Parameter.....	26
6. Konfiguration Usereinstieg.....	27
6.1. Konfiguration der Bridge	27
6.2. Konfiguration der HF-Parameter	28
7. Unterschiede beim Einsatz von Routern mit integrierten WLAN-Modulen.....	30
8. Konfiguration einer Ubiquity Außeneinheit.....	31
9. Konfiguration des zentralen Routers.....	35
9.1. IP-Adressen den Interfaces zuweisen.....	35
9.2. DNS-Server eintragen	36
9.3. NTP Client einrichten.....	36
9.4. NTP Server einrichten.....	38
9.5. DHCP Server konfigurieren.....	39
9.6. DHCP-Server für das Usernetzwerk eintragen	41
9.7. Optional: HF Parameter den WLAN Ports zuweisen.	43
9.8. Identity eintragen.....	43
9.9. BGP Monitoring einschalten.....	43
10. Ethernet over IP (EoIP) Tunnel nutzen	46
10.1. Was ist EoIP?	46
10.2. Wann benötigt man EoIP?.....	46
10.3. Verkabelung der Routerboards untereinander.....	46
10.4. EoIP konfigurieren	48
10.5. WLAN-Interfaces des RB433AH mit dem zentralen Router „verbinden“	49
10.6 EoIP intelligent nutzen	51
11. VLAN am HAMNET Knoten nutzen.....	53
11.1 Einleitung zu VLAN	53

11.2	Konfigurationsbeispiel.....	53
12.	Konfiguration BGP Routing.....	61
12.1.	Begriffserklärungen	61
12.2.	Vorbereitungen	61
12.3.	BGP Instanz (16 Bit) einrichten.....	62
12.3.1.	16 Bit BGP.....	62
12.3.2.	Peers einrichten.....	62
12.3.3.	Eintragungen im Reiter „Networks“	64
12.4.	BGP Instanz (32 Bit) einrichten.....	65
12.4.1.	32 bit BGP	65
12.4.2.	Peers einrichten.....	67
12.4.3.	Eintragungen im Reiter „Networks“	68
12.5.	Kontrolle	68
13.	Sende- und Strahlungsleistungen im Hamnet.....	69
14.	Sendebetrieb mit ISM Parametern	70
14.1.	Wann ist ISM Betrieb notwendig bzw. sinnvoll?.....	70
14.2.	ISM Sendeparameter Allgemein.....	70
14.3.	ISM Parameter bei Mikrotik RouterOS.....	72
14.4.	ISM Parameter bei Ubiquity AirOS V.....	73
15.	VPN Server (PPTP) einrichten	74
15.1.	Voraussetzungen und IP-Einstellungen.....	74
15.2.	PPTP Server in RouterOS konfigurieren	74
16.	Sonderfälle beim RSSI-Monitoring	77
17.	PoE Stromversorgung einer Powerbox und ähnliche PoE Switches	80

1. Allgemeines zum Thema Hamnet

Das Hamnet ist ein international koordiniertes auf dem TCP/IP Protokoll basierendes Datennetzwerk zwischen automatisch arbeitenden Amateurfunkstationen (Backbone). Da im Hamnet aber auch viele Dienste angeboten werden, ist es auch für User interessant.

Da Amateurfunkbänder direkt neben den ISM Bändern angesiedelt sind bzw. sich auch teilweise mit ihnen überschneiden, kann handelsübliche WLAN Hardware eingesetzt werden.

Zur Verwendung kommen in der Regel Komponenten von den Herstellern Mikrotik und Ubiquity, da diese sich auch auf Amateurfunkfrequenzen betreiben lassen. Da es sich hierbei um Produkte mit großen Produktionsstückzahlen handelt, sind diese für Amateurfunkverhältnisse preisgünstig zu bekommen.

In Deutschland ist die HAMNET Nutzung im 13cm (2,3 GHz), 9cm (3,4 GHz) und 6cm (5,7 GHz) Band erlaubt. Aufschluss über die verwendbaren Frequenzen geben die Bandpläne.

Quelle: <http://www.darc.de/referate/vus/bandplaene>

13cm Band: (Maximale Bandbreite 5 MHz)

2362 MHz* 2392 MHz 2397 MHz

9cm band: (Maximale Bandbreite 10 MHz)

3415 MHz 3425 MHz 3435 MHz 3445 MHz 3455 MHz

6cm Band: (Maximale Bandbreite 10 MHz)

5675 MHz 5685 MHz 5695 MHz 5705 MHz 5715 MHz 5725 MHz

5735 MHz 5745 MHz 5755 MHz** 5775 MHz 5785 MHz 5795 MHz

5805 MHz 5815 MHz 5825 MHz

* 2362 MHz wird laut diverser Aussagen aktuell nicht mehr von der BNetzA genehmigt

** 5755 MHz als Schutzkanal zum Schmalbandbereich darf nur im Notfall belegt werden

Traditionell wird das 13cm Band für UserEinstiege verwendet und das 6cm Band für Linkstrecken und UserEinstiege. Das 9cm Band wird bisher kaum genutzt, da geeignete Hardware nur eingeschränkt zur Verfügung steht.

2. Mikrotik RouterOS Vorbereitungen

2.1. Arbeiten mit WinBox und RouterOS

2.1.1. Aufgabe und Download von winbox.exe

WinBox ist ein mächtiges Tool von Mikrotik zum Konfigurieren von RouterOS, der Software auf den Mikrotik Routern. Es läuft nativ unter Windows, kann aber auch mit entsprechenden Emulatoren unter MacOS und Linux genutzt werden. Das Programm besteht aus einer einzigen .EXE Datei und muss nicht installiert werden, läuft also „portable“ von allen denkbaren Speichermedien.

Der Download erfolgt von der Mikrotik-Webseite, dort befindet sich die stets aktuelle Version. Ältere Versionen können manchmal nicht mehr mit den neueren RouterOS Versionen kommunizieren.

<http://www.mikrotik.com/download>

Mit WinBox kommt man auf alle Mikrotik Router drauf, selbst wenn diese noch keinerlei IP-Adressen besitzen. Voraussetzung ist, dass sich der Router und der PC im selben Subnetz befinden. Die Kommunikation läuft in diesem Fall über die MAC-Adresse. Dies ist bei der Inbetriebnahme eines „leeren“ Mikrotik Routers auch notwendig, da er ja noch nicht über eine IP-Adresse ansprechbar ist. Hat man dem Router eine IP-Adresse zugewiesen, kann man sich ab dann auch über die IP-Adresse einloggen bzw. das Webinterface von RouterOS nutzen. Das Webinterface, welches über die IP-Adresse des Routers erreichbar ist, bietet im Prinzip den gleichen Funktionsumfang wie WinBox, ist allerdings etwas träge zu bedienen.

2.1.2. Anschluss der Hardware

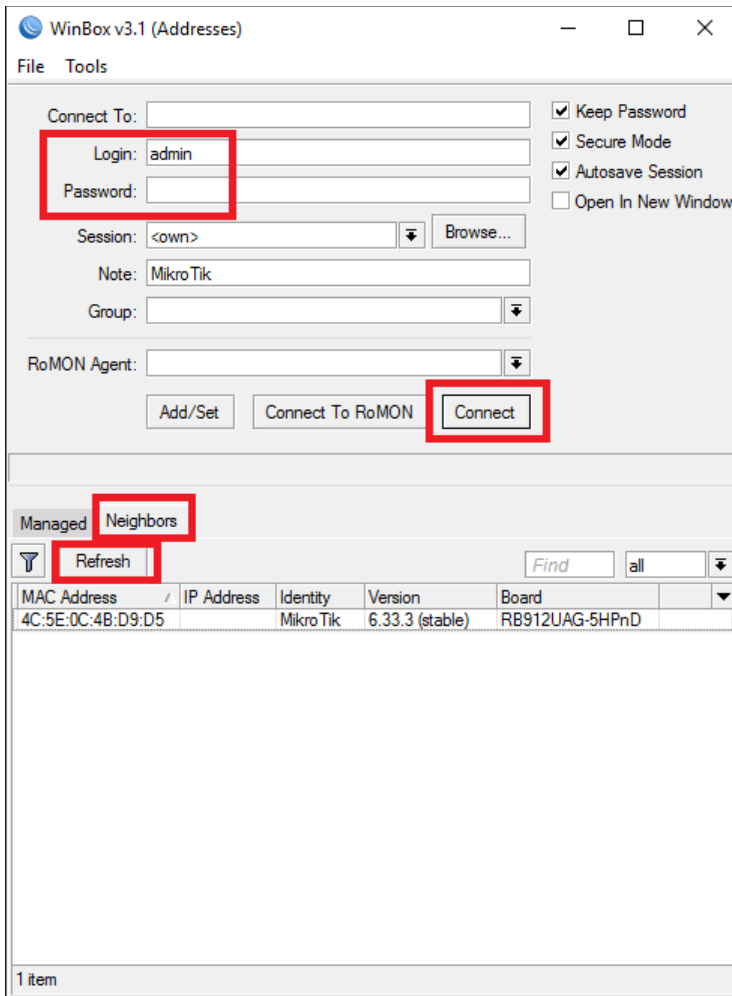
Den Router kann man entweder direkt per Ethernet-Kabel an den PC oder aber auch ans Heimnetzwerk (LAN) anschließen. In beiden Fällen wird er von WinBox gefunden und kann angesprochen werden. Der Anschluss im LAN hat den Vorteil, dass man dem Router per Defaultroute einen Internetzugang bekannt machen kann, um z.B. RouterOS Updates direkt online abzurufen.

2.1.3. Spannungsversorgung der Router

Selbstverständlich muss der Router auch mit Strom versorgt werden, entweder per Netzteil direkt (wenn möglich), oder per „Power over Ethernet“ (PoE). PoE versorgt die Router über die unbenutzten Adernpaare Nr. 4, 5, 7 und 8 mit Strom. Die Versorgungsspannung kann bei Mikrotik Routern ca. 9 bis 30 Volt betragen (bei manchen auch bis 48V). Bei der Stromversorgung über längere Kabel sollte man mindestens ein 24 Volt Netzteil verwenden, da die Spannung mit der Leitungslänge abfallen und es dadurch zu Fehlfunktionen kommen kann.

Tipp: Bei den meisten Mikrotik Routern lässt sich die anliegende Versorgungsspannung direkt in WinBox unter SYSTEM > HEALTH ablesen. Sollte der Verdacht bestehen, dass es mit der Spannungsversorgung Probleme gibt, ist ein Blick dahin sehr hilfreich.

2.1.4. Login mit WinBox über die Mac-Adresse



Ist der Router im LAN angeschlossen und wird mit Strom versorgt, startet man WinBox und öffnet unten den Reiter „Neighbours“. Hier sollte nun der Router angezeigt werden. Ein Klick auf „Refresh“ aktualisiert die Ansicht falls der Router erst zwischenzeitlich hinzugekommen ist.

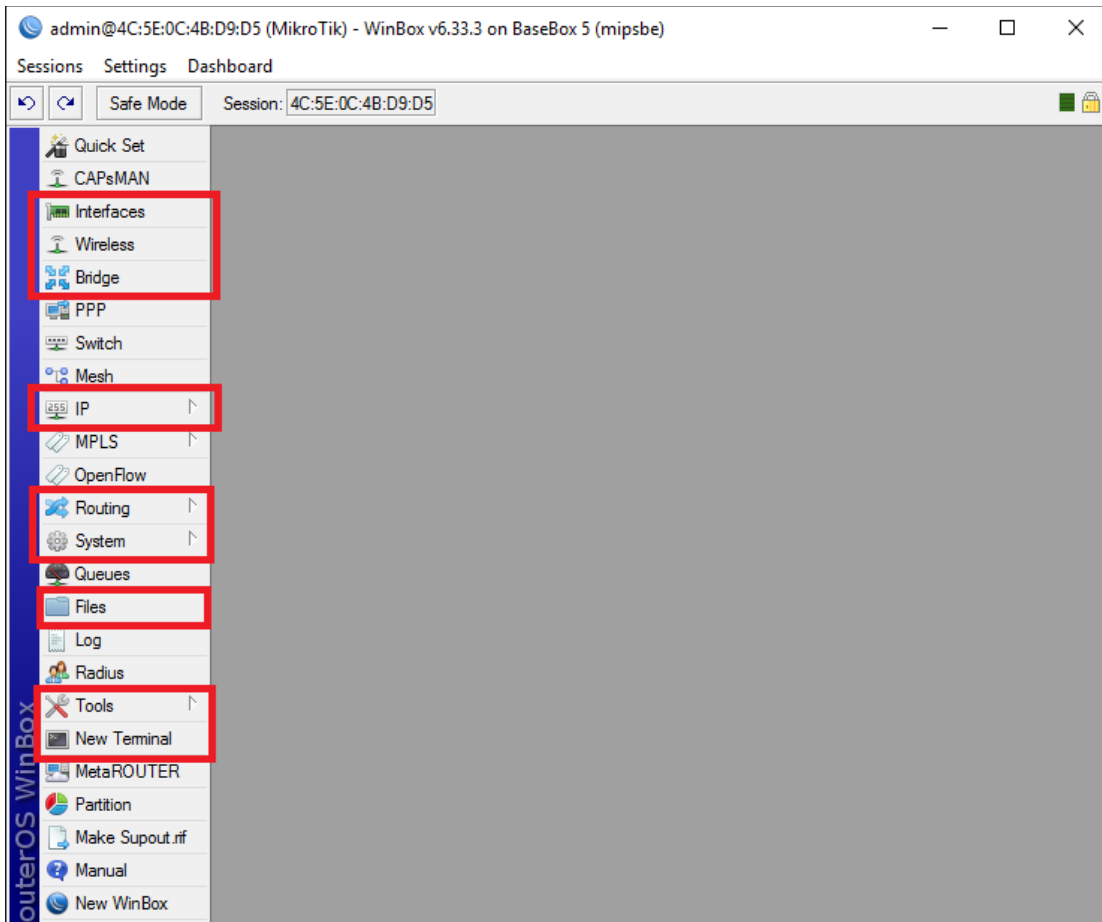
Man sieht die MAC-Adresse, die installierte RouterOS Version und das Routermodell. Wurde dem Router bereits eine IP-Adresse zugewiesen, erscheint diese ebenfalls unter „IP Address“.

Wenn man nun auf die MAC-Adresse des Routers klickt, wird diese in das „Connect To“ Feld oben übernommen. Klickt man auf die vorhandene IP-Adresse wird die IP-Adresse übernommen. Diese muss dann aber auch netzwerktechnisch erreichbar sein, will man sich damit verbinden. Hat der Router eine 10.x.y.z Adresse und befindet man sich selbst aber in einem 192.168.x.y-Netz, schlägt der Verbindungsaufbau über die IP-Adresse fehl.

Die Standard-Zugangsdatei bei Mikrotik lauten:

```
Login:      admin
Password:   nicht vorhanden bzw. bleibt leer
```

2.1.5. Erste Schritte mit WinBox



Nach dem Login öffnet sich die WinBox GUI. In der Titelleiste sind MAC- bzw. IP-Adresse, die installierte RouterOS-Version und der Routertyp sichtbar. Die Ansicht ist bei allen Routermodellen identisch, unabhängig von der technischen Ausstattung.

In der linken Spalte befinden sich die Konfigurationsmenüs. Die wichtigen Menüs sind hervorgehoben.

- **Interfaces:** Hier können alle physischen (LAN, WLAN) und virtuellen (Bridges, EoIP, VPN Tunnel etc.) Interfaces konfiguriert werden
- **Wireless:** Hier werden die Wireless Interfaces konfiguriert
- **Bridge:** Hier können Bridges „gebildet“ werden
- **Switch:** Hier können VLAN Einstellungen vorgenommen werden.
- **IP:** Hier werden alle IP Einstellungen vorgenommen (Adresse, DNS, DHCP, Firewall etc.)
- **Routing:** Hier wird das für das Hamnet wichtige BGP Routing konfiguriert.
- **System:** Hier werden die technischen Parameter des Routerboards konfiguriert, wie z.B. Userverwaltung, Paketverwaltung und es gibt Möglichkeiten für Reboot, shutdown etc.)
- **Files:** Alle lokal gespeicherten Daten werden hier aufgeführt. Diese lassen sich per drag and drop von bzw. in den Windows Explorer hin und her kopieren.
- **Tools:** Wichtige Tools wie „ping“ und „traceroute“ finden sich hier
- **New Terminal:** Öffnet ein Kommandofenster. RouterOS ist komplett per Kommandozeile konfigurierbar.

Die erste Aktion sollte das setzen eines Admin Kennwortes sein unter **SYSTEM > PASSWORD**

2.2. RouterOS Upgrade (offline)

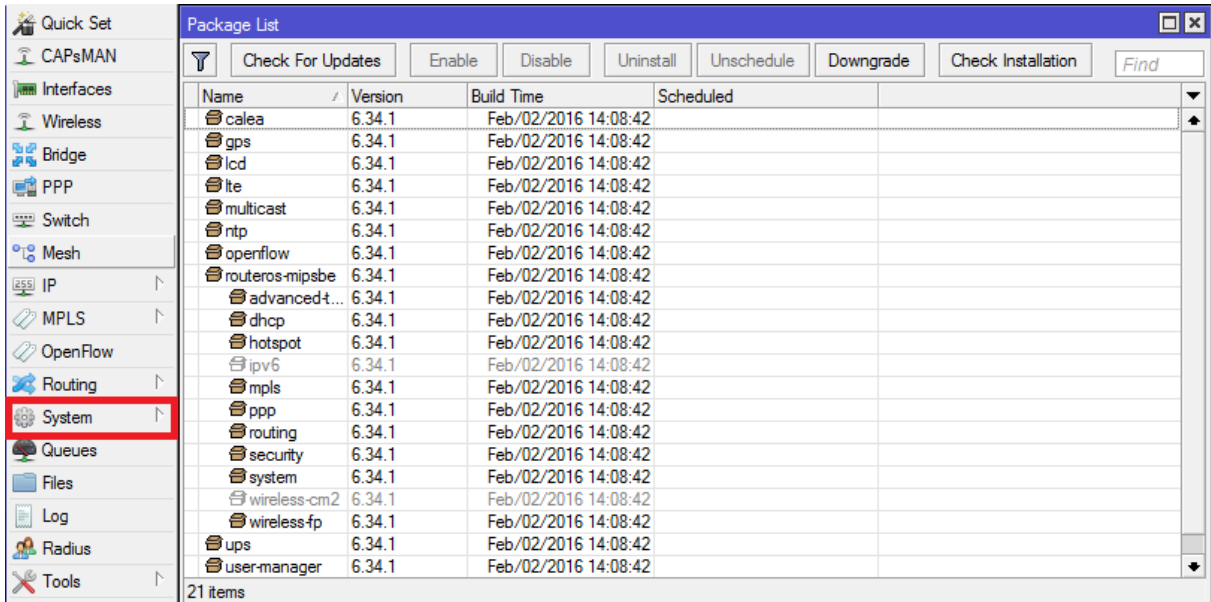
Nach dem Ändern des Admin Kennworts sollte man zuerst die Firmware und das RouterOS prüfen und gegebenenfalls aktualisieren.

Aktuelle RouterOS Pakete kann man über <http://www.mikrotik.com/download> beziehen. Hier sollte man wenn möglich die aktuelle und stabile Version laden (Current). Release Candidate (RC) Versionen sind Vorabversionen und können Fehler enthalten, sind also nicht zu empfehlen. Man sollte nach Erscheinen einer neuen (Current-)Version erst einmal abwarten und diese keinesfalls sofort installieren. Gelegentlich sind diese auch fehlerhaft. Man kann also ruhig auch eine geringfügig ältere Version nehmen. Von Vorteil ist es auf allen Routern zumindest die gleiche Version zu installieren, um Kompatibilitätsprobleme zwischen den Versionsständen zu vermeiden.

Hinweis: Mit RouterOS Version 6.37 gab es eine grundsätzliche Änderung bei der Behandlung der Wireless-Devices. Aktualisiert man von einer Version 6.36 oder kleiner auf 6.37 oder höher, verschwinden anschließend die Wireless-Devices aus der Übersicht, als wenn sie nicht mehr da wären. Es muss daher das „neue“ Zusatzpaket „wireless.npk“ installiert und der Router neu gestartet werden. Anschließend sind die Wireless Devices wieder verfügbar. Man sollte dieses Update also nicht machen, wenn man keinen direkten Zugriff per LAN auf das Routerboard hat, sonst sperrt man sich aus.

Ablauf des Updates:

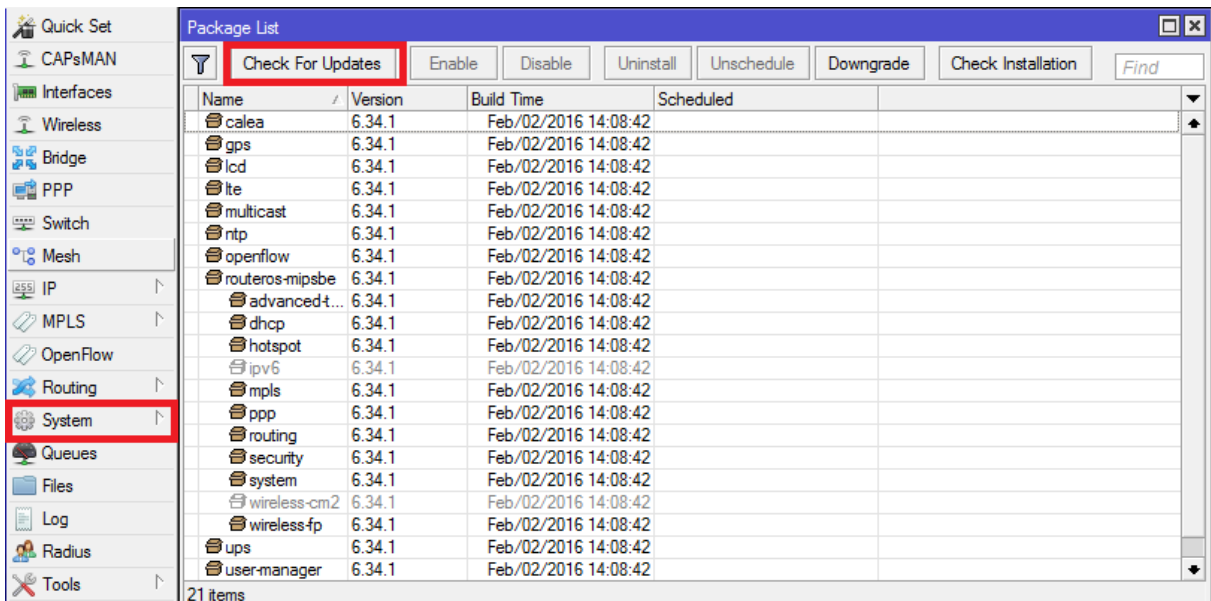
- a) Download der aktuellen RouterOS Pakete. Das „Main package“ enthält das eigentliche RouterOS. Die „Extra packages“ enthalten weitere Module, von denen auch einige benötigt werden.
- b) Das Untermenü „Files“ wird geöffnet, es zeigt alle vorhandenen Dateien auf dem internen Speicher an. In der Statusleiste sieht man übrigens die aktuelle Speicherplatzbelegung.
- c) Bei geöffnetem WinBox Fenster werden die *.npk Dateien per „drag and drop“ aus dem Windows Explorer in das „Files“ Fenster gezogen. Dadurch werden die Dateien auf das Routerboard kopiert. Falls Das Routerboard nicht genug Speicher hat (manche haben auch nur 16 MB Speicher), kann man dies auf zweimal machen. Zuerst das RouterOS NPK File rüberschieben und das Routerboard aktualisieren lassen. Dann im zweiten Rutsch die restlichen Dateien.
- d) Die Aktualisierung beginnt beim nächsten Reboot automatisch. Der Reboot lässt sich auch durch SYSTEM > REBOOT sofort durchführen
- e) Über SYSTEM > Packages lässt sich anschließend der Versionsstand der Pakete prüfen:



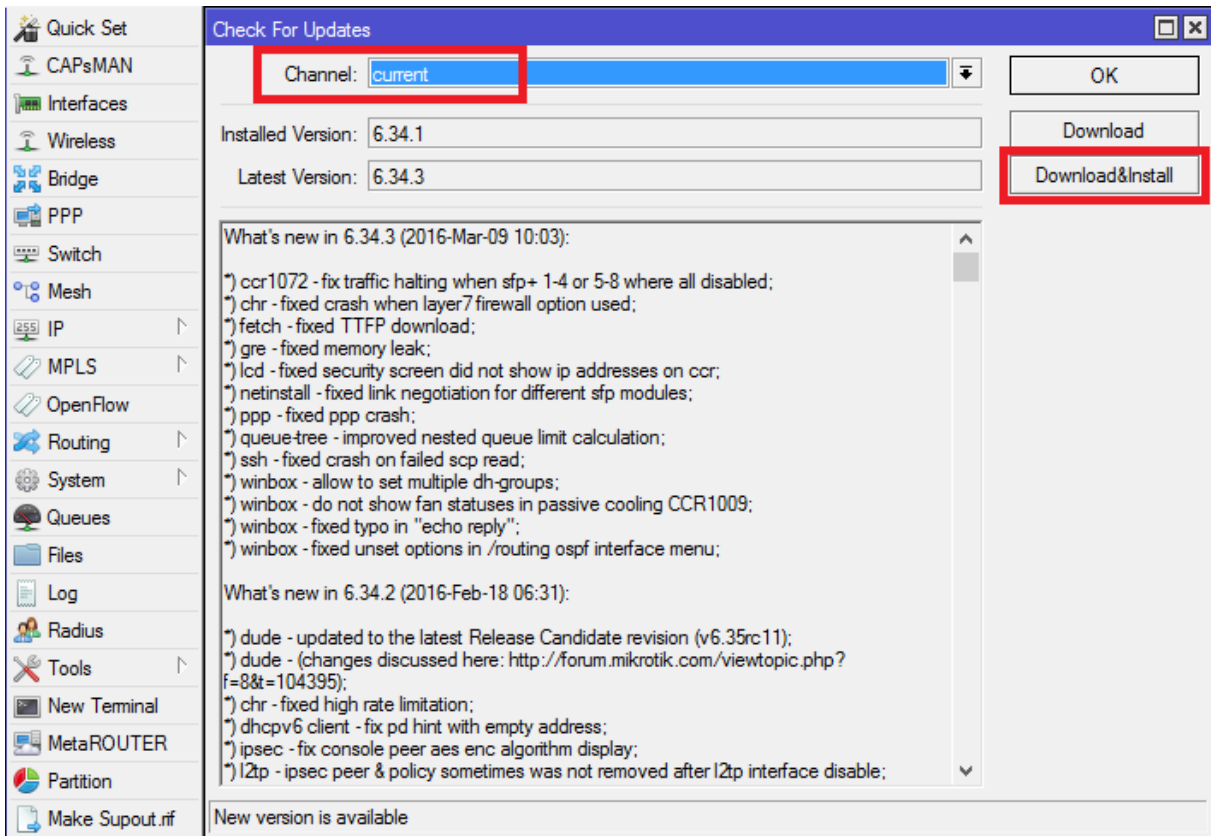
Ausgegraute Module sind im Router deaktiviert.

2.3. RouterOS Upgrade (online)

Wenn dem Router eine Internetverbindung bekannt ist, kann das Upgrade bzw. die Upgradeprüfung auch online durchgeführt werden. Dazu ist mindestens eine Defaultroute ins Internet und ein eingetragener DNS Server notwendig. Auch dies kann unter SYSTEM > Packages geprüft werden.



Beim Klick auf „Check for Updates“ führt der Router eine Onlineprüfung nach einer aktuelleren Version durch.



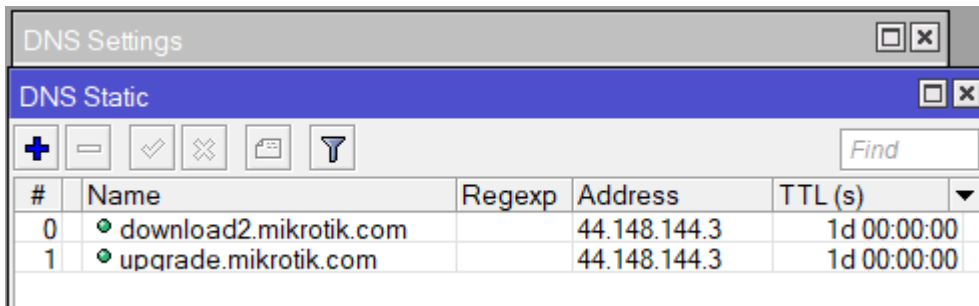
Bei „Channel“ kann man den Release Kanal auswählen. „Current“ wäre hier die richtige Auswahl, da Betaversionen nicht produktiv eingesetzt werden sollten. Über den Button „Download & Install“ wird das Paket automatisch geladen und der Router rebootet um die Installation durchzuführen

2.4. Mikrotik-RouterOS Upgrade Mirror im Hamnet

Quelle: <https://de.ampr.org/services>

Im HAMNET sind zahlreiche Mikrotik-Geräte mit unterschiedlichster Hardware-Architektur installiert. Viele davon haben keinen direkten Zugriff auf das Internet. Die im System integrierten, automatischen Upgrade-Funktionen können deshalb nicht ohne weiteres genutzt werden. Das Aktualisieren auf die neueste RouterOS-Version gestaltet sich für den Admin dann relativ umständlich und zeitraubend. Um auch solchen Mikrotik-Geräten ein automatisches Upgraden mit wenigen Klicks zu ermöglichen, betreibt die DL-IP-Koordination einen im HAMNET erreichbaren RouterOS-Mirror. Er ist nicht allgemein einsehbar, sondern nur für die Upgrade-Prozeduren in den Mikrotik-Geräten im HAMNET erreichbar.

Um ein Mikrotik-Device auf automatisches Upgrade innerhalb des HAMNET umzustellen, müssen im eigenen DNS des Gerätes die IP-Adressen für die originalen Upgrade-Server von Mikrotik auf die IP-Adresse des HAMNET-Upgrade-Mirrors umgeschrieben werden. Das geschieht durch zwei statische Einträge in den DNS-Cache des jeweiligen Gerätes. In der WinBox sieht das dann folgendermaßen aus:



#	Name	Regex	Address	TTL (s)
0	download2.mikrotik.com		44.148.144.3	1d 00:00:00
1	upgrade.mikrotik.com		44.148.144.3	1d 00:00:00

Der HAMNET-Upgrade-Server der DL-IP-Koordination unterstützt derzeit alle von Mikrotik bereitgestellten Hardware-Plattformen und Version-Channels:

- Channel current mipsbe ppc x86 mipsle tile smips arm
- Channel release candidate mipsbe ppc x86 mipsle tile smips arm
- Channel bugfix mipsbe ppc x86 mipsle tile smips

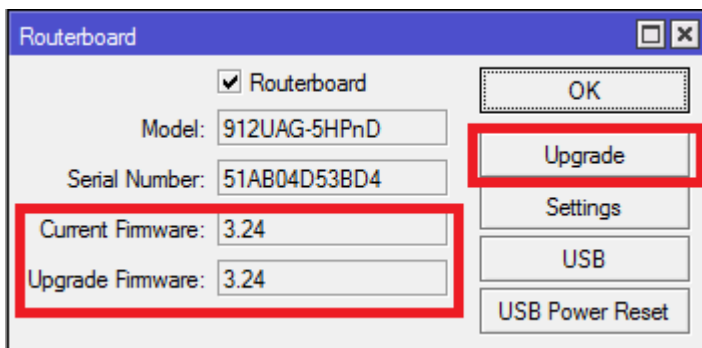
Seit 2016 existiert auch noch ein zweiter Mirror im Hamnet bei DBOSDA, die IP lautet 44.225.164.2

Quelle: <https://www.afu.rwth-aachen.de/news/144-routeros-update-per-hamnet-aus-aachen>

2.5. Firmware Upgrade

Nach dem RouterOS Upgrade sollte man die Firmware noch prüfen und ggf. aktualisieren. Diese prüft man unter SYSTEM > ROUTERBOARD

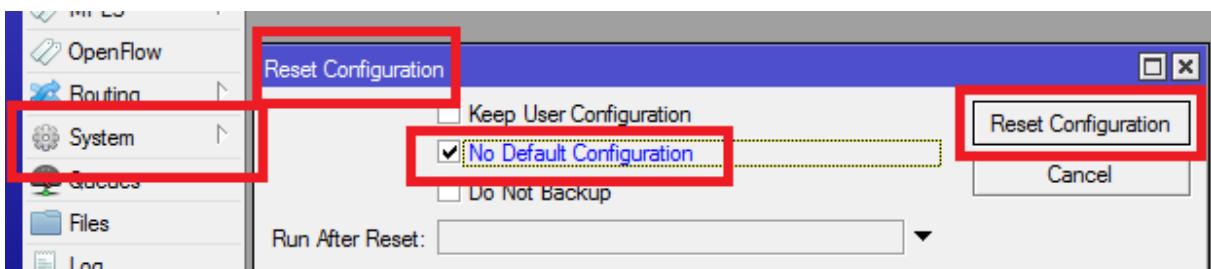
Sollte nach der Installation des aktuellen RouterOS ein neues Firmwarepaket vorliegen, wird dies unter „Upgrade Firmware“ angezeigt. Mit einem Klick auf „Upgrade“ wird die Firmware beim nächsten Reboot installiert.



2.6. Konfiguration des Routers zurücksetzen

Bei manchen Routern ist bei der Auslieferung eine Beispielkonfiguration aufgespielt. Grundsätzlich sollten daher vor der Konfiguration eines Mikrotik Routers für das Hamnet alle vorhandenen Einstellungen zurückgesetzt werden, um ungewollte Fehlkonfigurationen zu vermeiden:

SYSTEM > Reset Configuration > „No Default Configuration“ aktivieren > „Reset Configuration“



Das Setzen des Häkchens bewirkt, dass nach dem Reset keine Standardkonfiguration geladen wird, sondern der Router jungfräulich bleibt.

Nachdem nun alle Vorbereitungen getroffen sind, werden die Außeneinheiten eingerichtet (Linkstrecken und UserEinstieg).

3. Allgemeines zur Konfiguration

In der folgenden Anleitung soll beschrieben werden, wie man mit Mikrotik und ggf. Ubiquity Hardware einen [HAMNET](#) Netzknoten aufbauen kann. Wir wollen dies am Beispiel von [DB0DAH](#) (Stand 06/2013) erläutern.

Grundkenntnisse in TCP/IP und Computernetzwerken sollten vorhanden sein und die folgenden Begriffe sollten keine Verständnisprobleme verursachen:

- [IP-Adresse](#), [Netzmaske](#), [DNS](#), [DHCP](#), [NTP](#), [Hub](#), [Switch](#), [Bridge](#), [PoE](#)

Zu Beginn wird kurz der Aufbau des Beispielknotens DB0DAH erklärt, das Handling mit RouterOS und WinBox beschrieben und gezeigt, welche Vorbereitungen zu treffen sind.

Im Anschluss werden zuerst die Außeneinheiten (Links, UserEinstieg) konfiguriert und danach der zentrale Router. Das hat den Vorteil das man schon während des Einrichtens des Routers das Zusammenspiel mit den Außeneinheiten überprüfen kann.

Anschließend wird die Ethernet over IP (EoIP) Technik erklärt, die es ermöglicht beliebig Routerboards zusammen zu schalten und als Einheit zu nutzen.

3.1. Grundsätzliches zum IP-technischen Aufbau eines HAMNET Knotens:

Jeder Hamnet Knoten erhält von den [Koordinatoren](#) mehrere IP-Subnetze zugewiesen. Pro Standort gibt es ein Site-Network mit einer Größe von /27 mit 30 nutzbaren Adressen, welches bei Bedarf auch auf /26 vergrößert werden kann (62 nutzbare Adressen). Das /27er Site-Network wird grundsätzlich in zwei /28er Netze aufgeteilt. Der erste Teil wird als Service-Network genutzt. In diesem befinden sich alle lokal angeschlossenen Geräte, z.B. RaspberryPi, Server, PCs sowie alle weiteren IP-fähigen Geräte. Auch kann man hier einen DHCP Server laufen lassen, der ein paar IPs dynamisch vergibt, falls sich ein Sysop am Standort ins Netzwerk einklinken möchte.

Im User-Network befinden sich alle User, die sich von außen in den Hamnet-Knoten einwählen. Quasi der „normale“ OM, der sich über HF mit dem Knoten verbindet. Man trennt die beiden Netze idealerweise voneinander, weil man dann auch die Gelegenheit hat diese unterschiedlich zu behandeln. Während evtl. ein PC oder RaspberryPi einen Internetzugriff benötigt für z.B. Updates, ist dies bei Usern weder gewünscht noch erlaubt. Dies wird man mit einer Firewall-Regel, nur für das User-Network, unterbinden.

Beispiel DB0FHC:

44.149.27.192/27	Site-Network
44.149.27.192/28	Service-Network
44.149.27.208/28	User-Network

Zusätzlich für jeden Link wird ein separates /29 Backbone-Network (sechs nutzbare Adressen) zugewiesen. Da bei Links pro Linkpartner i.d.R. zwei IP-Adressen benötigt werden, sind es insgesamt vier pro Link die letztendlich benötigt werden. Die IPs werden wie folgt im Netz verwendet:

Beispielnetz: 44.148.12.8/29 DB0DRH-DB0FHC							
.8	.9	.10	.11	.12	.13	.14	.15
Netz	DB0DRH	DB0DRH	frei	frei	DB0FHC	DB0FHC	Broadcast
n.B.	Router	TRX			TRX	Router	n.B.

Es gibt auch eine Konvention, die festlegt, welche DNS-Namen bestimmte Geräte am Standort erhalten. Die Einheitlichkeit erleichtert das „Verstehen“ des Aufbaus eines Standorts bereits aus der HamnetDB heraus. Siehe folgendes Beispiel DB0FHC:

Host-IP	M	Hostname	Type
44.148.12.13	●	trx-db0drh.db0fhc	Service
44.148.12.14	●	bb-db0drh.db0fhc	Routing-Radio
44.148.12.17	●	bb-dl1nux.db0fhc	Routing-ISM
44.148.12.18	●	trx-dl1nux.db0fhc	Service
44.148.12.33	●	bb-db0son.db0fhc	Routing-Radio
44.148.12.34	●	trx-db0son.db0fhc	Service
44.148.240.234	●	wan-hamcloud.db0fhc	Routing-Tunnel
44.149.27.192	●	network.db0fhc	Service
44.149.27.193	●	router.db0fhc	Service
44.149.27.209	●	gw.db0fhc	Service
44.149.27.211	●	nsm-so.db0fhc	Service
44.149.27.220	●	sxt5-no.db0fhc	Service

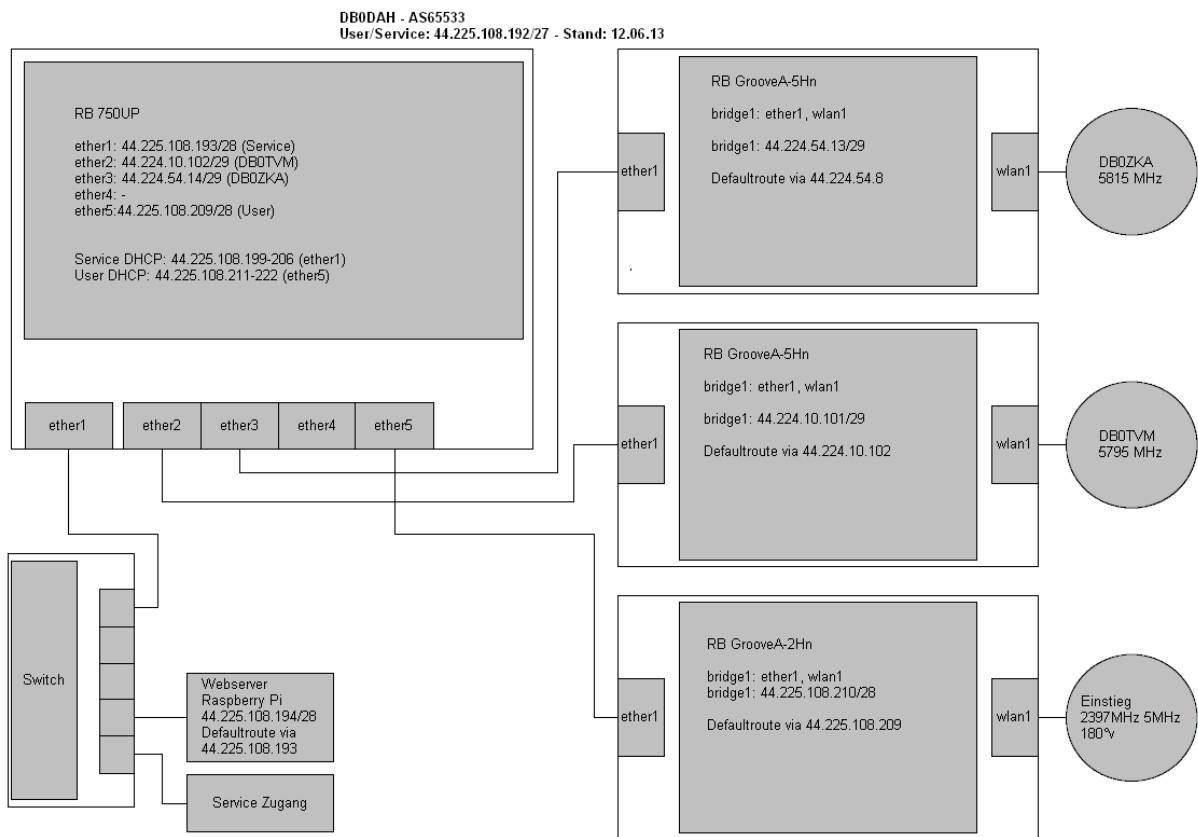
- Die erste IP-Adresse im Service-Network ist der Router selbst und erhält den DNS-Namen „**router.rufzeichen**“ (rot markiert)
- Die erste IP-Adresse im User-Network ist ebenfalls der Router selbst und erhält den DNS-Namen „**gw.rufzeichen**“ (gelb markiert). Dies bezeichnet für die User das „Gateway“ aus dem Usernetz heraus.
- Das Routing-Network zu DB0DRH ist eine Tabelle vorher nochmal genau aufgeschlüsselt. Der Router am Standort bekommt die erste bzw. letzte nutzbare IP im Subnetz und den DNS-Namen „**bb-gegenstation.rufzeichen**“ (blau markiert). BB steht hier für „Backbone“. „Gegenstation“ ist das Rufzeichen der Gegenstation.
- Die zweite bzw. fünfte (vorletzte) nutzbare Adresse ist für die eigentlichen Antennen bzw. Außeneinheiten reserviert. Diese bekommen den DNS-Namen „**trx-gegenstation.rufzeichen**“ (grün markiert). Vor Beginn der IP-Umstellung in DL hatten diese noch den DNS-Namen „Ink-gegenstation.rufzeichen“. Im Zuge der IP-Umstellung sollten diese alten DNS-Namen auf den neuen Standard „trx“ anstatt „Ink“ migriert werden.

3.2. To-Do Liste vor der Konfiguration

- Hardware besorgen (Bei Mikrotik Geräten auf Lizenzlevel achten! Geräte für den Benutzereinstieg müssen mindestens Lizenzlevel 4 haben, damit sie den Access Point Modus können. Für Backbone-Links gehen auch Geräte mit Lizenzlevel 3, da hier der Bridge-Modus reicht.)
- Verschaltungsplan erstellen, am besten gleich mit dem „[Diagram Designer](#)“
- IP-Koordinatoren kontaktieren und unter Angabe der Linkpartner Subnetze und eine Knotennummer (AS-Nummer) für das BGP-Routing zuteilen lassen
- IP-Adressen und DNS-Namen für die wichtigsten Geräte in der HamnetDB eintragen bzw. eintragen lassen. Als Sysop sollte man sich bei einem Verantwortlichen einen Schreib-Zugang für die HamnetDB erstellen lassen, um seinen Standort dort selbst verwalten zu können.
- Außerdem sollte man die für die Region passenden DNS und NTP Server erfragen oder ggf. die Informationen im Serviceverzeichnis des Amateurfunk-Wiki nachschlagen:
<http://www.amateurfunk-wiki.de/index.php/Serviceverzeichnis>

3.3. Aufbau des Beispielknotens DB0DAH

Dieser Netzknoten wurde ausgewählt, da er eine sehr überschaubare Konfiguration aufweist ohne irgendwelche Komplikationen, also einem „Standardknoten“ sehr nahekommt.



DB0DAH hat einen zentralen Mikrotik Router (RB 750UP) und drei angeschlossene Außeneinheiten (GrooveA). An ether2 und ether3 sind HF-Links für 5 GHz angeschlossen. Ein HF-UserEinstieg für 2 GHz ist an ether5 angeschlossen.

An ether1 liegt das Servicenetz an. Dort können z.B. Server (RaspberryPi) und andere Geräte angeschlossen werden. Auch könnte man sich hier per LAN-Kabel in das Hamnet einklinken. Sowohl am Serviceanschluss (ether1) als auch am UserEinstieg (ether5) laufen je ein DHCP Server welche dynamische IP-Adressen vergeben.

In der folgenden Grafik sieht man einen Ausschnitt aus der HamnetDB, aus welcher man die zugewiesenen Subnetze für den Knoten ansehen kann.

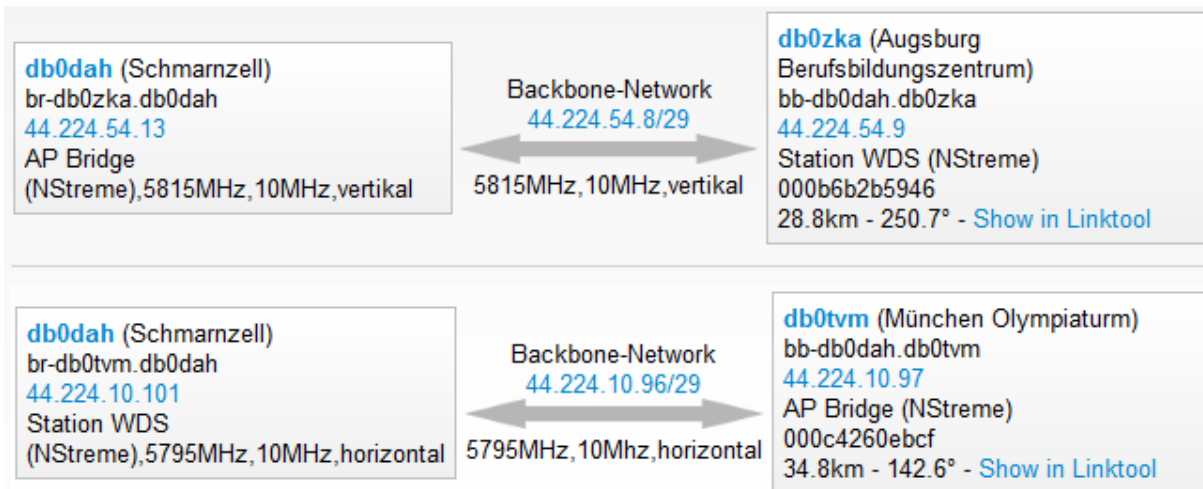
Hinweis: Der Link zu DB0PUC wird in dieser Dokumentation nicht behandelt.

Man sieht in dieser Tabelle auch deutlich die Zweiteilung des Service-Subnetzes.

Surrounding subnets:

Subnet-IP	Type	Own AS	Parent	Radio parameters / Comment
44.224.10.0/23	AS-Backbone	-	AS64625	
44.224.10.96/29	Backbone-Network	-	AS64625	<i>db0tvm,db0dah</i> - 5795MHz, 10MHz, horizontal
44.224.10.136/29	Backbone-Network	-	AS64625	<i>db0dah,db0puc</i> - 5805MHz, 10MHz, horizontal
44.224.54.0/23	AS-Backbone	-	AS64647	
44.224.54.8/29	Backbone-Network	-	AS64647	<i>db0dah,db0zka</i> - 5815MHz, 10MHz, vertikal
44.225.108.0/22	AS-User/Services	-	AS64647	
44.225.108.192/27	Site-Network	AS65533	AS64647	<i>db0dah</i>
44.225.108.192/28	Service-Network	-	AS64647	<i>db0dah</i>
44.225.108.208/28	User-Network	-	AS64647	<i>db0dah</i>

Alle notwendigen Daten für die Links werden nochmals in dieser Übersicht schön dargestellt:



Jeweils in der Mitte sieht man das zugewiesene Subnetz, links und rechts die zugewiesenen IP-Adressen für die Bridges in den Außeneinheiten. Außerdem sieht man wer AP Bridge ist und wer Station ist.

Bei DB0DAH wird der „WDS“ Modus für die Linkstrecken verwendet, dies ist aber nicht zwingend notwendig. Man kann auch als normal „station pseudobridge“, also ohne WDS Modus arbeiten.

Als Ergänzung findet man meist noch Informationen zur Linkfrequenz, der Bandbreite und der Antennenpolarisation.

Wenn beide Linkpartner nur über Level3 Lizenzen verfügen, steht der Modus „AP Bridge“ nicht zur Verfügung. Man kann daher alternativ die Modi „Bridge“ und „Station Bridge“ verwenden. Der Linkpartner mit dem „Bridge“-Modus, entspricht dem „Access Point“, welcher seine SSID aussendet. „Station Bridge“ ist der Client, der den anderen Linkpartner „connected“. Eine Station im „Bridge-Modus“ kann im Gegenteil zum „AP-Modus“ nur von **einer** Station connected werden.

4. Konfiguration der Linkstrecke zu DBOZKA

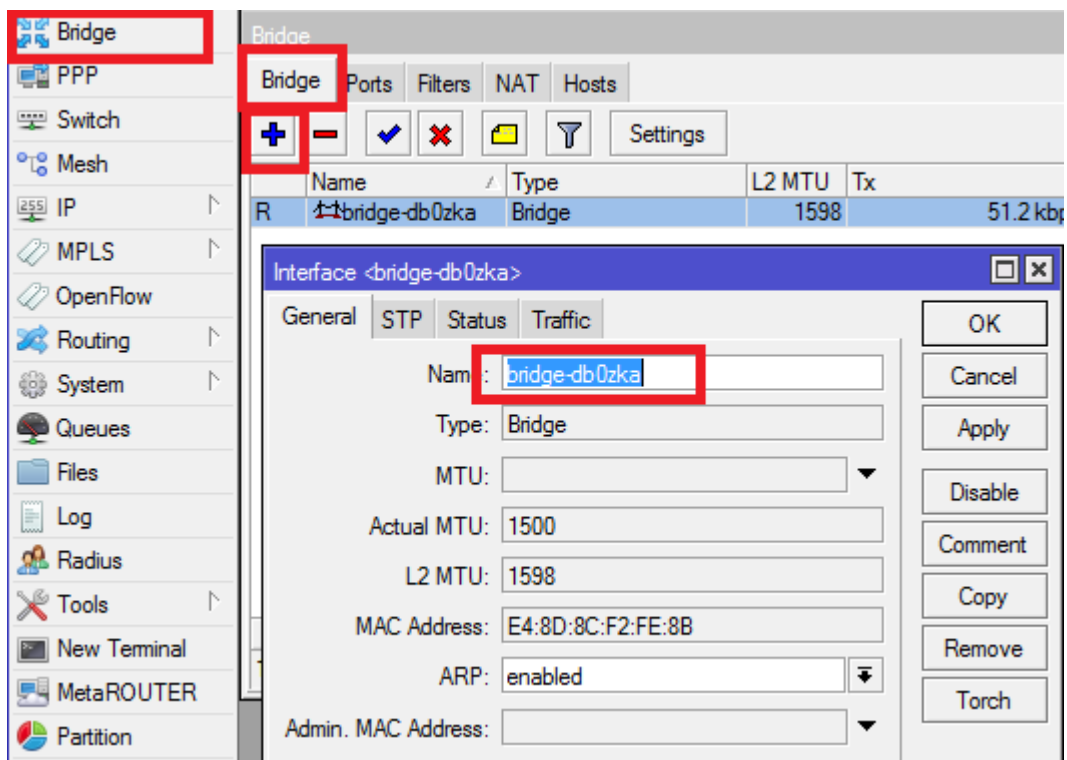
Kurzübersicht der Einstellungen einer Antenne bzw. Außeneinheit:

- Eine Bridge zwischen LAN und WLAN-Schnittstelle erstellen
- Der Bridge eine IP-Adresse zuweisen
- Default-Route eintragen
- DNS-Server eintragen
- (S)NTP-Server eintragen (Zeitsynchronisation)
- System-Identity (idealerweise den eigenen DNS-Namen) eintragen
- User-Passwort setzen (ggf. weitere User hinzufügen)
- Wireless-Parameter festlegen

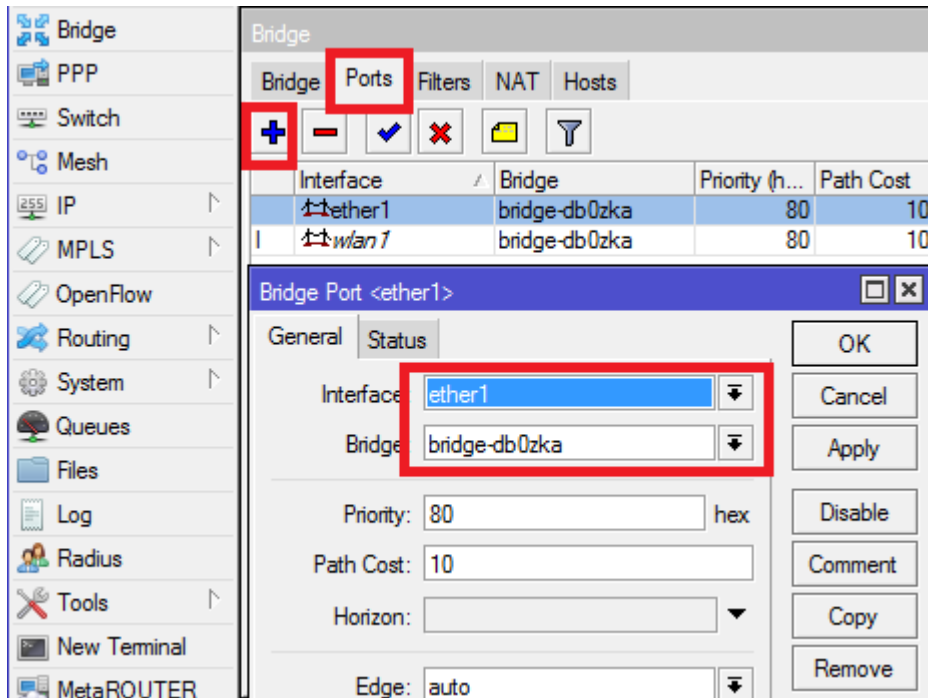
4.1. Einrichten der IP-Parameter in der Außeneinheit

- a) Damit die eingehenden Pakete 1:1 zum zentralen Router durchgeleitet werden können, erstellen wir eine Bridge zwischen LAN und WLAN-Interface.

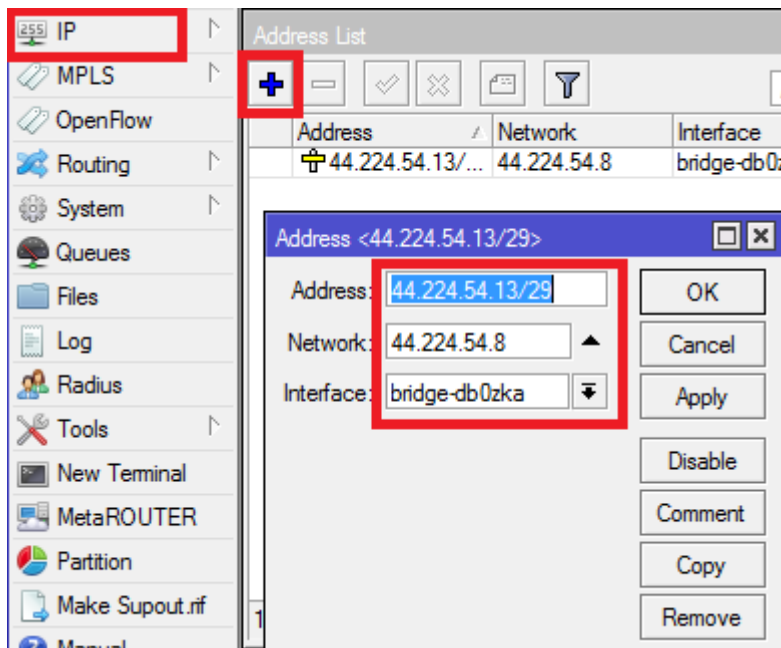
BRIDGE > BRIDGE



- b) Wurde die Bridge erstellt, müssen wir das LAN und WLAN-Interface der Bridge hinzufügen
BRIDGE > PORTS



- c) Wir teilen der bridge eine IP-Adresse zu
IP > ADDRESSES

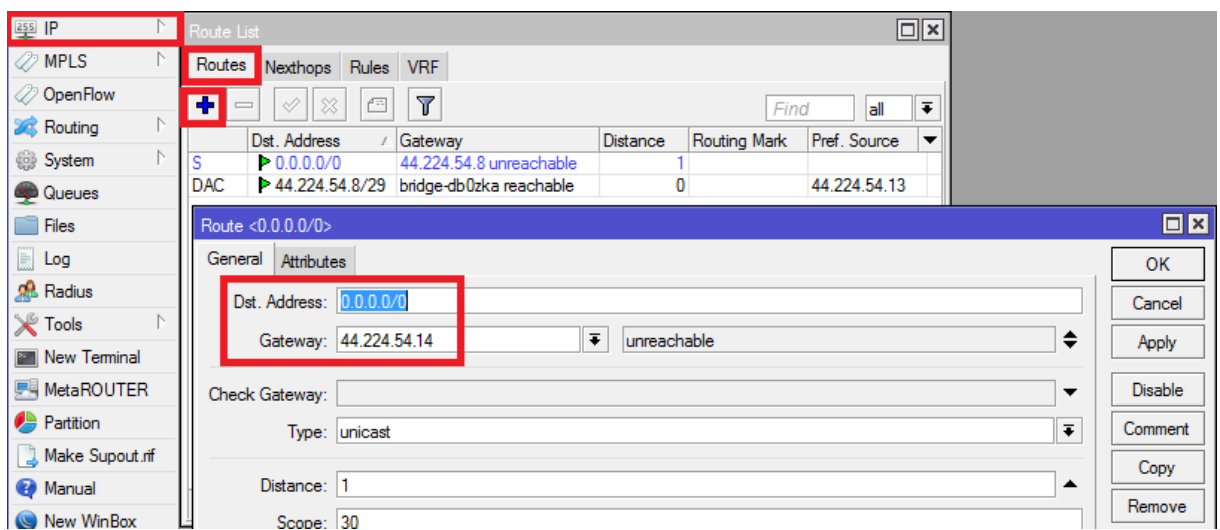


Die Bridge erhält eine IP-Adresse aus dem für diesen Link zugewiesenen Subnetz. In der Regel steht ein /29 Netz mit 8 Adressen (davon 6 nutzbar) pro Link zur Verfügung. Die erste und die letzte Adresse aus diesem Subnetz sind nicht nutzbar, da es sich um die „Network“ bzw. „Broadcast“ Adresse handelt. Die zweite und dritte IP-Adresse gehört dem einen Linkpartner, die sechste und siebte Adresse dem anderen Linkpartner. Die zweite bzw. siebte Adresse des Subnetzes erhält für gewöhnlich der Port im zentralen Router, an welchem die Außeneinheit angeschlossen ist. Die Außeneinheit selbst (bzw. die Bridge) erhält dann die dritte bzw. sechste Adresse aus dem Subnetz. In unserem Fall haben wir die hinteren Adressen, und vergeben daher der Bridge die sechste Adresse aus dem Subnetz.

d) Die Eingabe einer Default Route ist nötig, damit man mit der Außeneinheit problemlos kommunizieren kann, denn sonst werden Pakete (z.B. Ping) nicht korrekt beantwortet. Die Default Route ist die IP des zentralen Routers in dem jeweiligen Routingnetz. Man hinterlegt sie unter **IP > ROUTES**

- Destination Address = 0.0.0.0/0
- Gateway = 44.224.54.14 (IP des zentralen Routers)

(warum in der Übersicht von DB0DAH die Default Route 44.224.54.8 lautet, und nicht 44.224.54.14, lässt sich nicht genau nachvollziehen. 54.8 wäre ja auch die Netzwerkadresse des Transfernetzes, und nicht die des Routers. Vermutlich handelt es sich hier um einen Tippfehler, im folgenden Screenshot steht es korrekt!)

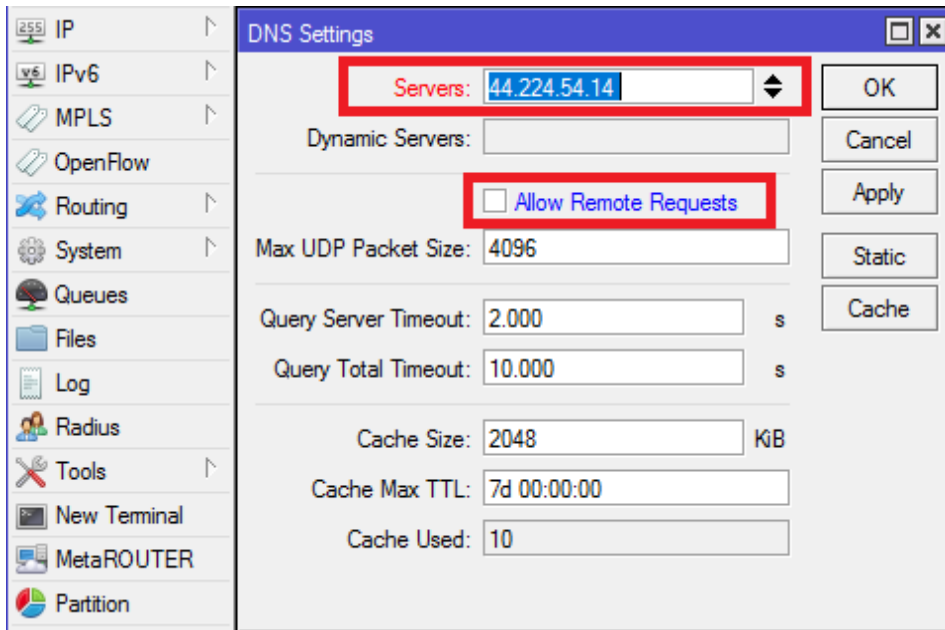


e) DNS-Server eintragen

Damit die Namensauflösung funktioniert, wird der Hauptrouter als DNS-Server hinterlegt.

Achtung! Hier muss die IP-Adresse aus dem Routing-Subnetz genommen werden, da dieses Routerboard nicht mit Routinginformationen versorgt wird.

IP > DNS

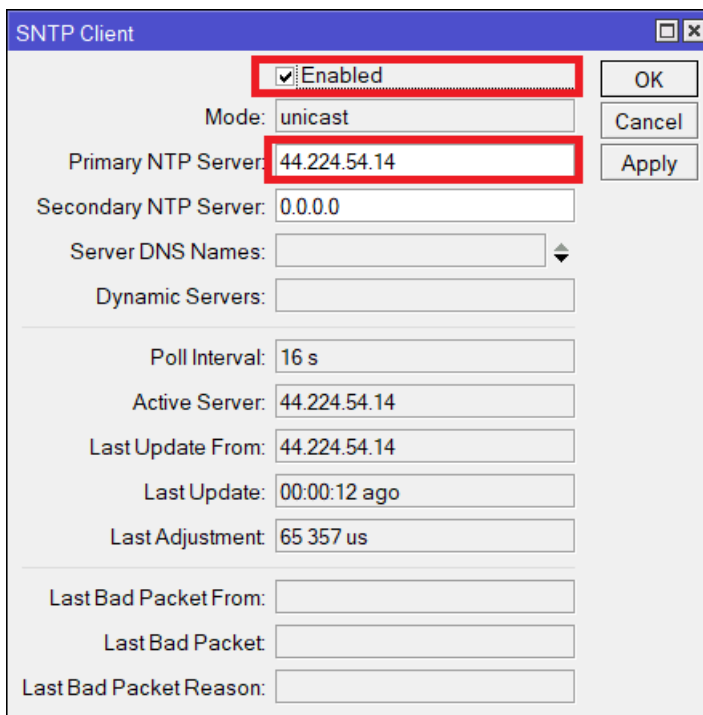


Der Haken bei „Allow Remote Requests“ braucht nicht gesetzt zu werden, da der Router nicht selbst als DNS Server dient.

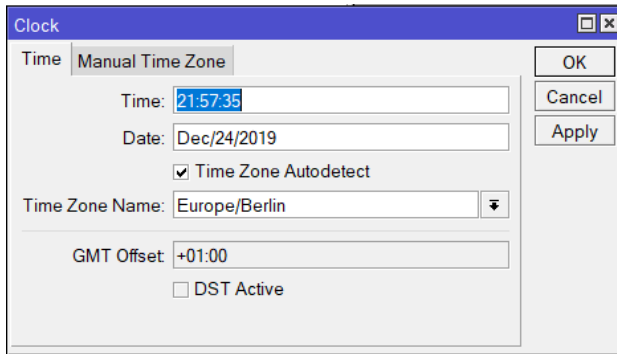
f) NTP Client einrichten

Damit Zeitangaben in den Logs auch nachvollziehbar werden, sollte hier der Hauptrouter als NTP Zeitserver eingetragen werden.

SYSTEM > SNTP Client



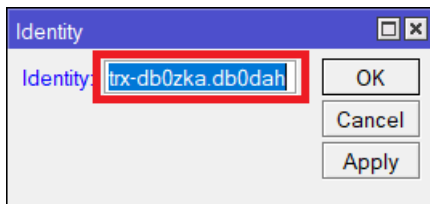
Unter SYSTEM > CLOCK kontrolliert man dann noch die synchronisierte Zeit und die Zeitzone. In der Regel lässt man die Zeitzone auf „Autodetect“ und korrigiert nur bei Bedarf.



Ist das Paket „ntp.npk“ installiert, sind die Einstellungen unter SYSTEM > NTP Client zu finden.

g) Identität eintragen

Unter SYSTEM > IDENTITY trägt man noch den DNS-Namen des Gerätes zur Identifikation ein. Der erscheint z.B. auch bei einem selbst und bei der Gegenstation unter „IP > NEIGHBOURS“



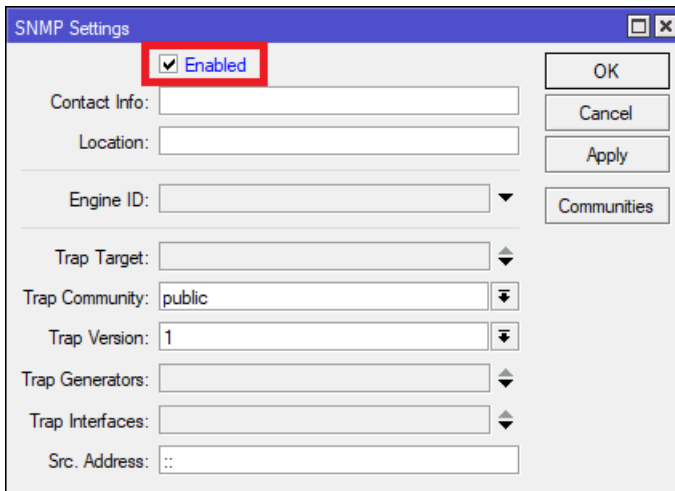
h) Sysop Passwort setzen und ggf. weitere User hinterlegen

- Unter SYSTEM > PASSWORD setzt man das Passwort für den aktuellen User (in der Regel „admin“).
- Unter SYSTEM > USERS kann man weitere User anlegen und verwalten, die auf das Gerät zugreifen dürfen.

i) RSSI Monitoring aktivieren

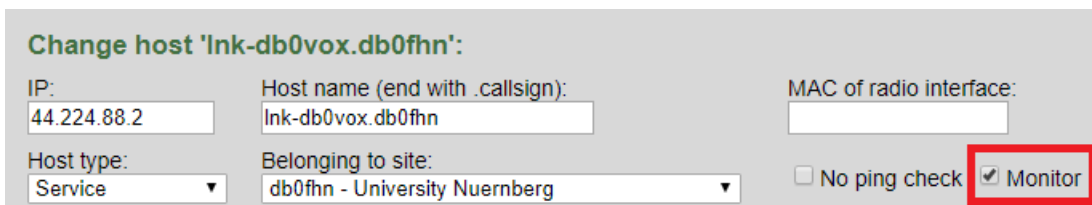
Seit 2019 enthält die HamnetDB ein Monitoring Tool für die Routingnetze. Dies liest die Feldstärken der Link-Verbindungen aus und stellt diese grafisch und textbasiert in der HamnetDB dar. Dies ist auch hilfreich, um Kontrolle über die Linkqualitäten zu bekommen.

Dazu muss SNMP im Linkdevice (Antenne) aktiviert werden. Bei Mikrotik findet man den Punkt unter IP > SNMP:



The image shows a 'SNMP Settings' dialog box. At the top, there is a checkbox labeled 'Enabled' which is checked and highlighted with a red box. Below this are several input fields: 'Contact Info:', 'Location:', 'Engine ID:' (with a dropdown arrow), 'Trap Target:' (with a dropdown arrow), 'Trap Community:' (containing 'public'), 'Trap Version:' (containing '1'), 'Trap Generators:', 'Trap Interfaces:', and 'Src. Address:' (containing '::'). On the right side of the dialog, there are buttons for 'OK', 'Cancel', 'Apply', and 'Communities'.

Bitte auch daran denken, das Monitoring-Flag für dieses Gerät in der HamnetDB zu setzen:

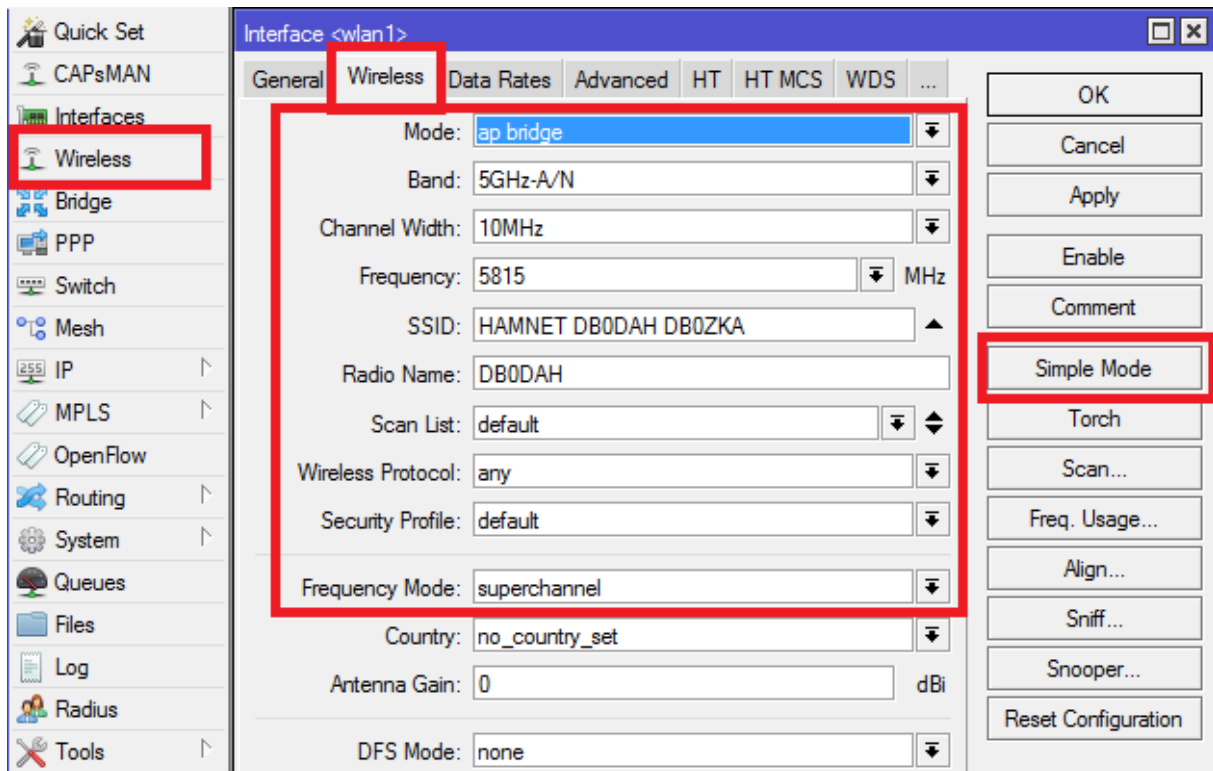


The image shows a 'Change host' configuration form for the host 'lnk-db0vox.db0fhn'. It contains several fields: 'IP:' (44.224.88.2), 'Host name (end with .callsign):' (lnk-db0vox.db0fhn), 'MAC of radio interface:' (empty), 'Host type:' (Service), 'Belonging to site:' (db0fhn - University Nuernberg), 'No ping check' (unchecked), and 'Monitor' (checked and highlighted with a red box).

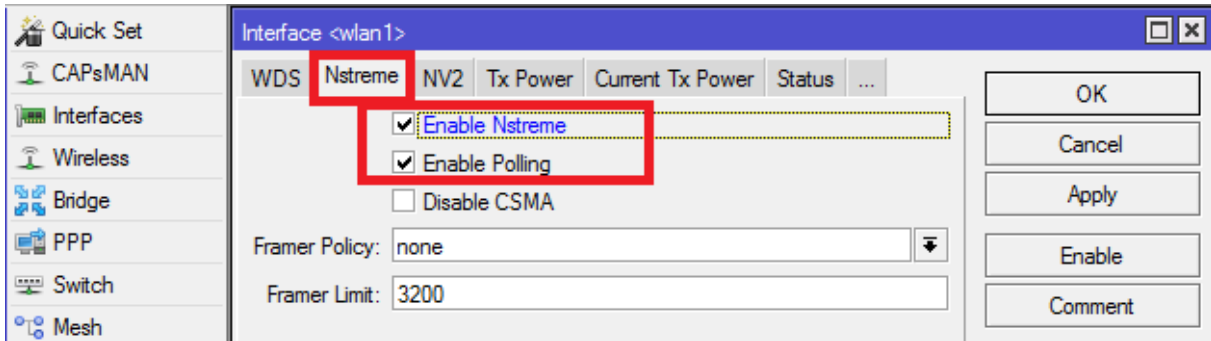
Es gibt Sonderfälle, die einer gesonderten Betrachtung notwendig sind. Beispielsweise bei Point-to-Multi-Point Links, oder wenn es gar keine Außeneinheit gibt, weil das WLAN direkt am Hauptrouter angeschlossen ist (z.B. RB433AH). Dies wird in einem separaten Kapitel behandelt (Siehe Kapitel 15).

4.2. Einrichten der HF-Parameter für die WLAN Verbindung

WIRELESS > Doppelklick auf das WLAN Interface



- a) Aktivieren des „**Advanced Mode**“, damit alle Parameter sichtbar werden.
- b) Unter „**Frequency Mode**“ den „superchannel“ auswählen und gleich auf „Apply“ klicken, damit der Modus sofort aktiv wird. Erst jetzt ist die erweiterte Frequenzauswahl möglich, um Frequenzen außerhalb der genormten WLAN-Kanäle auswählen zu können.
- c) **Mode**: Ein Linkpartner ist der Accesspoint, also „AP Bridge“. Der andere ist der Client, also „Station Pseudobridge“. In unserem Beispiel sind wir die „AP Bridge“. (Alternativ auch „Bridge“ und „Station Bridge“).
- d) **Band**: i.d.R. 5 GHz. Die WLAN Modi (A, N) müssen auf beiden Seiten übereinstimmen.
- e) **Channel Width**: 10 MHz (Standard für Links in Deutschland)
- f) **Frequency**: Zugewiesene Linkfrequenz (5815 MHz)
- g) **SSID**: HAMNET CALL(AP) CALL(station) => HAMNET DB0DAH DBOZKA
- h) **Radio Name**: Das eigene Relais-Rufzeichen
- i) **Security Profile**: „default“. Hier könnte man ein Profil mit Verschlüsselungsparametern auswählen. Da im HAMNET aber nicht verschlüsselt werden darf, bleibt der „default“ Eintrag stehen. Will man einen Link unter ISM-Bedingungen aufbauen, kann man Sicherheitsprofile in der Wireless-Übersicht im Reiter „Security Profiles“ anlegen und dann in Wireless-Konfiguration auswählen.
- j) „**Nstreme**“ sollte auf beiden Seiten aktiviert werden, dies verbessert den Datendurchsatz. Achtung, „nstreme“ ist ein Mikrotik eigenes Protokoll und nicht mit Geräten anderer Hersteller kompatibel!



- k) Mit manchen Mikrotik-Routern lässt sich in MIMO funken, also vertikal und horizontal gleichzeitig. Dies verdoppelt nochmal den Datendurchsatz. Selbstverständlich müssen dies beide Linkpartner unterstützen. Eingestellt wird dies im Reiter „HT“ bei den „chains“. Chain 0 ist die eine Polarisierung, chain 1 die andere. Unterstützt ein Routerboard dies nicht, erscheint nur die chain 0. Damit auf beiden Ebenen gefunkt wird, müssen alle vier Haken gesetzt werden. Bei manchen Routerboards (z.B. RB433AH) ist allerdings ein Reboot notwendig, damit diese Einstellung aktiv übernommen wird. Für unser Beispiel ist dies nicht relevant, da wir darüber keine Informationen haben. **Wichtig:** Wenn ein Dual-Polarity Router mit nur einer Polarisierung betrieben werden soll, weil z.B. die Gegenstation nur eine Polarisierung unterstützt. Müssen trotzdem beide RX chains aktiviert sein, um einwandfreie Funktion zu gewährleisten. Nur ein Haken bei der TX Chain kann dann entfallen.
- l) **Country:** Seit Version 6.47 von RouterOS muss bei neu eingerichteten Antennen das Land „Debug“ angegeben werden, da sonst keine nicht konformen WLAN Frequenzen genommen werden können (also keine Amateurfunk Frequenzen nutzbar).

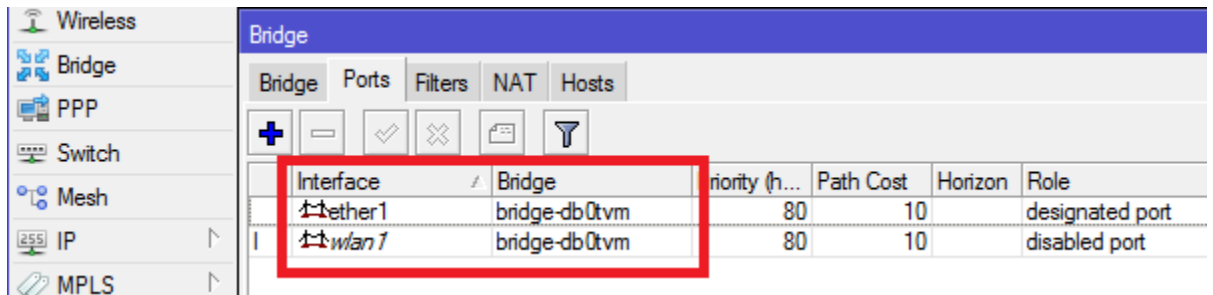


- m) Wird das WLAN-Interface nun im Wireless-Hauptmenü aktiv geschaltet, ist der Access Point bereit und kann connected werden. Im Status „disabled“ sendet der Transceiver nicht, sondern empfängt nur. Im Wireless-Hauptmenü kann man nun unter „Registration“ sehen, wenn sich eine Station eingeloggt hat.

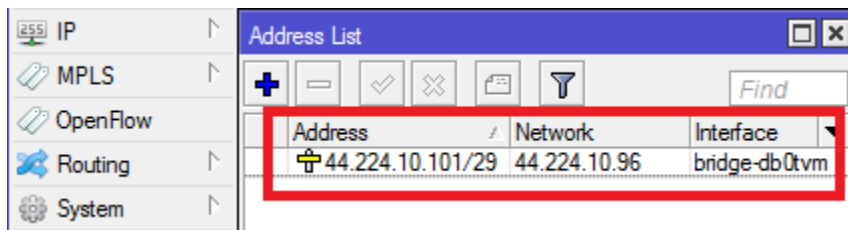
5. Konfiguration der Linkstrecke zu DBOTVM

5.1 Einrichten der IP-Parameter in der Außeneinheit (analog zum DBOZKA Link)

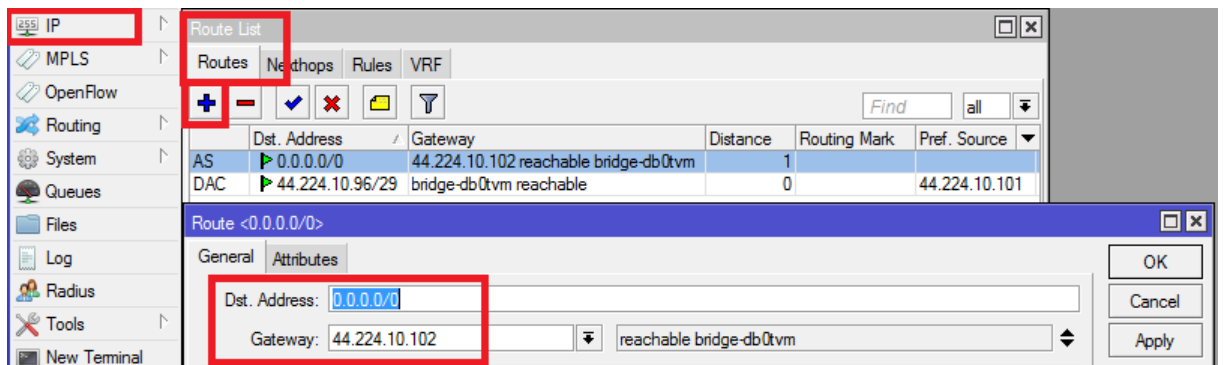
- a) Erstellen der Bridge, hinzufügen der Ports



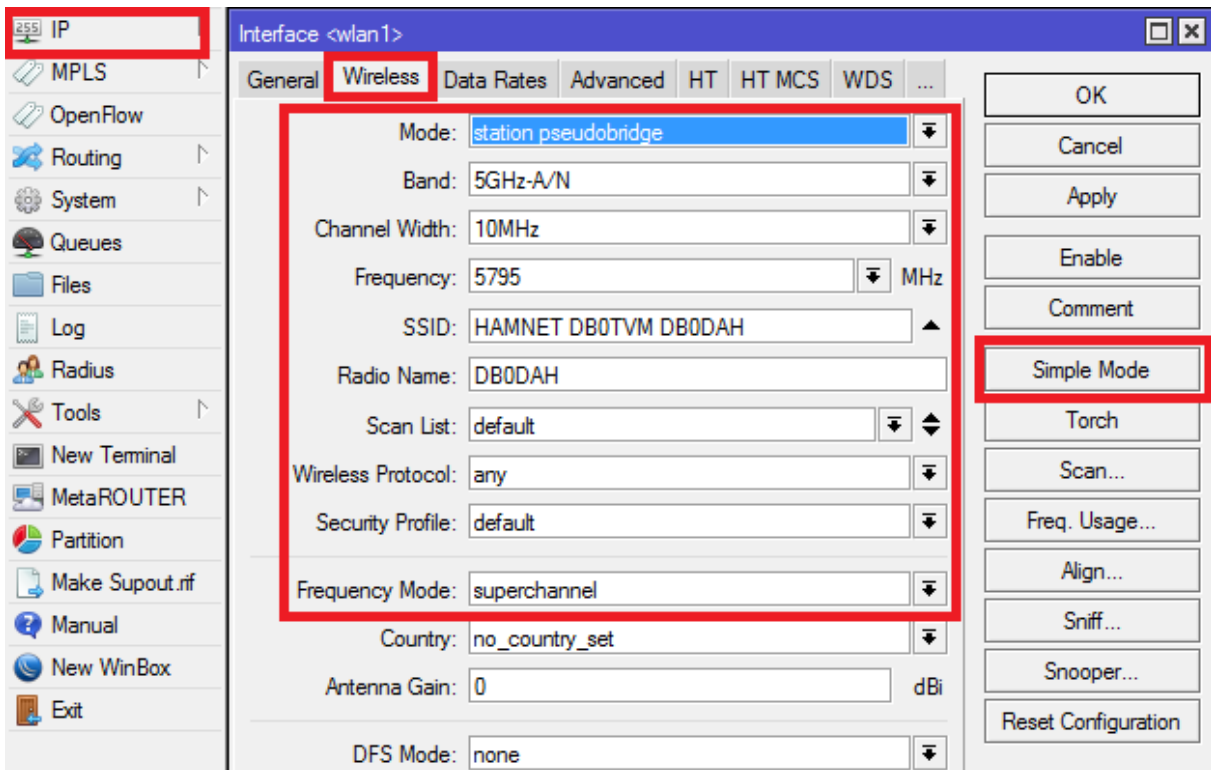
- b) Hinzufügen der IP-Adresse für die Bridge



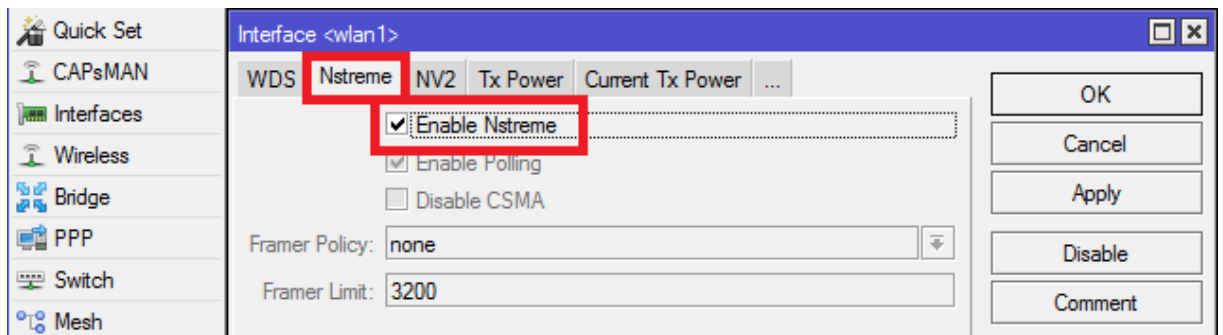
- c) Hinterlegen der Default Route



5.2. Einrichten der HF-Parameter für die WLAN-Verbindung



1. Konfiguration der HF Parameter unter Wireless analog zum Link zu DB0ZKA. Der einzige Unterschied ist der Mode „station pseudobridge“, da wir hier der Client sind, DB0TVM ist der Access Point.
2. Nstreme wird auch noch aktiviert.



3. Wird das WLAN-Interface nun im Wireless-Hauptmenü aktiv geschaltet, versucht sich das Board nun automatisch mit dem Linkpartner zu verbinden. Unter „Status“ könnt ihr den Linkstatus sehen, unter „Traffic“ den aktuellen Datendurchsatz.

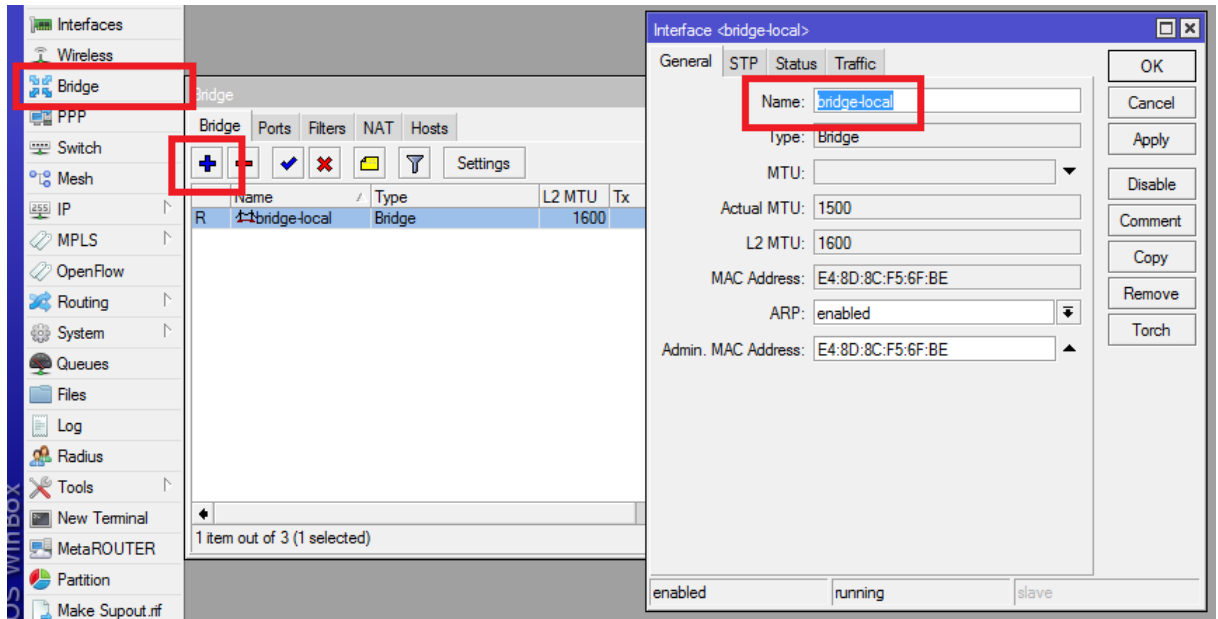
5.3. Weitere Parameter

Auch in dieser Linkeinheit sollten noch der DNS-Server, der NTP Server, die Identity und das Sysop-Passwort eingetragen werden, analog zum Link zu DB0ZKA. Screenshots sind hier verzichtbar.

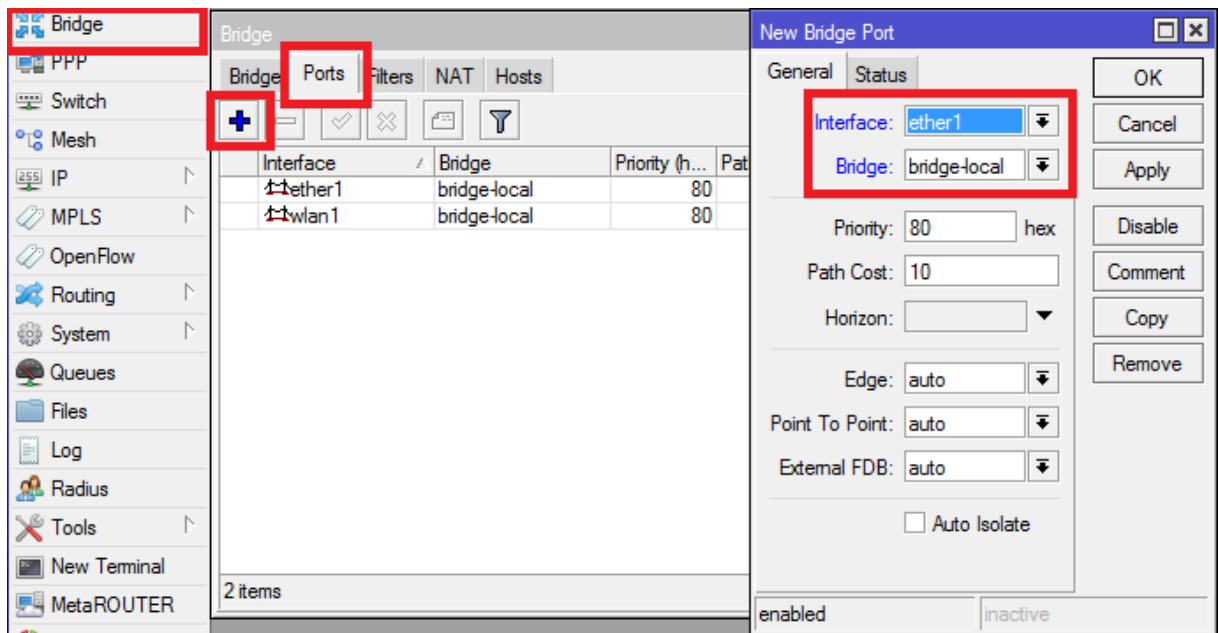
6. Konfiguration UserEinstieg

6.1. Konfiguration der Bridge

1. Auch hier erstellen wir zunächst eine bridge zwischen LAN und WLAN-Interface

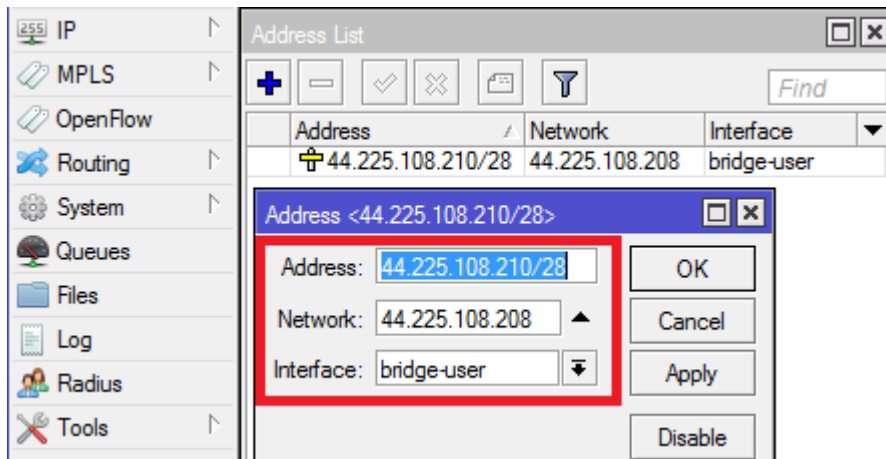


2. Hinzufügen der beiden Ports zu der bridge



3. Vergeben einer IP-Adresse für die Bridge

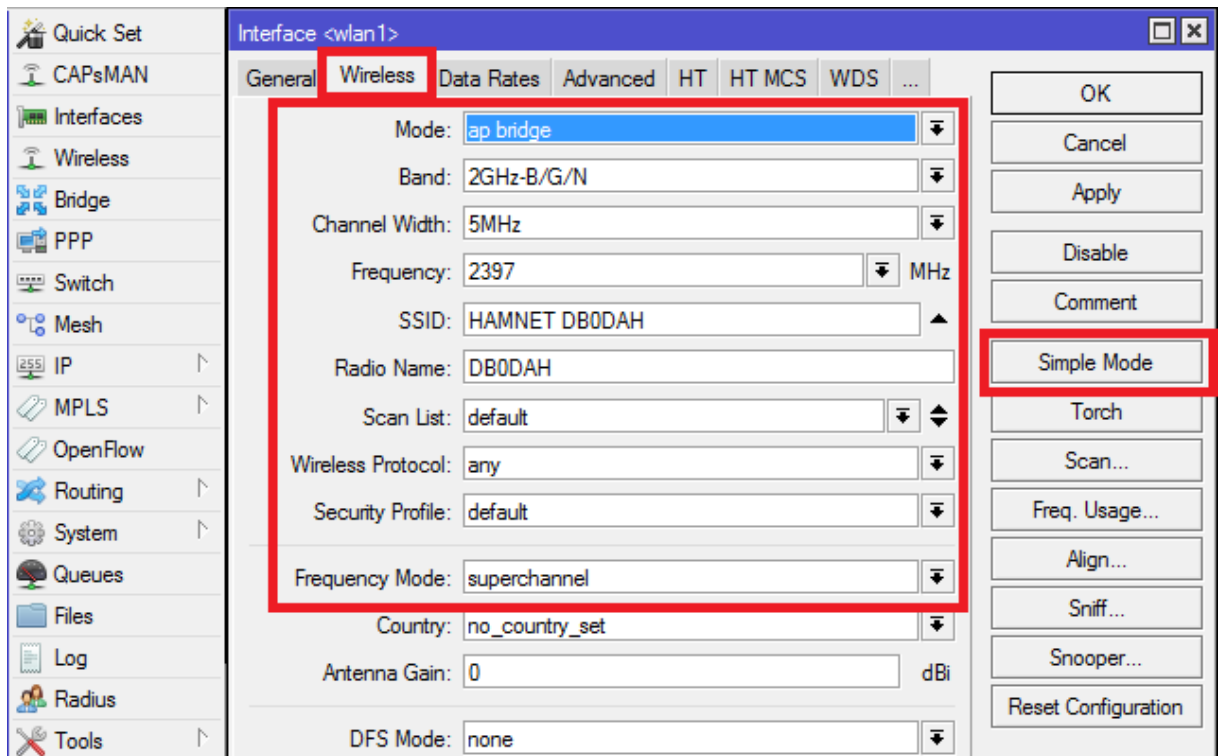
IP > ADDRESSES



Die Bridge des UserEinstieg erhält eine IP-Adresse aus dem User-Netz, dafür ist der Bereich ab 44.225.108.209 vorgesehen. Genau wie bei den Links erhält die erste nutzbare IP-Adresse der Port am zentralen Router, die Bridge in der Außeneinheit dann die zweite. In unserem Fall ist dies die 44.225.108.210.

4. Wie bei den Antennen sollten hier auch noch die Parameter DNS-Server, NTP-Server, Identity, Sysop Passwort hinterlegt und SNMP für das RSSI-Monitoring aktiviert werden.

6.2. Konfiguration der HF-Parameter
WIRELESS > Doppelklick auf das WLAN-Interface



1. Aktivieren des „**Advanced Mode**“
2. **Mode:** „ap bridge“.
3. Unter „**Frequency Mode**“ den „superchannel“ auswählen, und auf „Apply“ drücken, damit es wirksam wird.
4. **Band:** Wunschband, z.B. 5 GHz oder 2 GHz (WLAN Modi beachten)
5. **Channel Width:** 10 MHz auf 5 GHz oder 5 MHz auf 2 GHz (max. erlaubte Bandbreite in DL)
6. **Frequency:** Zugewiesene Userfrequenz, z.B. 2392 MHz, 2397 MHz etc.
7. **SSID:** HAMNET + das eigene Relais-Rufzeichen (dies ist regional unterschiedlich, manchmal wird hier auch das eigene Rufzeichen weggelassen und nur unter „HAMNET“ gesendet).
8. **Radio Name:** Das eigene Relais-Rufzeichen
9. **Security Profile:** „default“. Hier darf nichts eingerichtet werden da HAMNET nicht verschlüsselt werden darf (es sei denn, man arbeitet unter ISM Bedingungen).
10. **Country:** Auf „Debug“ stellen um Amateurfunkfrequenzen auswählen zu können
11. Hat man einen MIMO Userzugang, kann man noch die chains konfigurieren



7. Unterschiede beim Einsatz von Routern mit integrierten WLAN-Modulen

Es gibt auch Mikrotik Router welche als vollwertiger Hamnet-Knoten verwendet werden können, da sie bereits WLAN-Transceiver eingebaut haben bzw. diese aufgesteckt werden können (z.B. RB433AH). Dies hat diverse Vor- und Nachteile:

Vorteile:

- Einfache Konfiguration, da nur ein Router im Einsatz.
- Es sind beliebige Antennen einsetzbar. Der Anschluss erfolgt i.d.R. über N oder RP-SMA Anschlüsse

Nachteile:

- Der Router muss in einem wetterfesten Gehäuse in der Nähe der Antennen angebracht werden. Es gibt aber auch Gehäuse mit bereits integrierten Antennen.
- Die Antennenkabel können je nach Länge sehr verlustreich sein. Eine Kabellänge von über einem Meter sollte vermieden werden.
- Gute Koaxialkabel und HF-Steckverbinder sind teurer als LAN-Kabel.

Abweichungen zum Vorgehen mit separater Außeneinheit:

- Keine separate Außeneinheit zu konfigurieren
- Ein Link bzw. ein Einstieg benötigt nur eine IP-Adresse, da die Bridge entfällt.
- Die IP-Adresse wird direkt dem WLAN-Interface im Router zugewiesen.
- Die HF-Parameter werden dann auch direkt im „zentralen“ Router eingestellt.

8. Konfiguration einer Ubiquity Außeneinheit

Als zentraler Router muss immer ein Router eingesetzt werden, welcher das BGP Routingprotokoll unterstützt (i.d.R. Mikrotik). Die HF-Einheiten müssen kein BGP unterstützen, da sie die WLAN-Signale nur auf das LAN umsetzen und an den zentralen Router weiterleiten. Deswegen nimmt man hier gerne auch Geräte vom Hersteller UBIQUITY. Diese sind recht einfach zu konfigurieren. Da sie aber von Haus aus erst mal keine Amateurfunkfrequenzen unterstützen, ist ein Eingriff notwendig.

Kompatible Geräte (Beispiele):

- Nanostation M2/M3/M5
- Nanostation M2/M5 Loco
- Nanobeam M2/M5
- Powerbeam M2/M5
- Airgrid M2/M5

WLAN „AC“ Geräte von Ubiquity sind nur eingeschränkt nutzbar. Zwar ist es mit einigen Geräten möglich auch 10 und 5 MHz Bandbreite sowie AFU Frequenzen zu nutzen, allerdings verhalten sich diese Geräte anders. Wenn, dann sollten beide Linkpartner Ubiquity AC Geräte nutzen. Eine Mischung verursacht erfahrungsgemäß Probleme (Stand 09/2017).

Vorbereitungen:

- a) Router Reset

Auch hier sollte man bei null beginnen. Wenn man den Reset-Taster 10 Sekunden lang gedrückt hält (alle Lämpchen blinken kurz auf), wird alles auf Werkzustand zurückgesetzt.

- b) Compliance Test aktivieren

Wenn man auf seinem Ubiquity Gerät einen Softwarestand von 5.5.6 oder höher hat, ist der für den Amateurfunk wichtige „Compliance Test“ Modus nicht auswählbar. Dieser sorgt dafür, dass man das Gerät auch auf Amateurfunkfrequenzen programmieren kann. Wie man den „Compliance Test“ Modus aktiviert, ist aus rechtlichen Gründen nicht öffentlich. In Deutschland erhält man diese Information von Andreas Kleiner DG4OAE. Sendet ihm eine E-Mail unter SEIN-RUFZEICHEN @gmx.de, und folgt seinen Anweisungen.

- c) Erster Login

Verbindet euch mit der Weboberfläche des Routers und beachtet dabei die IP-Einstellungen. Das Mustergerät, eine Nanostation M2, war standardmäßig auf 192.168.1.20 eingestellt. Man gibt dem eigenen LAN-Interface im Computer z.B. die 192.168.1.21 und die Netzmaske 255.255.255.0. Wenn man nun im Browser die IP-Adresse des Ubiquity-Gerätes eingibt, erscheint in der Regel erst einmal ein Warnhinweis. Da standardmäßig das Webinterface über HTTPS abgefragt wird und die Rechner das SSL Zertifikat nicht anerkennen, muss erst einmal die Erlaubnis erteilt werden die Seite anzuzeigen. Wurde die Erlaubnis erteilt, erscheint die Anmeldemaske.



The screenshot shows the airOS login interface. On the left is the airOS logo. On the right, there are four input fields: Username (empty), Password (empty), Country (dropdown menu with 'Select Your Country' selected), and Language (dropdown menu with 'English' selected).

In der Länderauswahl (Country) muss man nun unbedingt den „Compliance Test“ Modus auswählen. **Achtung:** Diese erste Länderauswahl ist nachträglich erst einmal nicht mehr zu ändern. Wenn man hier das falsche Land auswählt, muss man erst den kompletten Router zurücksetzen und beginnt anschließend wieder von vorne. Als Sprache wählt man Deutsch aus. Die Zugangsdaten lauten i.d.R. von Haus aus „ubnt“ für Benutzername und Passwort.



The screenshot shows the airOS login interface with the following values: Username: ubnt, Password: masked with dots, Country: Compliance Test, and Language: Deutsch. A red rectangular box highlights the entire input area.

d) Admin-Zugang absichern

Als erstes sollte man im Reiter SYSTEM unter BENUTZERKONTEN den Admin-Zugang ändern. Hierzu einfach auf die Lupe klicken, einen Neuen Usernamen vergeben, das alte Kennwort (ubnt) sowie zweimal das neue Kennwort eingeben, und die Einstellungen übernehmen. Nach jeder Änderung fragt die Software ob man die geänderten Einstellungen erst einmal testen oder gleich anwenden will.



The screenshot shows a blue confirmation dialog box with the text: "Die Konfiguration wurde geändert. Möchten Sie sie speichern?". There are three buttons: "Test", "Anwenden" (highlighted with a red box), and "Verwerfen".

Nach dem Klick auf „Anwenden“ werden die Einstellungen übernommen. Sicherheitshalber sollte man nun den Router neu starten und sich mit den neuen Zugangsdaten einloggen. Meistens tut er dies aber auch schon automatisch.

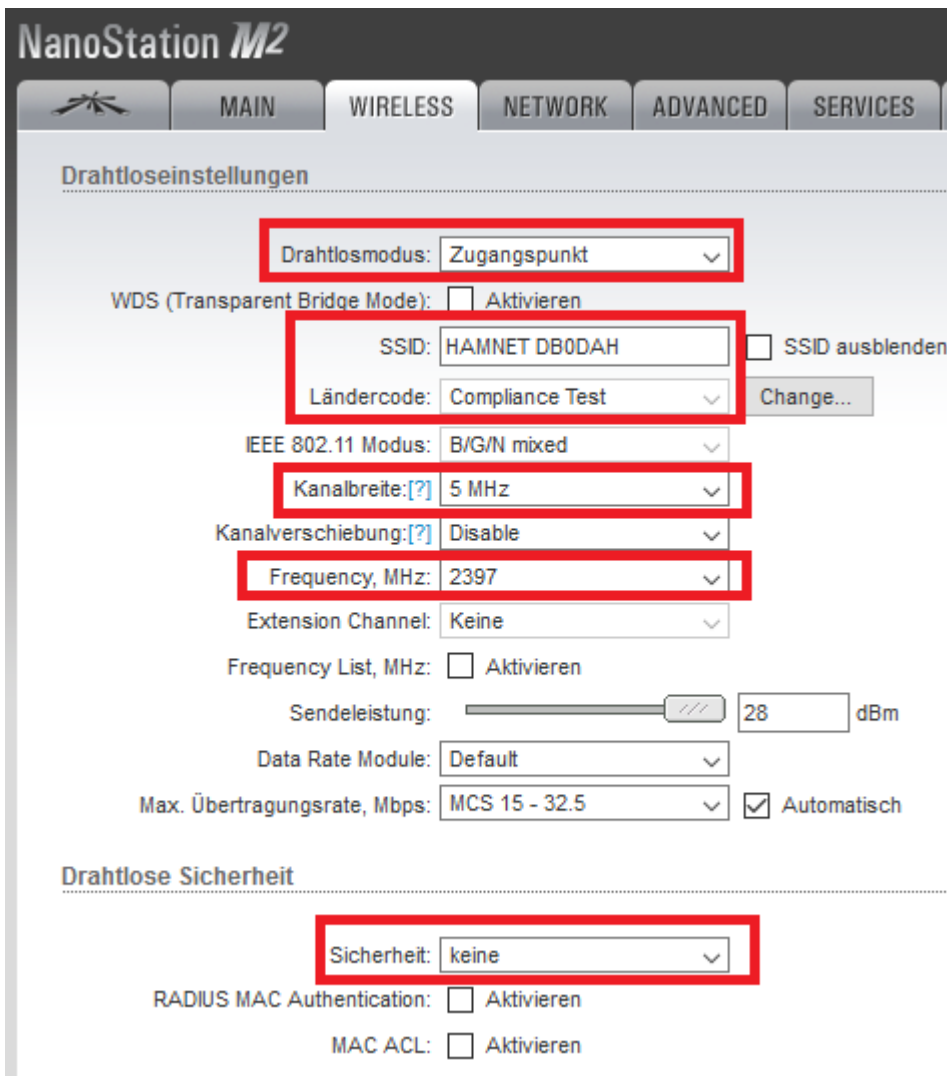
e) AirMax deaktivieren (bei Userestiegen)

Als erstes sollte der AirMax Modus deaktiviert werden. Dies ist ein Ubiquity eigenes Protokoll und funktioniert nur, wenn auf der Gegenseite auch Ubiquity Hardware verwendet wird. Bei Linkstrecken sollte AirMax aber aktiviert bleiben, sofern beide Linkpartner Ubiquity Hardware einsetzen.



f) WIRELESS Einstellungen

Im Reiter WIRELESS müssen die WLAN Parameter gesetzt werden.



- Der Drahtlosmodus wird auf „Zugangspunkt“ bzw. „Station“ gestellt, je nachdem ob man Access Point oder Client ist.
- Die SSID lautet HAMNET + ggf. das Relaisrufzeichen bei UserEinstiegen. Bei Links entsprechend HAMNET CALL-AP CALL-STATION

- Als Ländercode ist der Compliance Test vorausgewählt, das soll auch so bleiben.
- Kanalbreite auf 5 MHz (bei 2 GHz) bzw. 10 MHz (bei 5 GHz)
- Frequenz je nach Genehmigung auswählen
- Unter Sicherheit darf nichts ausgewählt sein, Amateurfunk ist unverschlüsselt.

Diese Einstellungen werden jetzt ebenfalls übernommen und angewendet.

g) NETWORK Einstellungen

Im Reiter NETWORK werden der Netzwerkmodus und die IP-Einstellungen festgelegt.

The screenshot shows the 'NETWORK' tab of the NanoStation M2 configuration interface. It is divided into three sections: 'Netzwerk Funktion', 'Configuration Mode', and 'Management Network Settings'. In the 'Netzwerk Funktion' section, 'Netzwerkmodus' is set to 'Bridge' and 'Netzwerk deaktivieren' is set to 'None'. In the 'Configuration Mode' section, 'Configuration Mode' is set to 'Simple'. In the 'Management Network Settings' section, 'Management IP Address' is set to 'Statisch' (Static), and the IP address is '44.225.108.210'. The subnet mask is '255.255.255.240' and the gateway IP is '44.225.108.209'. Other options like 'Primäre DNS IP', 'Sekundäre DNS IP', 'MTU', 'Management VLAN', 'Auto IP Aliasing', and 'STP' are all set to their default or disabled states.

- Der Netzwerkmodus wird auf „Bridge“ gestellt.
- Die IP-Adresse wird auf statisch gestellt und in das Feld darunter unten eingegeben.
- Die Netzmaske lautet 255.255.255.240 bei einem /29er Netz.
- Die Gateway-IP entspricht der Default Route.

Diese Einstellungen werden nun übernommen und angewendet.

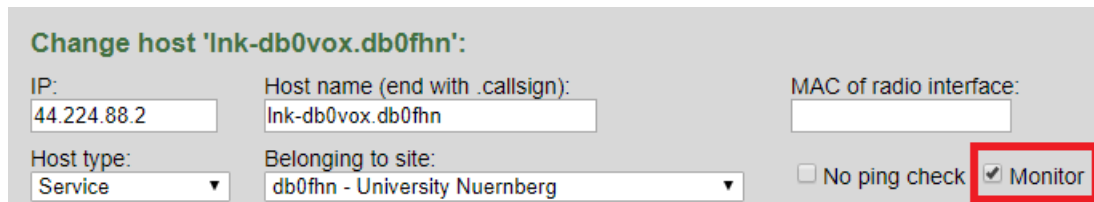
Hier fliegt man unweigerlich aus der Oberfläche heraus, da sich die IP-Adresse geändert hat. Man kann nun den Ubiquity-Router an den vorgesehenen Port am Mikrotik-Router anschließen und hochfahren lassen. Über das HAMNET bzw. den Service-Zugang am Mikrotik Router kann man die Oberfläche nun mit der neuen IP-Adresse erreichen.

h) RSSI-Monitoring aktivieren

Wird das Ubiquity-Gerät für eine Linkstrecke verwendet, sollte man hier ebenfalls SNMP aktivieren, um das RSSI-Monitoring für die HamnetDB zu aktivieren: Dies geschieht im Menüpunkt „Services“:



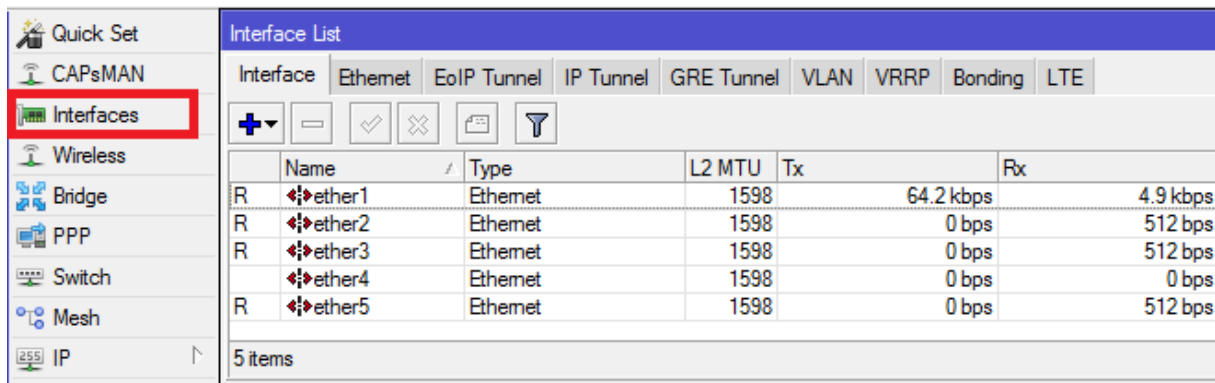
Bitte auch daran denken, das Monitoring-Flag für dieses Gerät in der HamnetDB zu setzen:



Es gibt Sonderfälle, die einer gesonderten Betrachtung notwendig sind. Beispielsweise bei Point-to-Multi-Point Links, oder wenn es gar keine Außeneinheit gibt, weil das WLAN direkt am Hauptrouter angeschlossen ist (z.B. RB433AH). Dies wird in einem separaten Kapitel behandelt (Siehe Kapitel 15).

9. Konfiguration des zentralen Routers

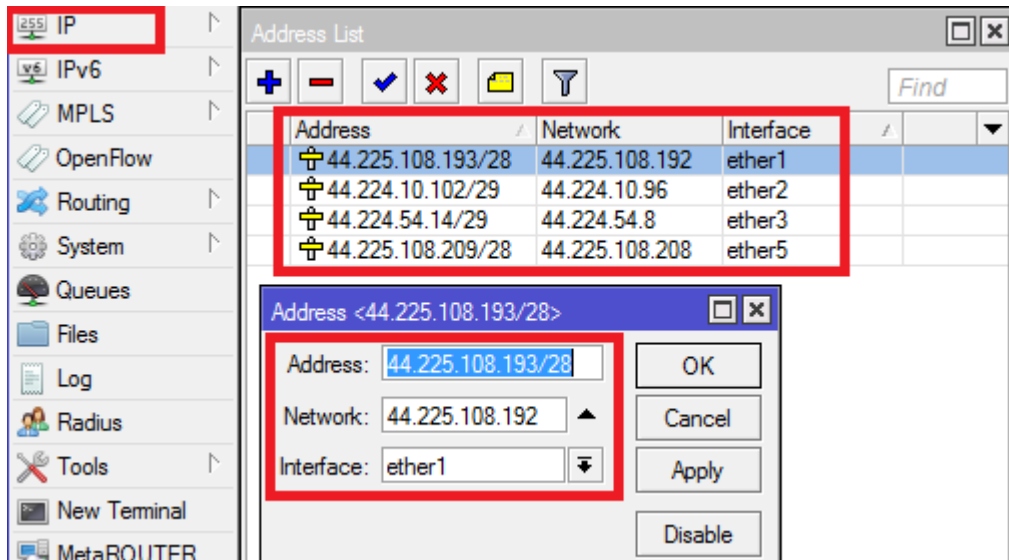
9.1. IP-Adressen den Interfaces zuweisen



In der „Interfaces“ Übersicht sieht man das auf ether1, 2, 3 und 5 bereits Aktivität herrscht bzw. etwas angeschlossen ist (Kennzeichnung „R“).

Als erstes werden den LAN (bzw. WLAN) Interfaces die passenden IP-Adressen zugewiesen. Dieser Vorgang ist bereits aus den vorhergehenden Instruktionen bekannt.

IP > Addresses

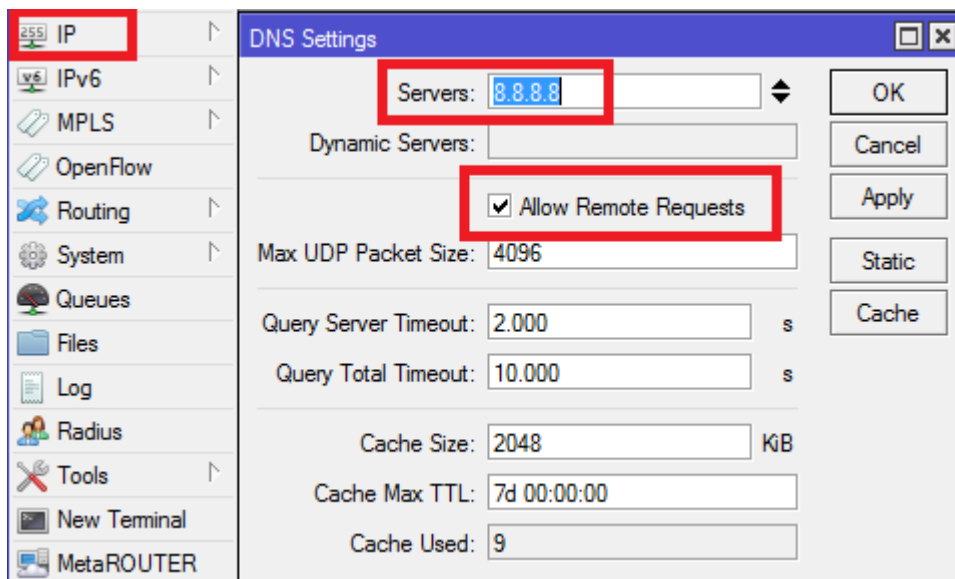


9.2. DNS-Server eintragen

Anschließend hinterlegen wir den zugehörigen DNS-Server unter

IP > DNS

und aktivieren das Kästchen „Allow remote requests“. Dadurch fragt der Router automatisch beim „Master“ DNS-Server an, falls er eine Adresse noch nicht selbst auflösen kann, wenn er sie noch nicht kennt. In der Grafik ist 8.8.8.8 nur ein Beispiel, hier kommt der Master DNS-Server für eure Region rein.



Unter <http://www.amateurfunk-wiki.de/index.php/Serviceverzeichnis> sind alle aktuellen DNS-Server aufgeführt. Aktuell stehen folgende zur Verfügung:

- 44.225.28.20 Hub-West (DBORES/Uni-Duisburg-Essen)
- 44.130.60.100 Hub-Süd (DB0FHN/FH-Nürnberg)
- 44.130.90.100 Hub-Ost (DB0TUD/TU-Dresden)

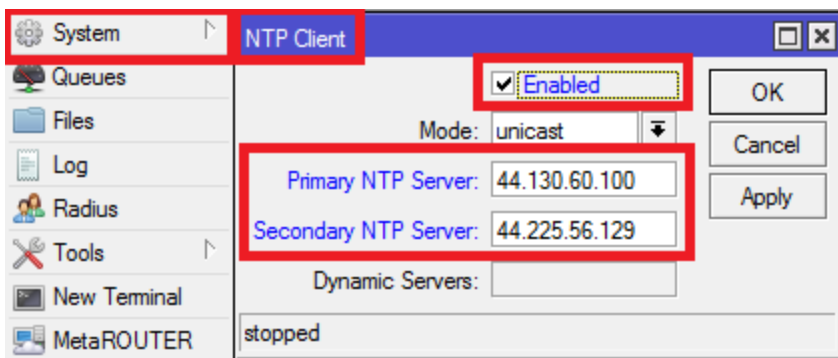
9.3. NTP Client einrichten

Damit in einem Netzwerk keine unterschiedlichen Zeitangaben auftreten, werden sogenannte NTP Server betrieben, auf denen ein einheitlicher Zeitgeber bereitgestellt wird. Alle Clients (Router,

Switches, Server etc.) können anhand dieser NTP Server regelmäßig ihre Systemzeit abgleichen. Im Hamnet sind mehrere NTP Server im Einsatz und sollten auch genutzt werden.

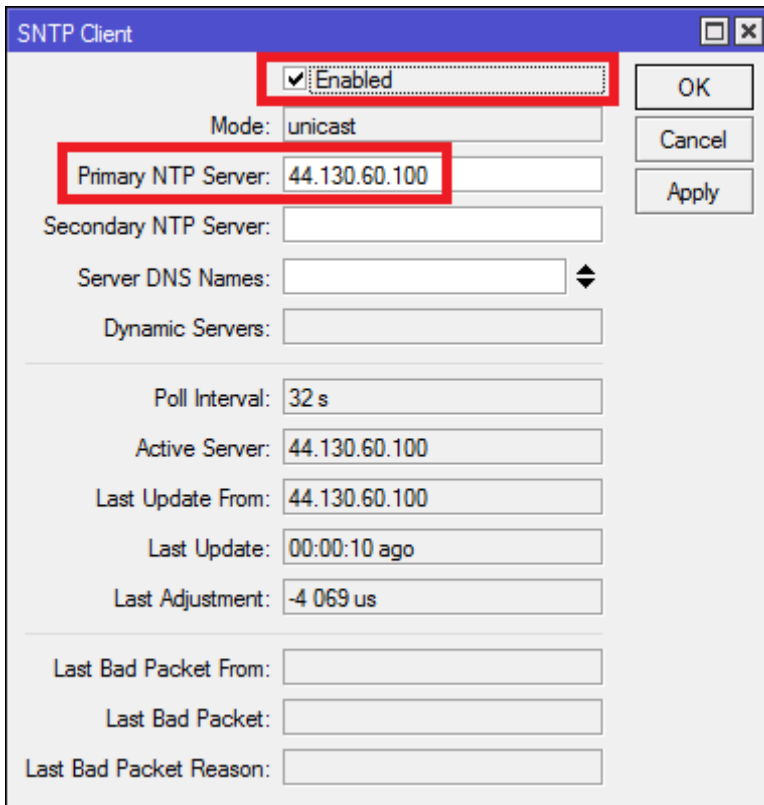
- 44.225.56.129 DB0SDA (RWTH Aachen, Internet)
- 44.225.52.20 DB0IUZ (Sternwarte Bochum, DCF77)
- 44.225.48.67 DB0OVN (Neuss, DCF77)
- 44.225.28.20 DB0RES (Rees/Niederrhein, Internet)
- 44.130.60.100 DB0FHN (FH-Nürnberg, Internet)
- 44.225.68.1 DFOUK (Karlsruhe, Internet)
- 44.225.29.129 IPKOORD-DL (Uni-Duisburg-Essen, Internet)
- 44.225.73.8 DB0LJ (Kruft/Mayen-Koblenz, DCF77)
- 44.225.160.74 DB0NDF (Niederdorfelden, Taunus-Relais-Gruppe, Internet, HAMNET)

SYSTEM > NTP Client

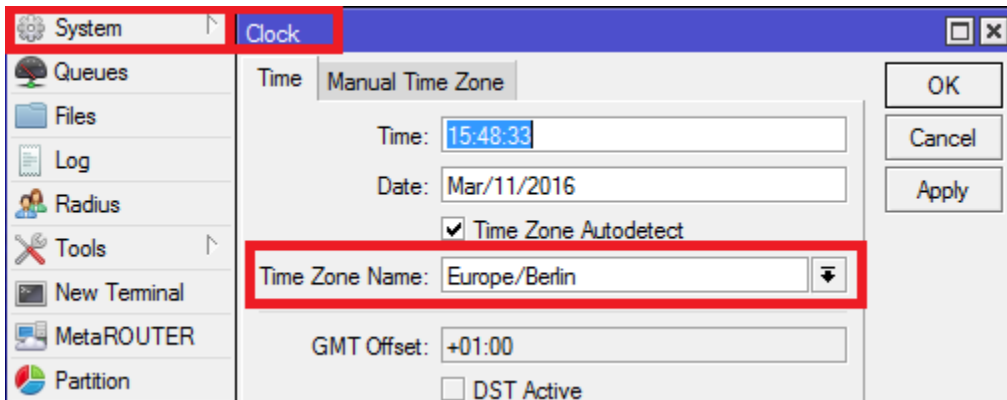


- a) „Enabled“ wird aktiviert
- b) Mindestens bei „Primary NTP Server“ wird die Adresse eines erreichbaren NTP Servers eingetragen
- c) Falls der Primary Server nicht erreichbar sein sollte, kann unter „Secondary NTP Server“ ein alternativer NTP Server eingetragen werden.

Achtung: Der Eintrag „SYSTEM > NTP Client“ existiert nur, wenn das Zusatzpaket „ntp.npk“ installiert wurde. Dadurch erscheinen im SYSTEM-Menü die Einträge „NTP Client“ und „NTP Server“. Wurde das NTP-Paket nicht installiert, heißt der Eintrag „SNTP Client“ und zeigt auch eine etwas andere Oberfläche:



Nun kann man unter SYSTEM > Clock die Systemzeit checken. Ist einer der NTP Server erreichbar, wird hier nun eine aktuelle Zeit angezeigt. Diese stimmt aber in der Regel noch nicht ganz, da die Zeitzone noch nicht bestimmt wurde. Ebenfalls unter SYSTEM > Clock lässt sich das gleich korrigieren.



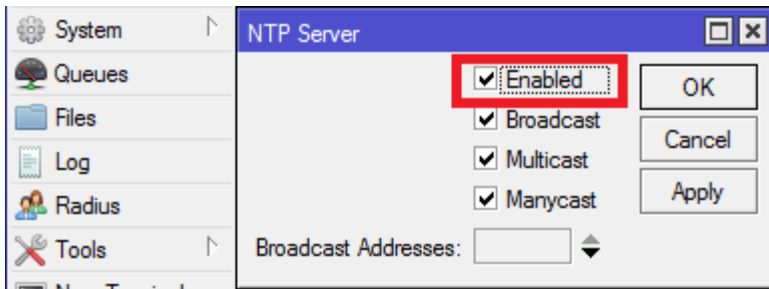
Hier muss nur unter „Time Zone Name“ die korrekte Zeitzone ausgewählt werden. In Deutschland wäre das Europe/Berlin. Nach dem Klick auf „Apply“ wird die Uhrzeit auch sogleich korrigiert.

9.4. NTP Server einrichten

Es macht Sinn den Hauptrouter auch als NTP Server zu konfigurieren. Dann genügt es in den Linkeinheiten nur den Hauptrouter als NTP Server zu hinterlegen. Dies spart Konfigurationsarbeit.

Achtung! Damit der NTP Server eingerichtet werden kann, muss das Zusatzpaket „ntp.npk“ installiert sein. Ansonsten ist der Eintrag nicht verfügbar.

SYSTEM > NTP Server



Der Haken bei „Enabled“ muss gesetzt werden, dann wird der NTP Server Dienst gestartet.

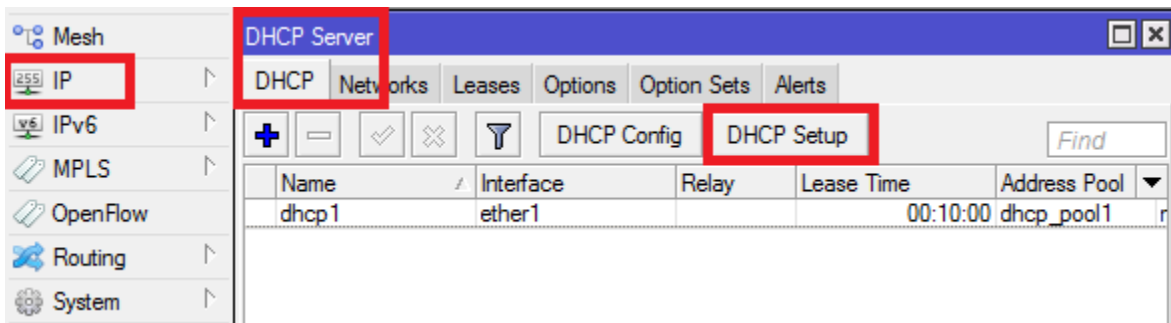
9.5. DHCP Server konfigurieren

Als nächstes werden die DHCP Server konfiguriert. Für unser Netz sind zwei Stück vorgesehen. Einer ist am ether1 aktiv im Servicebereich (falls man sich vor Ort befindet und mit einem Rechner einklinkt), der andere auf ether5 im UserEinstieg. Den DHCP-Server am UserEinstieg sollte man etwas anders konfigurieren wie im Servicenetz. Dazu aber weiter unten mehr. Zuerst wird die Einrichtung des DHCP-Servers im Usernetz erklärt.

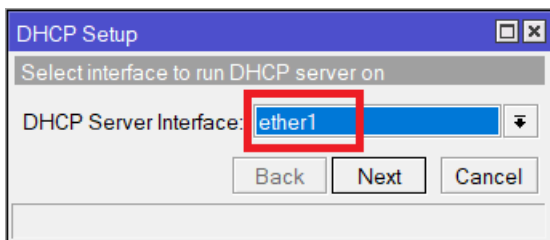
Man sollte alle anderen IP-Einstellungen an den Interfaces vorab eingerichtet haben bevor man hier weitermacht, denn dann werden viele Angaben automatisch vorbelegt.

Der Einstieg beginnt unter:

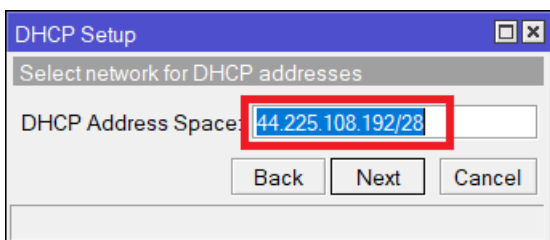
IP > DHCP Server



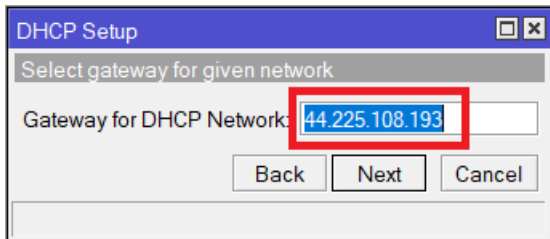
Hier klickt man im Reiter DHCP auf den button „DHCP Setup“ und folgt den Anweisungen.



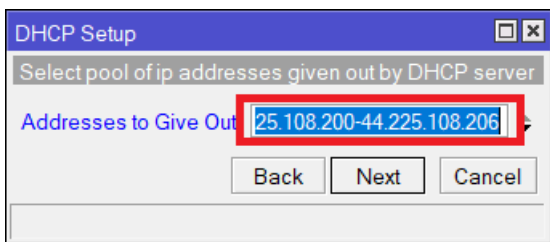
Hier gibt man das Interface an, auf dem der DHCP Server aktiv sein soll.



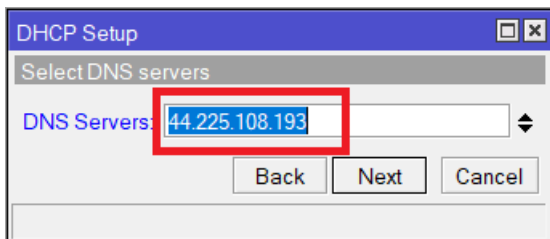
Ist vorher alles korrekt eingepflegt worden, erscheint hier automatisch der richtige Bereich für das genutzte Subnetz.



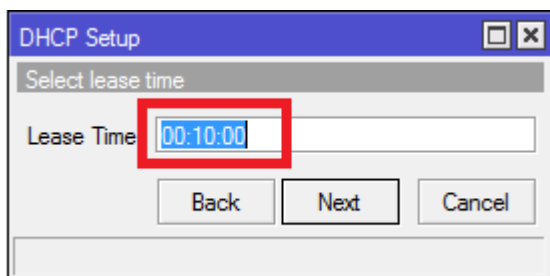
Dies ist die Default Route (IP-Adresse des Routers im Servicenetz). Sie wird aus den vorliegenden Informationen automatisch eingetragen und muss i.d.R. nicht geändert werden. Sie wird an die Clients weitergegeben.



Hier wird der zu vergebende Adresspool angegeben. Es müssen nicht alle Adressen aus dem Subnetz automatisch vergeben werden. Man kann auch einige Adressen frei halten für feste Adressvergaben bzw. für Server oder Computer im Servicenetz.

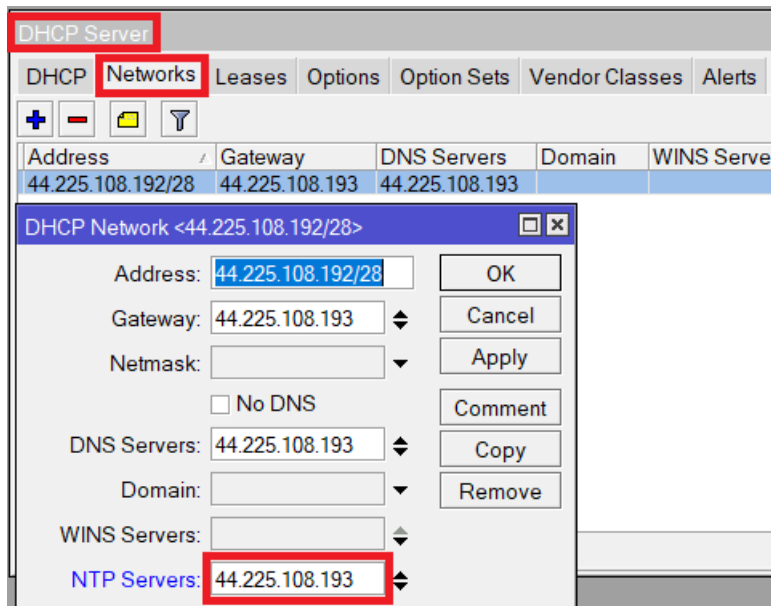


Automatisch wird hier der voreingestellte DNS-Server übernommen. Da der Router selbst als DNS-Server fungiert, müssen nicht alle Anfragen dauernd weitergeleitet werden, und man trägt auch hier die IP-Adresse des Routers im Servicenetz ein. Auch dies wird an die Clients weitergegeben.



Eine Lease Zeit von 10 Minuten ist voreingestellt und kann nach Wunsch verändert werden.

Über DHCP kann man noch viel mehr Informationen den Clients übergeben, aber was gibt es noch sinnvolles? Da unser Router ja auch als NTP-Server fungiert, kann man diesen natürlich auch noch „bewerben“.



Im DHCP-Server im Reiter Networks klickt man auf den soeben erstellten DHCP-Server. Dort kann man unter „NTP Servers“ auch noch die eigene IP-Adresse des Routers eintragen, der eben auch als NTP-Server fungiert. Diese Information wird dann ebenfalls über DHCP an die Clients übertragen. Diese können die Information nutzen, müssen es aber nicht.

9.6. DHCP-Server für das Usernetzwerk eintragen

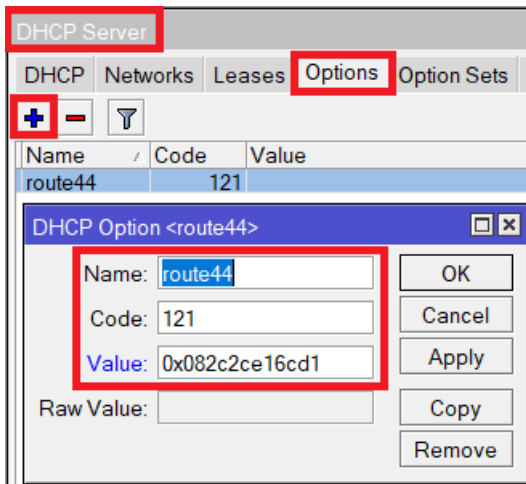
Man kann prinzipiell den DHCP-Server für das Usernetzwerk genau so einrichten, wie für das Service-Netzwerk. Allerdings kann es unter gewissen Umständen zu Problemen kommen, da man auf diese Weise ein Default Gateway an die Clients „verschickt“. Das bedeutet, dass die angeschlossenen Rechner und Geräte alle Anfragen, also auch die ins Internet, an den Hamnet-Digi schicken. Da der aber kein Internet hat und nur 44er Hamnet-IP Adressen routet, kann es hier zu Problemen kommen. Beispielsweise, wenn ein User seine Hamnet-Hardware aktualisieren möchte. Das RouterOS oder AirOS würde dazu im Internet nachsehen wollen. Der Hamnet-Digi erreicht diese Server aber nicht, da der Internetzugriff für User unterbunden bzw. nicht möglich ist.

Um dies zu verhindern, kann man dem DHCP-Server auch sagen, dass er nur die 44er Hamnet-Adressen als Route bekannt geben soll. Die Clients erhalten dann die Info das alle 44er Adressen darüber erreichbar sind, würden aber Anfragen ins Internet nicht in das Hamnet schicken, sondern an ein lokal verfügbares Internetgateway (DSL-Router) schicken.

Schritt für Schritt Anleitung:

Als erstes geht man vor wie im Abschnitt zuvor und erstellt einen DHCP-Server am UserEinstieg (ether5) mit Defaultgateway.

Anschließend erstellt man eine sogenannte DHCP-Option.



- Als „Name“ gibt man einfach etwas ein, was man sich merken kann.
- Der „Code“ gibt die jeweiligen DHCP Option an, die genutzt werden soll. Eine IP-Route wird mit Option 121 mitgeteilt.
- Unter „Value“ muss man den entsprechenden hexadezimalen Wert angeben. Wie man diesen berechnen kann, kann man in der [RouterOS Dokumentation](#) nachlesen. Natürlich gibt es im Internet auch Generatoren dafür, so dass man den betreffenden Wert einfach generieren kann.

Ein Beispiel eines solchen Generators findet sich z.B. hier:

https://ip-pro.eu/en/mikrotik_dhcp_option_121_generator

Generator DHCP Option 121

Option 121 String Generator

Dst-address= / gateway=

DHCP Option 121 value:

This calculator is provided for free without any warranty it will reflect real data usage in Mikrotik Routerboard.

Auf der Seite angekommen gibt man die entsprechende Route mit Netzmaske sowie das entsprechende Gateway ein. Das Gateway ist die IP-Adresse des Router im Usernetz. Damit wird dem Client mitgeteilt, dass er alle 44er IP-Adressen über den Hamnet-Knoten erreichen kann.

Achtung:

Ab 1.11.2020 wird sich die Route allerdings ändern. Wenn der Umzug der deutschen Hamnet IP-Adressen in den neuen Bereich abgeschlossen ist, besteht das Hamnet nicht mehr aus dem Adressraum 44.0.0.0/8, sondern aus den folgenden beiden Bereichen:

44.0.0.0/9 sowie 44.128.0.0/10

Die DHCP-Option berechnet man dann wie folgt:

Generator DHCP Option 121

Option 121 String Generator

Dst-address=	44.0.0.0	/	8	gateway=	44.225.108.209
Dst-address=	44.128.0.0	/	10	gateway=	44.225.108.209

Add New Row

DHCP Option 121 value:

0x082c2ce16cd10a2c802ce16cd1

Zu beachten ist, dass diese „neue“ DHCP-Option erst gesetzt wird, wenn ALLE Router und Geräte im deutschen Hamnet umgestellt wurden (Veröffentlichungen der IP-Koordination beachten!). Macht man es vorher, ist der Zugriff auf Geräte im „alten“ Netz nicht mehr möglich.

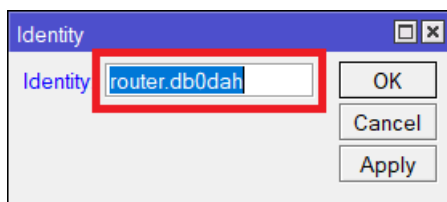
9.7. Optional: HF Parameter den WLAN Ports zuweisen.

Wenn man z.B. einen RB433AH verwendet, kann man an dieser Stelle noch die WLAN-Einstellungen an den WLAN-Interfaces vornehmen, analog zu den Einstellungen bei den Außeneinheiten.

9.8. Identity eintragen

Auch der Router sollte eine passende Identity haben, um besser identifiziert werden zu können:

SYSTEM > IDENTITY



9.9. BGP Monitoring einschalten

Anfang 2020 wurde in der HamnetDB ein BGP Monitoring eingebaut. Die Darstellung der BGP-Verbindungen auf der HamnetDB-Karte soll den HAMNET-Teilnehmern ermöglichen den zu erwartenden Pfad einer Wegeverfolgung (HamnetDB-Karte) mit dem tatsächlich beobachteten Pfad zu vergleichen (Traceroute).

Ein Router kann in die Monitoring-Lösung mit aufgenommen werden, wenn folgende Bedingungen erfüllt sind:

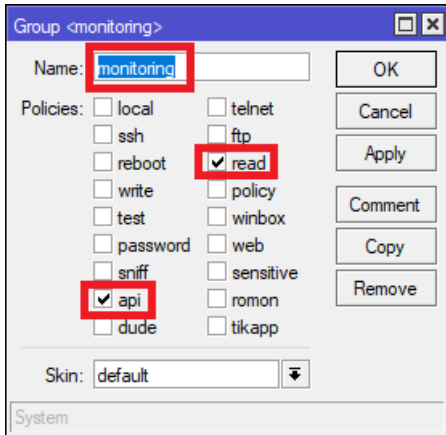
- Es werden nur BGP-Router von Mikrotik unterstützt.
- Die Mikrotik-API ist auf dem Standardport des BGP-Routers für 44.148.230.161 erreichbar.
- Der User "monitoring" ist mit passenden Rechten auf dem Router eingerichtet.
- In der HamnetDB ist der Hosteintrag des Routers im Sitenetwork mit dem Routing-Flag versehen (in der Regel die erste IP aus dem Sitenetwork mit Hostnamen "router.<call>")

Erstellen der Benutzergruppe und des Benutzers "monitoring":

SYSTEM > USERS

Tab: Groups > "+" drücken

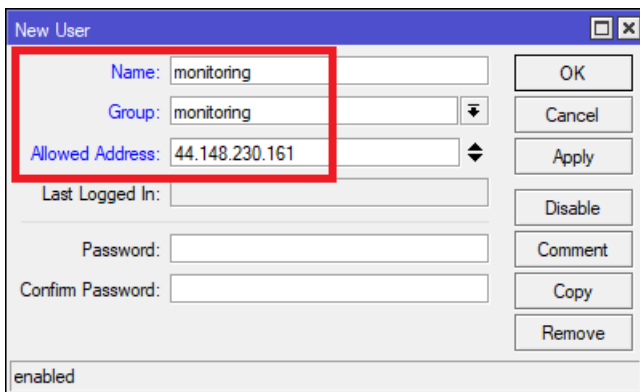
- Name = monitoring
- Policies = read, api



SYSTEM > USERS

Tab: Users > "+" drücken

- Name = monitoring
- Group = monitoring
- Allowed Address = 44.148.230.161



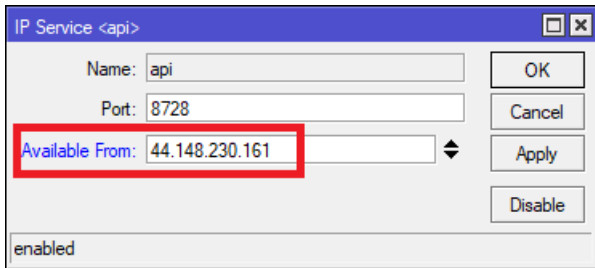
Überprüfen, ob die Mikrotik API aktiviert ist:

IP > SERVICES > „api“ aktiv

IP Service List			
Name	Port	Available From	
api	8728		
X api-ssl	8729		

Wer ein höheres Sicherheitsbedürfnis hat, der kann den Zugriff auf die Mikrotik-API auf die Monitoring-Plattform einschränken.

IP > SERVICES > "api" doppelklicken:



IP Service <api>

Name: api

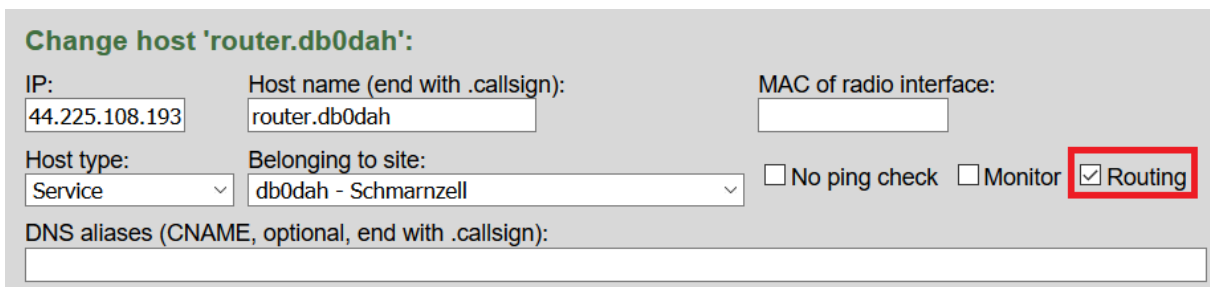
Port: 8728

Available From: 44.148.230.161

enabled

"Available From: 44.148.230.161"

Nach der Vorbereitung des BGP-Routers kann das "Routing"-Flag in der HamnetDB gesetzt werden.



Change host 'router.db0dah':

IP: 44.225.108.193

Host name (end with .callsign): router.db0dah

MAC of radio interface:


Host type: Service

Belonging to site: db0dah - Schmarzell

No ping check Monitor Routing

DNS aliases (CNAME, optional, end with .callsign):

Wenn der Host angeklickt wird, dann kann die Erreichbarkeit der Mikrotik-API durch die Monitor-Plattform manuell geprüft werden:



Host router.db0dah - 44.225.108.193 (Service)

Routing monitoring - **Enabled**

[test Routing monitoring](#)

Monitoring - Routing:

enabled

Ping:

ok

Features:

BGP successfully tested

Traceroute successfully tested

10. Ethernet over IP (EoIP) Tunnel nutzen

10.1. Was ist EoIP?

EoIP ist ein Mikrotik eigenes Verfahren und funktioniert daher auch nur mit Mikrotik-Routern untereinander. Es erzeugt ein virtuelles EoIP Tunnelinterface und ermöglicht dadurch die einfache Kommunikation über IP-Grenzen hinweg, z.B. zum Verbinden zweier LANs über das Internet. So als wenn beide Netze mit einem LAN-Kabel verbunden wären. Über dieses Tunnelinterface kann alles geschickt werden, was auch über ein Ethernet Kabel zu übertragen ist, unabhängig vom Protokoll.

10.2. Wann benötigt man EoIP?

EoIP wird beispielsweise dann benötigt, wenn man mehrere Mikrotik Router zusammenschalten möchte, z.B. wenn alle Ports am zentralen Router belegt sind bzw. nicht mehr genug frei sind für die noch zu realisierenden Linkstrecken. Kombiniert man beispielsweise zwei RB433AH Router miteinander, hätte man gleichzeitig sechs HF Ports zur Verfügung. Da aber immer nur einer der Router die „Zentrale“ sein kann, muss das andere Routerboard entsprechend „angedockt“ werden, damit man dessen WLAN-Interfaces so mit nutzen kann, als wären sie Teil des ersten Routerboards.

Ein anderes Beispiel wäre, wenn man z.B. den zentralen Router sicher im Gebäude verstaubt, dann mit EINEM LAN-Kabel auf den Mast und in einen Switch geht, wo dann mehrere Außeneinheiten (Nanostation, Mikrotik SXT, Groove oder Metal) angeschlossen sind. Jede dieser Außeneinheiten muss vom zentralen Router separat über ein eigenes Interface angesprochen werden. EoIP hilft dabei.

10.3. Verkabelung der Routerboards untereinander

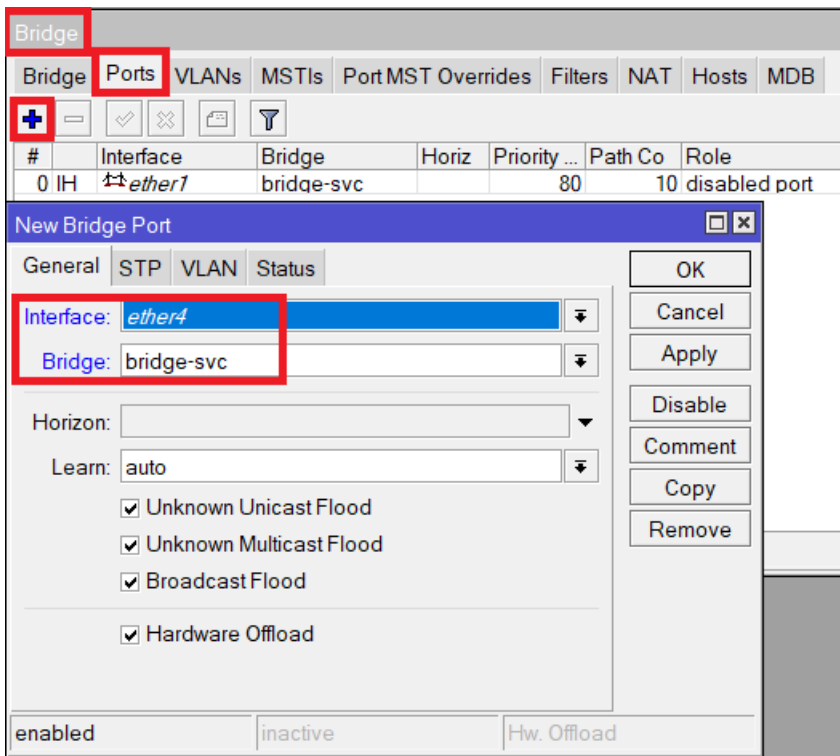
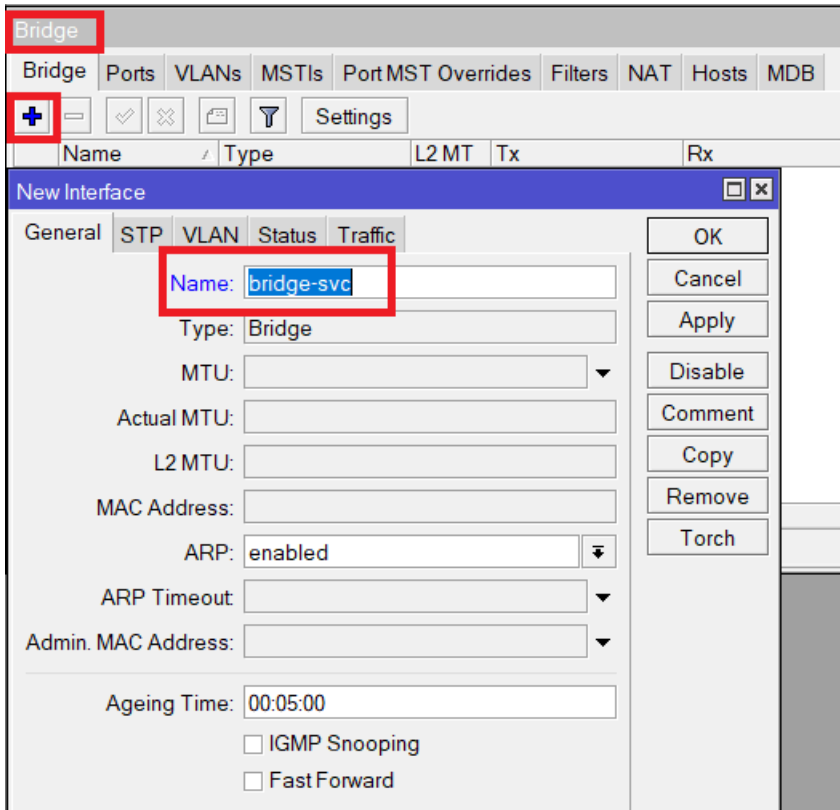
In der nun folgenden Beispielkonfiguration soll der RB750 mit zwei weiteren Linkstrecken ergänzt werden. Jedoch ist nur noch ein Ethernet Anschluss am Router frei, ether4. Des Weiteren muss das Routerboard IP-technisch im Service-Netz untergebracht werden.

Es gibt nun zwei Möglichkeiten die Routerboards mechanisch miteinander zu verbinden. Die erste Möglichkeit wäre, man schließt das RB433AH an den Switch an, der an ether1 hängt. Damit hängt er direkt im Servicenetz. Besser aber wäre die Möglichkeit, den RB433AH am ether4 des RB750 anzuschließen. Dann hätte man sogar die Möglichkeit das RB433AH über das LAN-Kabel mit Strom zu versorgen (PoE). Was die EoIP Konfiguration angeht, gibt es aber keinen Unterschied zwischen den beiden Varianten.

Achtung: Der Folgende Abschnitt wurde an RouterOS Version 6.41 und höher angepasst. Das Switch/Bridge Handling hat sich hier deutlich verändert.

Als erstes muss man dafür sorgen, dass der ether4 mit am Servicenetz hängt. Dazu erstellt man eine Bridge und fügt die zwei Ports ether1 und ether4 der Bridge hinzu.

RouterOS erkennt übrigens automatisch, wenn zwei Ports zusammen an einem mechanischen Switch hängen und lässt diese hardwaremäßig über den Switch kommunizieren. Dies entlastet den Prozessor erheblich. Sind diese nicht an einem gemeinsamen Switch, erfolgt die Verbindung softwareseitig über den Prozessor.



Das „H“ im Status („IH“) bedeutet, dass diese Ports über den Hardwareswitch miteinander verbunden sind.

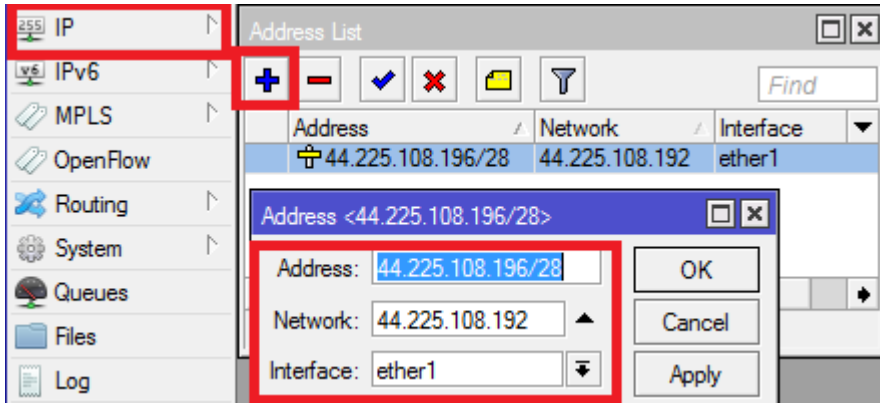
Beim Erstellen der Bridge ist darauf zu achten, dass die IP-Adresszuweisung dann nicht mehr auf dem Ethernet-Port (ether1) zu erfolgen hat, sondern direkt auf der bridge. Man ändert also einfach unter

IP > ADDRESSES einfach die Portzuordnung im entsprechenden IP-Adresseintrag von „ether1“ auf „Bridge-svc“

Anschließend muss man nun dem RB433AH eine IP-Adresse aus dem Servicenetz zuteilen, damit die Routerboards miteinander kommunizieren können.

Ether1 im RB433AH erhält daher die folgende Adresse

44.225.108.196/28; Network = 44.225.108.192

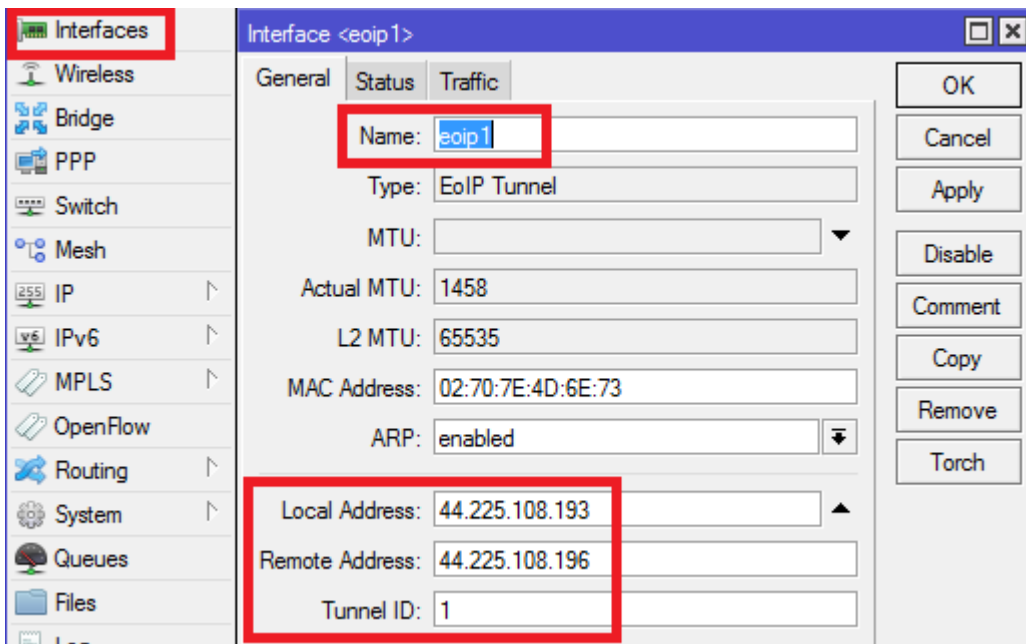


10.4. EoIP konfigurieren

Nachdem die Routerboards nun miteinander kommunizieren können, können die EoIP Interfaces konfiguriert werden.

Es sollen die Interfaces WLAN1 und WLAN2 im RB433AH genutzt und mit dem RB750 „verbunden“ werden. Das bedeutet man legt erstmal zwei EoIP Tunnel vom RB750 zum RB433AH an. Erstellt werden die Tunnel unter:

INTERFACES > Reiter „EoIP Tunnel“



Man gibt jedem Tunnelinterface einen Namen und ganz unten eine eindeutige Tunnel-ID. Die Tunnel-ID dient dem eindeutigen Identifizieren der Tunnel untereinander. Der Interfacename selbst dient nur der Darstellung in der Oberfläche und erscheint dann auch in der Interfaces Übersicht.

- Local Address = das lokale „Interface“ wo der Tunnel „beginnt“ (44.225.108.193)
- Remote Address = das Zielinterface am anderen Router (44.225.108.196)

Es werden zwei Tunnel „eoi1“ und „eoi2“ mit denselben Daten erstellt, jedoch mit unterschiedlicher Tunnel-ID.

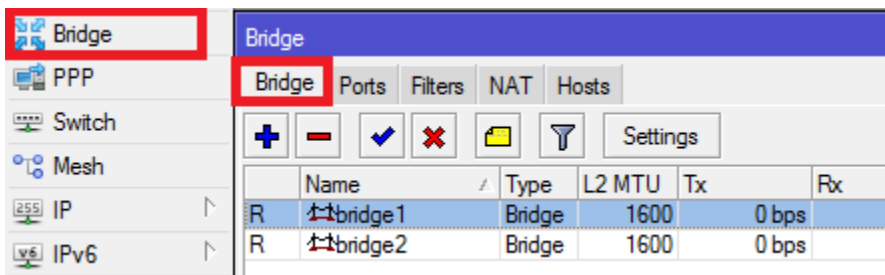
Das Gleiche wird auch im RB433AH gemacht, nur mit vertauschtem Start und Ziel. Sprich, es werden „Local Address“ und „Remote Address“ miteinander vertauscht.

Damit sind die Interfaces erstellt und die Router arbeiten so miteinander, als wären sie mit zwei LAN-Kabeln verbunden.

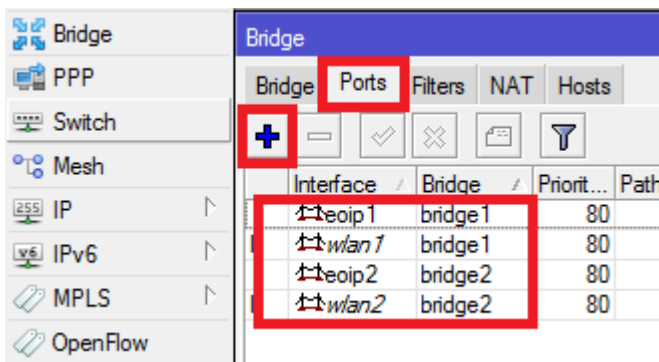
10.5. WLAN-Interfaces des RB433AH mit dem zentralen Router „verbinden“

Nun müssen die Enden des EoIP Tunnels im RB433AH noch mit den WLAN-Interfaces verbunden werden. Das ist genauso, wie wenn ein normales Außeninterface konfiguriert würde. Bei Außeninterfaces bridged man den LAN-Anschluss mit dem WLAN-Anschluss. Hier wird der LAN-Anschluss durch das EoIP Interface ersetzt. Man erstellt also zuerst zwei bridges unter

BRIDGE > BRIDGE



Und anschließen fügt man die Interfaces zu den jeweiligen bridges hinzu. Eoi1 und wlan1 zur bridge1 sowie eoi2 und wlan2 zur bridge2.



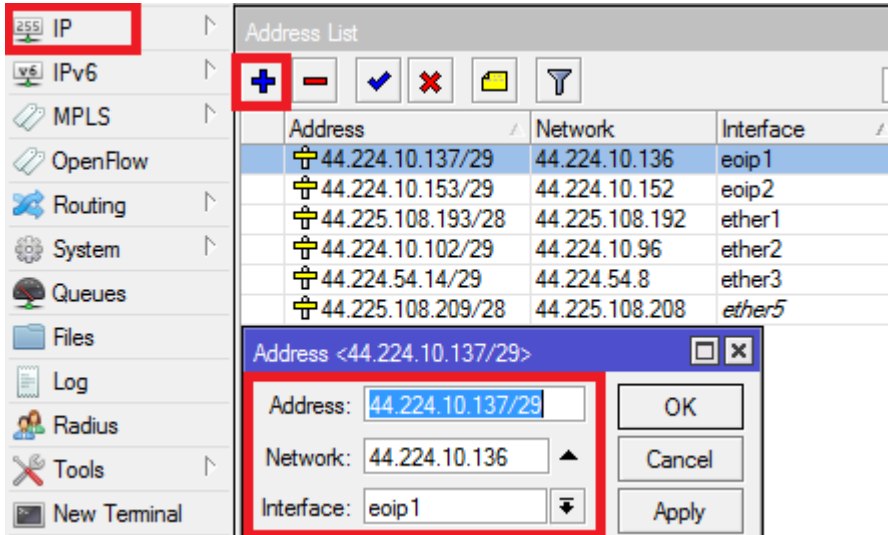
Damit sind die beiden WLAN-Interfaces mit dem Router technisch verbunden. Was jetzt noch fehlt ist die IP-Konfiguration. Dies funktioniert genauso wie weiter oben beschrieben.

Um dies einzurichten, benötigt man die Informationen über die zu verwendenden IP-Subnetze für die Links. Es wird angenommen, den Links wurden die folgenden Subnetze zugewiesen und der eigene Knoten verwendet jeweils die ersten beiden nutzbaren Adressen aus dem Subnetz, die Linkpartner die letzten beiden:

- Link 3 auf WLAN1/eoip1/bridge1 nutzt das Subnetz 44.224.10.136/29
- Link 4 auf WLAN2/eoip2/bridge2 nutzt das Subnetz 44.224.10.152/29

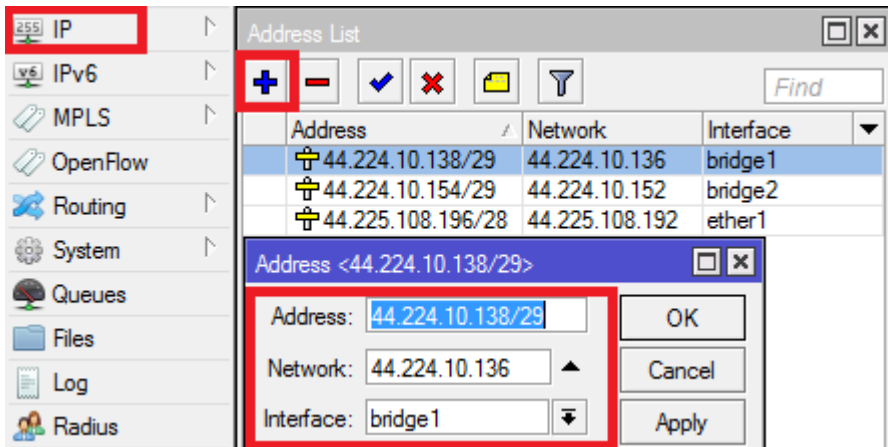
Im zentralen Router RB750 werden folgende Adressen vergeben:

- Interface eoip1 = 44.224.10.137/29; Network = 44.224.10.136
- Interface eoip2 = 44.224.10.153/29; Network = 44.224.10.152



Im RB433AH vergibt man die Adressen den bridges:

- Interface bridge1 = 44.224.10.138/29; Network = 44.224.10.136
- Interface bridge2 = 44.224.10.154/29; Network = 44.224.10.152



Nun sind die externen WLAN-Interfaces des RB433AH direkt mit dem RB750 „verbunden“, als wären sie separat angeschlossen. Anschließend müssen natürlich noch im RB433AH die passenden HF-Parameter in den WLAN-Interfaces hinterlegt werden, damit die Verbindung auch aufgebaut werden kann. Wie das geht, wurde bereits weiter oben beschrieben.

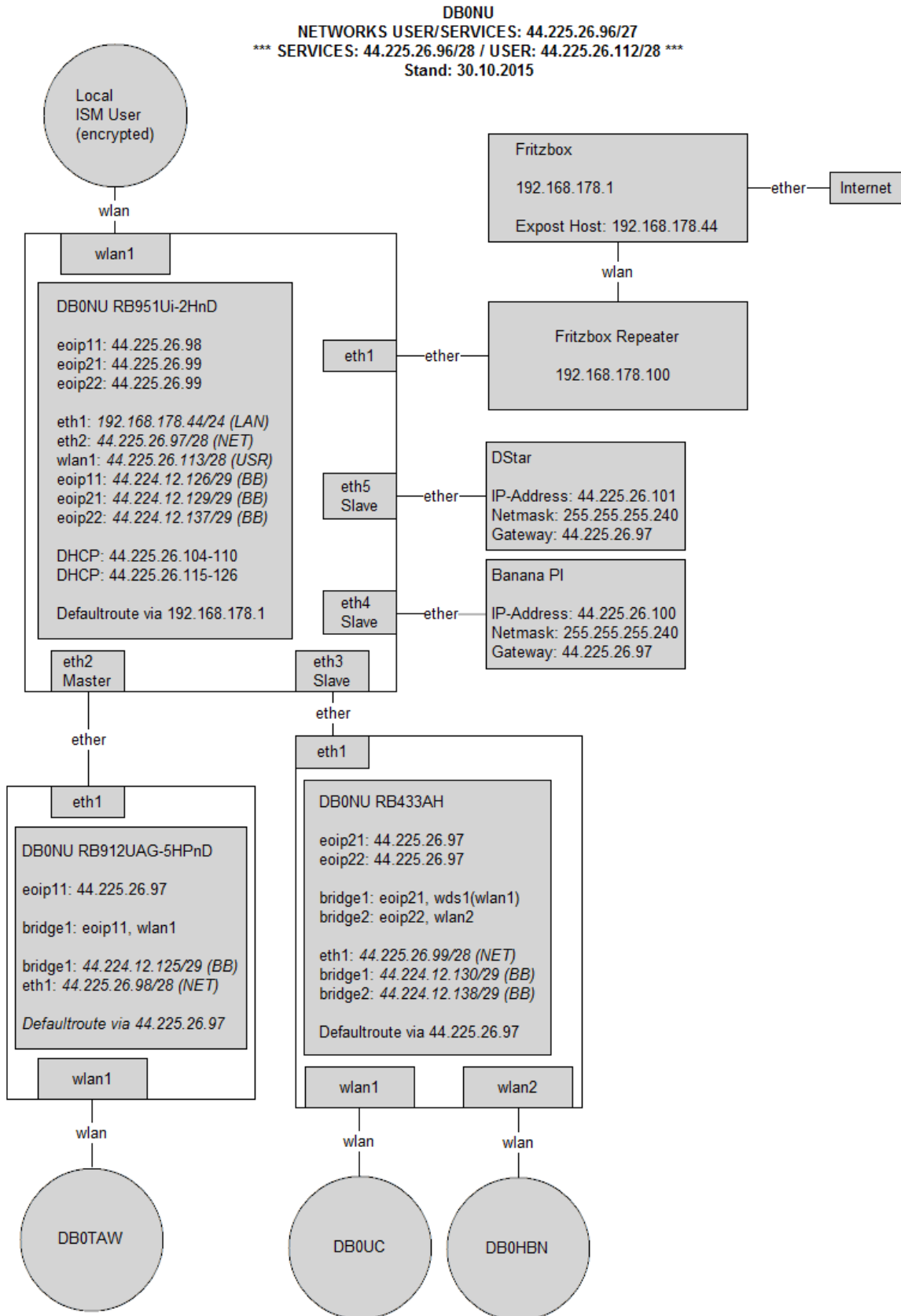
10.6 EoIP intelligent nutzen

EoIP macht nicht nur Sinn, wenn man wie oben beschrieben mehrere entfernte WLAN-Ports auf anderen Routerboards „andocken“ möchte. Für administrative Zwecke kann es durchaus Sinn machen, alle Außeneinheiten über EoIP einzubinden. Vorausgesetzt man setzt durchweg auf Mikrotik Hardware. Mit Ubiquity Geräten geht dies leider nicht. Man kann das Prinzip schön (bei einem alten Stand) von DBONU erkennen (nächstes Bild).

An ether2 ist ein einzelnes RB912 angeschlossen. An ether3 ist ein RB433AH verbunden. Während es beim RB433AH Sinn macht, mit EoIP zu arbeiten, da so dessen zwei WLAN-Ports mitgenutzt werden, ist dies eigentlich beim RB912 nicht notwendig. Aber warum macht man das?

Zum einen vereinheitlicht man damit die Konfiguration. Zum anderen hat dies auch einen großen Vorteil. Aber zuerst soll die Konfiguration erklärt werden: Die Ports ether2 bis ether5 sind alle in einem Switch zusammengefasst, ether2 ist der Master und es liegt hier das Service-Netz 44.225.26.96/28 an. Demnach sind alle Komponenten von ether2 bis ether5 direkt im Servicenetz angebunden. Jede dieser Komponenten, ist mit einer IP aus dem Servicenetz ausgestattet. All diese Geräte, inklusive dem zentralen Router, können nun miteinander direkt im Servicenetz kommunizieren. Mit EoIP spricht man die WLAN-Interfaces an den entfernten Routerboards an und nutzt diese z.B. für den Backbone. Als Administrator klinkt man sich daher einmalig in dieses Servicenetz ein (direkt am Knoten oder über den Usereinstieg), und hat damit direkt Kontakt mit allen Geräten, ohne irgendwie routen zu müssen. Nach Öffnen der WinBox werden direkt alle Geräte angezeigt, egal ob diese bereits eine IP-Adresse haben oder nicht und unabhängig davon ob die Routerboards untereinander konfiguriert sind bzw. überhaupt miteinander kommunizieren. Wären die entfernten Routerboards nur über die Transernetze ansprechbar, und gäbe es dort ein Konfigurationsproblem, könnte man sich mit diesen nicht mehr direkt verbinden, sondern müsste sich direkt an das LAN-Kabel anschließen um nachzusehen. Etwas mehr Konfigurationsaufwand führt hier zu mehr Flexibilität und mehr Übersicht.

Eine nicht-proprietäre Alternative zu Ethernet-over-IP ist VLAN, denn das wird von den meisten Herstellern unterstützt. Mehr dazu im nächsten Kapitel.



11.VLAN am HAMNET Knoten nutzen

11.1 Einleitung zu VLAN

Wie im letzten Kapitel 10 bereits beschrieben gibt es manchmal Situationen an Standorten, die etwas „Zauberei“ erfordern. Und zwar immer dann, wenn man mehrere Devices über ein LAN-Kabel an den Hauptrouter anbinden möchte. EoIP ist dann eine einfache Sache. Es hat aber zwei deutliche Nachteile: Zum einen erzeugt es eine Menge Daten-Overhead, zum anderen geht es nur mit MikroTik Geräten. VLAN dagegen ist standardisiert und wird so ziemlich von allen Herstellern unterstützt.

Ich möchte hier nicht auf die Grundlagen von VLAN eingehen, das könnt ihr im entsprechenden Wikipedia-Artikel nachlesen: https://de.wikipedia.org/wiki/Virtual_Local_Area_Network

Im Grunde genommen ermöglicht VLAN es, mehrere logisch voneinander getrennte Netzwerke über eine LAN-Verbindung zu führen. Man erspart sich also zusätzliche LAN-Kabel. Unterschieden werden die einzelnen Netze durch Ihre VLAN-ID, genau wie bei EoIP. Die Konfiguration ist ähnlich und erfolgt ebenfalls auf beiden Seiten.

Vorab wichtig zu wissen ist, das MikroTik es mit RouterOS 6.47 immer noch nicht geschafft die hardwarebasierte VLAN-Konfiguration so einfach zu gestalten wie seinerzeit die Bridge-Konfiguration. Bei Bridges entscheidet RouterOS selbst, ob der hardwarebasierte Switch-Chip benutzt wird (hardware offload) oder die Daten softwareseitig über den Prozessor laufen. Ökonomischer und performanter ist natürlich die hardwarebasierte Variante. Es unterstützt auch praktisch jedes MikroTik Gerät das hardwarebasierte VLAN switching. Dieses zu konfigurieren ist jedoch recht komplex und unterscheidet sich auch noch von Gerätetyp zu Gerätetyp, nachzulesen hier:

https://wiki.mikrotik.com/wiki/Manual:Basic_VLAN_switching

Da im Hamnet in der Regel eh keine großen Datenraten anfallen, sollte es allerdings kein Problem darstellen die vergleichsweise einfach zu konfigurierende softwarebasierte VLAN Konfiguration anzuwenden.

11.2 Konfigurationsbeispiel

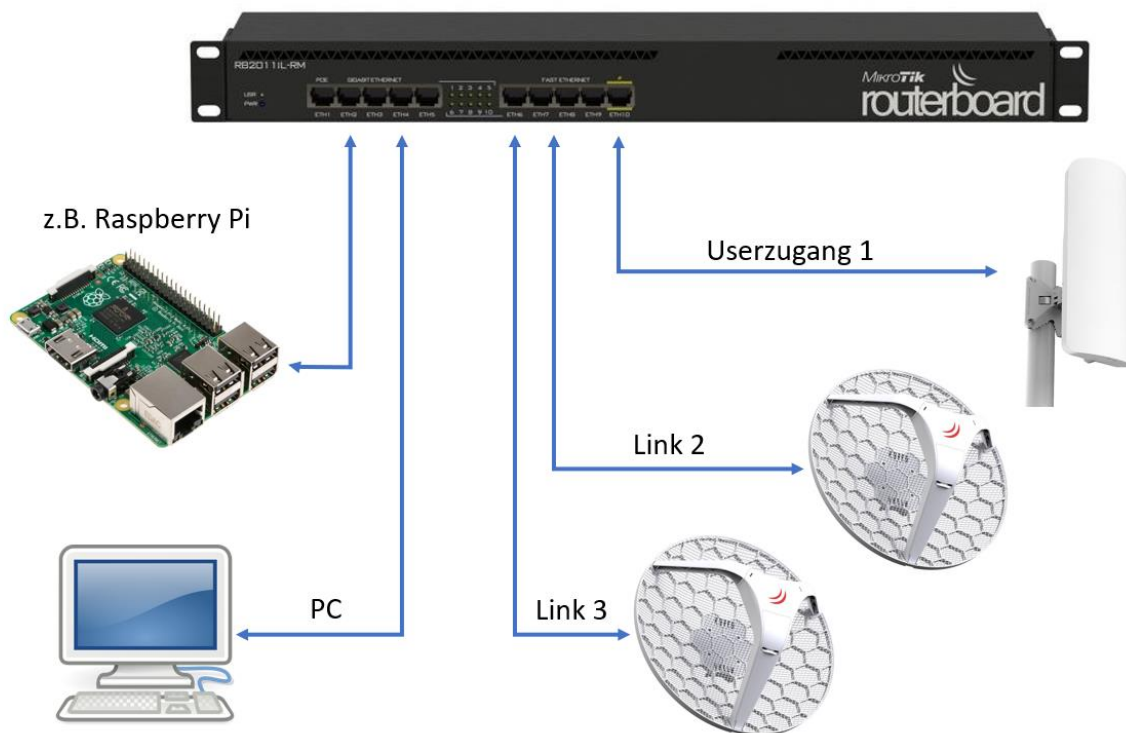
Im folgenden Beispiel soll ein Hauptrouter (RB2011, ether5) mit einem Outdoor PoE Switch (Powerbox, ether1) erweitert werden. Die Powerbox ist mit einem LAN-Kabel an dem Hauptrouter angeschlossen. An der Powerbox sollen erstmal zwei weitere Geräte angeschlossen werden. Eine Link-Antenne und eine zusätzliche Antenne für den UserEinstieg.

Die Ausgangslage sieht wie folgt aus:

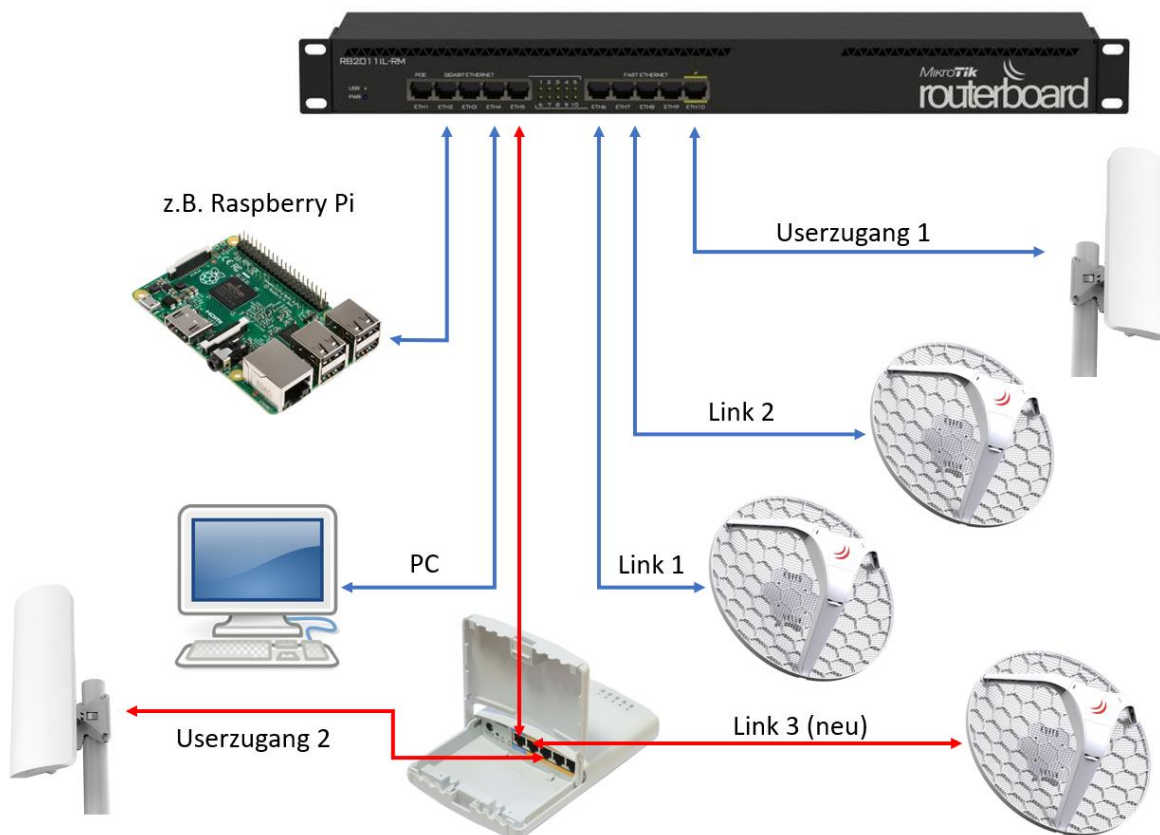
Hauptrouter RB2011:

ether1 bis ether5 sind in einer Bridge (Service-Bridge) wo sich alle lokalen Geräte befinden. An ether6 und ether7 befinden sich zwei Linkstrecken. An ether10 ist eine einzelne Antenne für den UserEinstieg vorhanden.

- service-bridge (ether1 bis ether5) = 44.149.25.1/28
- ether6 = 44.148.12.1/29 (Backbone-IP Link 1)
- ether7 = 44.148.12.57/29 (Backbone-IP Link 2)
- ether10 = 44.149.25.17/28 (Gateway Userzugang)



Nach der Erweiterung wird es so aussehen:



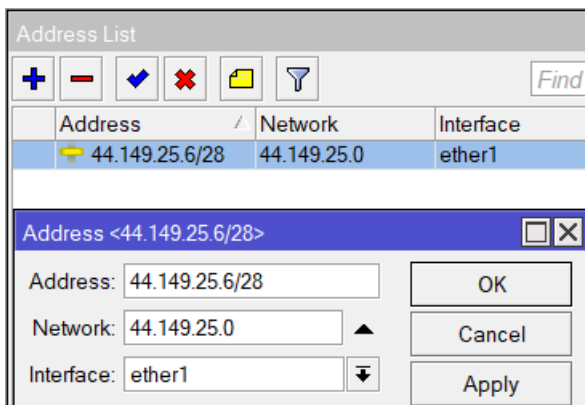
Schritt 1: Powerbox vorbereiten

Die Powerbox wird nun als erstes in das Servicenetz integriert, damit wir darauf arbeiten können. Die Minimalkonfiguration sind eine IP-Adresse, ein eingetragener DNS-Server und eine Default-Route. Natürlich sollte man auch Dinge wie Admin-Kennwort, NTP-Server usw. nicht vergessen. Auf die genaue Konfiguration gehe ich nicht ein, das ist analog zu der Konfiguration von anderen Geräten.

Konfiguration PowerBox:

- ether1 = 44.149.25.6/28 (Teil des Servicenetzes)
- Default-Gateway, DNS-Server, NTP-Server = 44.149.25.1 (Hauptrouter)

Es spielt übrigens keine Rolle, wenn wir auf einem Ethernet Interface sowohl eine „normale“ LAN-Verbindung haben als auch zusätzliche VLAN Interfaces. Diese stören sich nicht gegenseitig.



Die Powerbox ist damit ein Teil des Servicenetzes. Bitte Default-Route und DNS Server einstellen nicht vergessen.

Alle weiteren Geräte sind ebenfalls bereits konfiguriert:

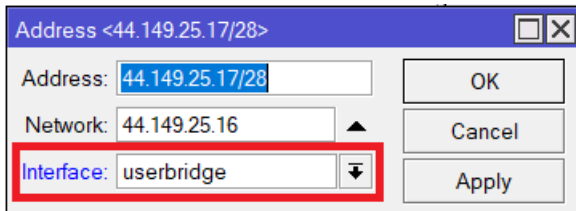
- Antenne Link 1: 44.148.12.2/29 (TRX-IP)
- Antenne Link 2: 44.148.12.58/29 (TRX-IP)
- Userzugang 1: 44.149.25.18/28 (IP des Access Points)
- NEU: Antenne Link 3: 44.148.12.66/29 (TRX-IP)
- NEU: Userzugang 2: 44.149.25.23/28 (IP des Access Points)

Die beiden neuen Geräte müssen nun korrekt an den Hauptrouter „angedockt“ werden, damit sie sich auch in „ihren“ Netzen befinden, und nicht im Servicenetz herumgeistern.

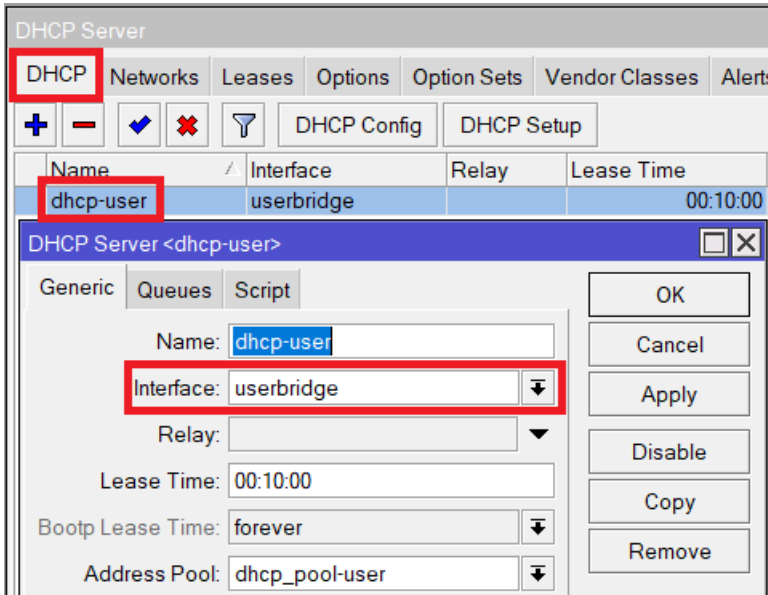
Schritt 2: Userbridge erstellen und IP-Einstellungen anpassen

Da der Userzugang zukünftig aus zwei Antennen besteht, erstellen wir im Hauptrouter als erstes eine Bridge für den Userzugang und legen alle IP-Einstellungen darauf:

Die User-Gateway-IP 44.149.25.17/28 wandert vom Interface ether10 auf das neue „userbridge“ Interface.



Ebenfalls muss der DHCP-Server von ether10 auf das „userbridge“ Interface umgestellt werden.



Nur so können sich User über beide Antennen gleichwertig verbinden und landen auch im gleichen Usernetz (44.149.25.16/28).

Schritt 3: VLAN Interfaces im Hauptrouter erstellen

Um auch für zusätzliche Geräte an der Powerbox gewappnet zu sein, konfigurieren wir gleich alle vier Schnittstellen der Powerbox für die VLAN Nutzung. So lässt es sich jederzeit problemlos erweitern.

INTERFACES > „+“-Symbol > VLAN

Im Hauptrouter RB2011 erstellen wir vier VLAN-Interfaces auf dem Anschluss ether5, denn hier hängt die Powerbox dran. Als VLAN-ID eignet sich eine Kombination aus Portnummer des Hauptrouters und Portnummer des „Ausgangs“ an der Powerbox. So ist immer eine logische Zuordnung möglich. Diese ID sollte man idealerweise auch in der VLAN-Bezeichnung einfügen, damit man weiß welches VLAN zu welcher VLAN-ID gehört.

Am RB2011 nutzen wir ether5 und das VLAN soll an der Powerbox ether2 ansprechen. Wir nennen das VLAN dann „VLAN52“ und es erhält die ID „52“. Das Gerät an ether3 der Powerbox erhält dann die VLAN-ID „53“ usw.

The screenshot shows the Mikrotik WinBox interface. At the top, the 'Interface List' window is open, displaying a table of network interfaces. A red box highlights the '+' icon in the toolbar, indicating the process of adding a new interface. The table below shows several Ethernet interfaces (ether1-5) and five VLAN interfaces (vlan52-55). The 'vlan52' interface is highlighted in blue.

	Name	Type	Actual MTU	L2 MTU	Tx
S	ether1	Ethernet	1500	1598	
S	ether2	Ethernet	1500	1598	
S	ether3	Ethernet	1500	1598	
S	ether4	Ethernet	1500	1598	
RS	ether5	Ethernet	1500	1598	
R	vlan52	VLAN	1500	1594	
R	vlan53	VLAN	1500	1594	
R	vlan54	VLAN	1500	1594	
R	vlan55	VLAN	1500	1594	

Below the table, the 'Interface <vlan52>' configuration window is open. A red box highlights the 'Name' field, which contains 'vlan52'. Another red box highlights the 'VLAN ID' field, which contains '52'. A third red box highlights the 'Interface' dropdown menu, which is set to 'ether5'. Other fields include 'Type: VLAN', 'MTU: 1500', 'Actual MTU: 1500', 'L2 MTU: 1594', 'MAC Address: E4:8D:8C:23:04:4F', 'ARP: enabled', and 'ARP Timeout'. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', and 'Torch'. At the bottom, there is a checkbox for 'Use Service Tag'.

Schritt 4: VLAN Interfaces in der Powerbox erstellen

Man macht hier nochmal das gleiche wie auf dem Hauptrouter, allerdings mit dem Unterschied, dass wir die VLAN Interfaces auf ether1 anlegen. Denn dieser Port ist die physikalische Verbindung zum RB2011 Hauptrouter.

The screenshot shows the 'Interface List' window with a table of interfaces. Below it, the configuration window for 'vlan52' is open, showing fields for Name, Type, MTU, Actual MTU, L2 MTU, MAC Address, ARP, and ARP Timeout. The 'VLAN ID' is set to 52 and the 'Interface' is set to ether1.

	Name	Type	Actual MTU	L2 MTU	Tx
R	ether1	Ethernet	1500	1598	
R	vlan52	VLAN	1500	1594	
R	vlan53	VLAN	1500	1594	
R	vlan54	VLAN	1500	1594	
R	vlan55	VLAN	1500	1594	

Interface <vlan52>

General | Loop Protect | Status | Traffic

Name: vlan52

Type: VLAN

MTU: 1500

Actual MTU: 1500

L2 MTU: 1594

MAC Address: E4:8D:8C:DF:BA:60

ARP: enabled

ARP Timeout:

VLAN ID: 52

Interface: ether1

Use Service Tag

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch

Nun sind die vier VLAN-Interfaces über das LAN-Kabel miteinander verbunden. Eine Verbindung zu den Geräten an der Powerbox besteht jedoch noch nicht.

Schritt 5: Bridges in der Powerbox erstellen

Für die Verbindung der VLAN-Interfaces mit den Ethernet Schnittstellen an der Powerbox verwendet man je zu verbindenden Port eine Bridge. Insgesamt werden vier Bridges erstellt. In jeder Bridge wird ein VLAN-Interface (z.B. VLAN55) mit dem passenden Ethernetanschluss (z.B. ether5) der Powerbox verbunden.

The screenshot shows the 'Bridge' window with a table of bridges. Below it, the configuration window for 'bridge-vlan55' is open, showing fields for Name, Type, and MTU.

	Name	Type	L2 MTU	Tx	Rx
R	bridge-vlan52	Bridge	1594	0 bps	
R	bridge-vlan53	Bridge	1594	0 bps	
R	bridge-vlan54	Bridge	1594	0 bps	
R	bridge-vlan55	Bridge	1594	0 bps	

Interface <bridge-vlan55>

General | STP | VLAN | Status | Traffic

Name: bridge-vlan55

Type: Bridge

MTU:

Buttons: OK, Cancel, Apply, Disable

The screenshot shows a network configuration window titled 'Bridge'. The 'Ports' tab is selected. Below the tabs is a toolbar with a '+' icon highlighted in red. A table lists bridge ports with columns for #, Interface, Bridge, Horizon, Trusted, Priority (h...), and Path. The table contains 8 rows, with the last row (7) highlighted in blue. Below the table is a dialog box for 'Bridge Port <vlan55>'. The 'General' tab is active. The 'Interface' dropdown is set to 'vlan55' and the 'Bridge' dropdown is set to 'bridge-vlan55', both highlighted with red boxes. Other fields include 'Horizon' (empty) and 'Learn' (set to 'auto'). Buttons for 'OK', 'Cancel', 'Apply', 'Disable', and 'Comment' are on the right.

#	Interface	Bridge	Horizon	Trusted	Priority (h...	Path
0	ether2	bridge-vlan52		no	80	
1	vlan52	bridge-vlan52		no	80	
2	ether3	bridge-vlan53		no	80	
3	vlan53	bridge-vlan53		no	80	
4	ether4	bridge-vlan54		no	80	
5	vlan54	bridge-vlan54		no	80	
6	ether5	bridge-vlan55		no	80	
7	vlan55	bridge-vlan55		no	80	

Die Ethernet Ports 2 bis 5 sind damit direkt mit dem Hauptrouter verbunden, bis hin zum dortigen VLAN-Interface.

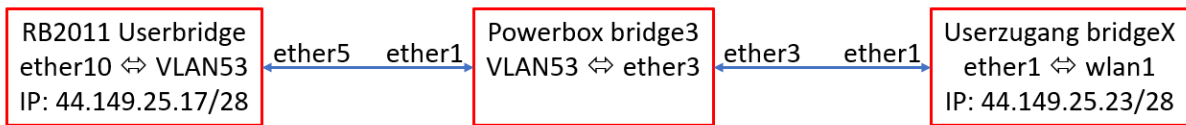
Schritt 6: Userzugang 2 verbinden

Der zweite Userzugang muss nun noch im Hauptrouter richtig verbunden werden. Die Antenne „endet“ noch im dortigen VLAN-Interface „VLAN53“. Dieses VLAN-Interface wird noch in die Userbridge mit aufgenommen und läuft damit parallel zum bestehenden Userzugang.

The screenshot shows a network configuration window titled 'Bridge'. The 'Ports' tab is selected. Below the tabs is a toolbar with a '+' icon highlighted in red. A table lists bridge ports with columns for #, Interface, Bridge, Horizon, Trusted, Priority (h...), and Path. The table contains 7 rows. Below the table is a dialog box for 'Bridge Port <vlan53>'. The 'General' tab is active. The 'Interface' dropdown is set to 'vlan53' and the 'Bridge' dropdown is set to 'userbridge', both highlighted with red boxes. Other fields include 'Horizon' (empty) and 'Learn' (set to 'auto'). Buttons for 'OK', 'Cancel', 'Apply', 'Disable', and 'Comment' are on the right.

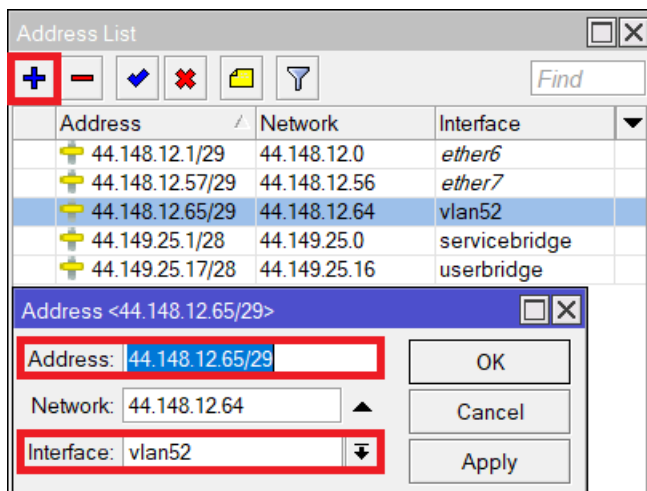
#	Interface	Bridge	Horizon	Trusted	Priority (h...	Path
0	ether1	servicebridge		no	80	
1	ether2	servicebridge		no	80	
2	ether3	servicebridge		no	80	
3	ether4	servicebridge		no	80	
4	ether5	servicebridge		no	80	
5	ether10	userbridge		no	80	
6	vlan53	userbridge		no	80	

Die Daten aus dem Userzugang 2 laufen dann über die Bridge in der Antenne in den Anschluss ether3 in der Powerbox. Ether3 ist dann wiederum über die Bridge in der Powerbox mit dem VLAN53 Interface verbunden, welches im Hauptrouter in der Userbridge landet.



Schritt 7: Neuen Link Nr. 3 einbinden

Für den neuen dritten Link muss noch eine IP-Konfiguration vorgenommen werden, da der Hauptrouter das Routing-Netzwerk noch nicht kennt. Wir legen deshalb einfach die Backbone-IP 44.148.12.65/29 des neuen Routing-Netzwerks auf das entsprechende VLAN-Interface „VLAN52“ im Hauptrouter.



Für den Link sind dann noch die BGP Routing Einstellungen vorzunehmen, dazu aber im nächsten Kapitel mehr.

Mit wenigen Schritten wurden nun die zwei neuen Geräte, welche an der Powerbox angeschlossen sind in den Hauptrouter integriert und es können sogar noch zwei weitere Geräte angeschlossen werden. Ein Limit ist nur die LAN-Verbindungsgeschwindigkeit der Ethernet-Schnittstelle. Also entweder 100 Mbit (PowerBox) oder 1 Gbit (PowerBox Pro).

Kleiner Hinweis: Wenn man eine Powerbox oder einen anderen PoE Switch verwendet und diese ebenfalls mit PoE versorgt, sollte unbedingt noch Kapitel 17 beachtet werden: PoE Stromversorgung einer Powerbox und ähnliche PoE Switches

12. Konfiguration BGP Routing

12.1. Begriffserklärungen

BGP (Border Gateway Protocol) ist ein Routingprotokoll für die OSI Layer Schicht 3. Es wird also IP basierend geroutet. Das (E)BGP wird im HAMNET dazu verwendet die einzelnen Autonomen Systeme (AS) zu verbinden.

Quelle: <http://www.amateurfunk-wiki.de/index.php/BGP>

Autonome Systeme (**AS**) sind logisch getrennte Netzwerkbereiche. Alle Netze im Internet werden in AS gruppiert und jeder Bereich bekommt eine AS-Nummer (ASN) fest zugeteilt. Es gibt aber in der Definition der AS-Nummern auch sogenannte private ASN: 64512 bis 65534.

Im AMPRNet wurde dann eine Verteilung über verschiedene Länder vorgenommen und für Deutschland wird der Bereich 64620 bis 64683 genutzt, d.h. es kann 64 "große" AS in DL geben. Innerhalb eines solchen AS kann es wieder kleine AS geben, die dann eine im HAMNET als privat deklarierte ASN zwischen 65510 bis 65534 haben kann. Man nennt dies auch eine Confederation.

Beispiel:

Im Bereich Südhessen, Mainz und Mittelhessen gibt es das AS DISTRIKT-F-640-AS mit der ASN 64640. Diese AS hat wiederum viele kleine AS wie DB0ZDF, DB0HRF, DB0ZAV usw. (um nur einige zu nennen) und diese haben die ASN 65520 bis 65531 in Benutzung. Fünfstellige private AS Nummern nennt man auch 16 Bit Nummern. In größeren AS werden aber auch bereits 32 Bit AS Nummern verwendet, welche 10-stellig sind. Die Konfiguration in einem 32bit AS ist etwas einfacher, mehr dazu weiter unten.

Quelle: <http://www.amateurfunk-wiki.de/index.php/AS>

12.2. Vorbereitungen

Zuerst sollte man sich eine Übersicht über die umgebenden AS verschaffen. Die Mitgliedschaft in einem AS sowie die eigene private AS Nummer ist aus der HamnetDB ersichtlich.

DB0DAH gehört zur AS 64647, dies ist die „Confederation“. Innerhalb der Confederation werden die privaten AS Nummern 65520 bis 65535 vergeben. DB0DAH hat die private AS Nummer 65533.

Da es zwei Linkstrecken gibt, müssen die Routinginformationen auch mit zwei Partnern ausgetauscht werden.

	DB0ZKA:	DB0TVM:
AS Nummer Confederation (Confederation)	64647	64625
AS Nummer privat (AS)	65534	65529
Privater AS Bereich (Confederation peers)	65520 – 65535	65520 - 65535

In Klammern ist jeweils die Feldbezeichnung in der WinBox angegeben, dies ist für die spätere Konfiguration wichtig.

Dieses Beispiel ist optimal, da es einen Linkpartner in der eigenen Confederation gibt (DB0ZKA), aber auch einen außerhalb der eigenen Confederation (DB0TVM). Es werden also beide Varianten behandelt.

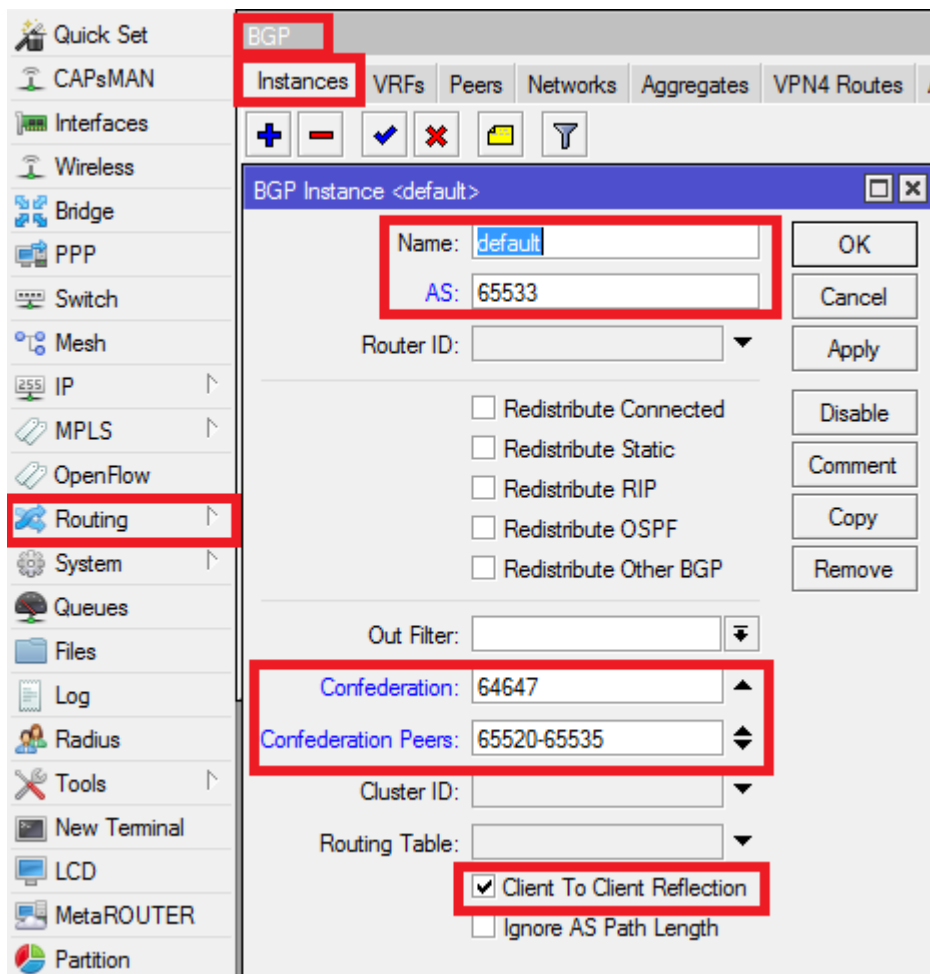
12.3. BGP Instanz (16 Bit) einrichten

12.3.1. 16 Bit BGB

ROUTING > BGP

Im Reiter Instances befindet sich bereits eine „default“ Instanz. Man kann entweder diese abändern oder eine neue erstellen.

Auf einem Hamnetknoten kann sich immer nur eine BGP Instanz befinden, unabhängig davon wie viele Linkpartner angeschlossen sind.



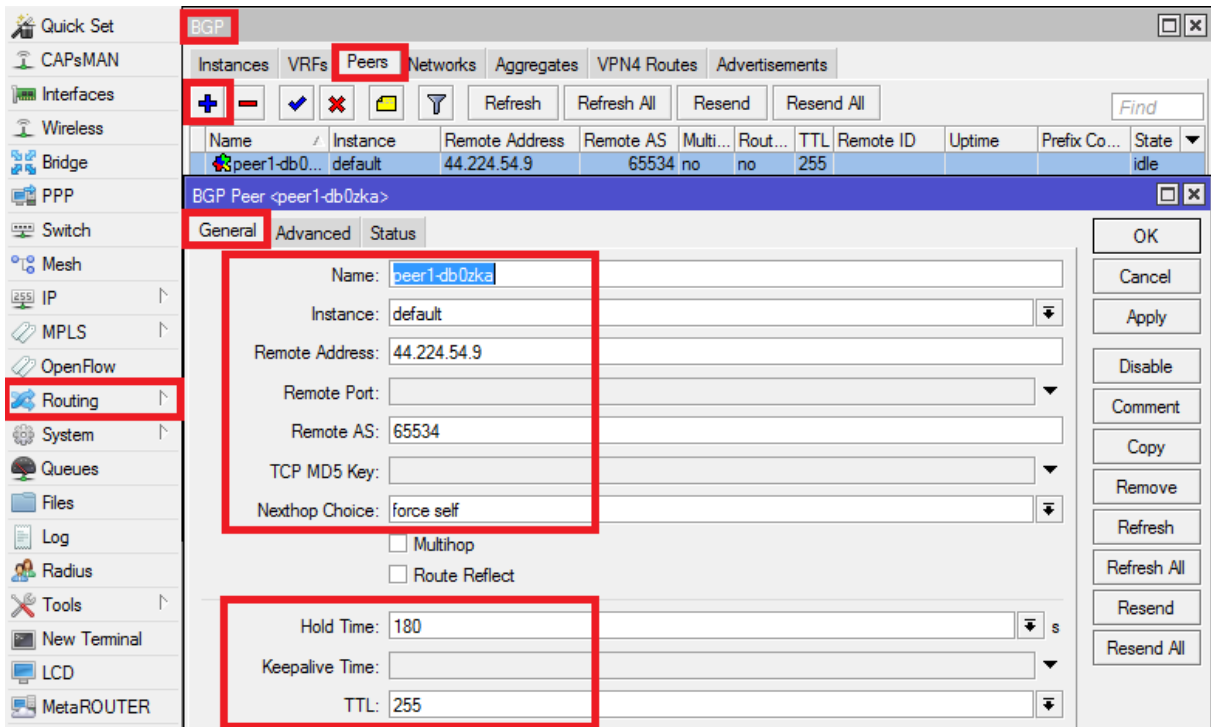
- Unter „Name“ steht der Name der Instanz, i.d.R. bleibt es bei „default“.
- Im Feld „AS“ steht die eigene private AS innerhalb der eigenen Confederation
- Unter „Confederation“ wird die AS Nummer der zugehörigen Confederation angegeben
- Unter „Confederation Peers“ wird der Bereich aller privaten AS Nummern der eigenen Confederation angegeben
- „Client to Client Reflection“ wird aktiviert

Alle anderen Eingabefelder oder Auswahlkästchen können leer bleiben.

12.3.2. Peers einrichten

Zu jedem physikalischen Linkpartner wird ein Peer eingerichtet. Über diesen Peer werden die Routinginformationen untereinander ausgetauscht.

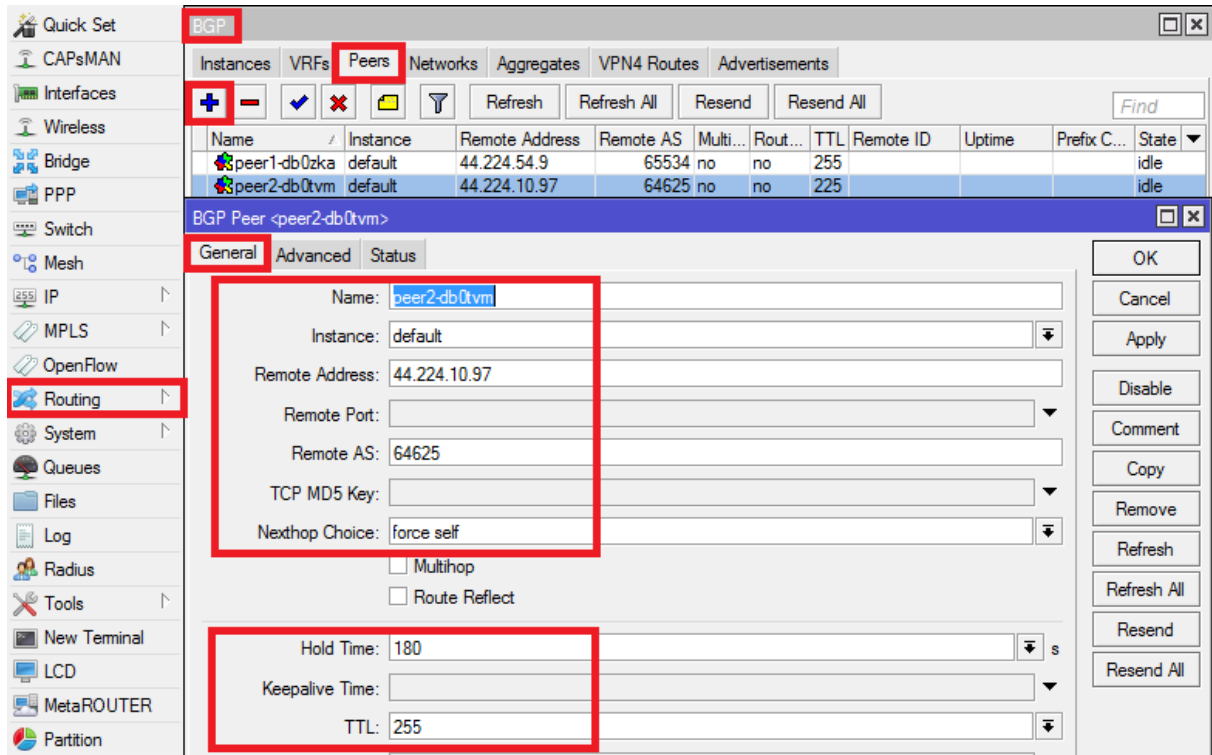
Peer Nummer 1 geht zu DB0ZKA:



- Unter „Name“ erhält der Peer einen eindeutigen Namen
- Unter „Instance“ muss die zuvor eingerichtete Instanz ausgewählt sein, i.d.R. „default“. Wurde vorher eine neue Instanz mit eigenem Namen erstellt, ist diese auszuwählen.
- „Remote Address“ ist die IP-Adresse, unter der wir den Linkpartner erreichen können (IP-Adresse aus dem Transfernetz)
- „Remote AS“ ist die AS Nummer des Linkpartners. Er gehört zu unserer eigenen Confederation, somit ist hier die private AS Nummer des Linkpartners einzutragen.
- Das Feld „Nexthop Choice“ wird auf „force self“ gestellt
- Die „Hold Time“ bleibt auf 180
- TTL wird auf 255 eingestellt

Alle anderen Felder bleiben leer.

Peer Nummer 2 geht zu DB0TVM:



Die Feldwerte werden analog zum Peer 1 eingetragen, allerdings mit einer Abweichung bei der „Remote AS“. Der Linkpartner DB0TVM gehört zu einer anderen Confederation. Daher wird hier die AS Nummer der Confederation des Linkpartners eingetragen.

Die Peers müssen immer auf beiden Knoten zueinander konfiguriert werden, damit sie aktiv werden. Hat ein Peer erfolgreich eine Verbindung zum Linkpartner aufgebaut, steht in der Peers-Übersicht der Status (State) auf „established“.

12.3.3. Eintragungen im Reiter „Networks“

Im Reiter Networks werden alle zu veröffentlichenden Subnetze eingetragen. Diese müssen zwangsweise lokal am Router anliegen. Z.B. Service- und Usernetze, aber auch die Transfernetze. Die Transfernetze werden bei beiden Linkpartner veröffentlicht. Diese Veröffentlichung geschieht HAMNET-weit. Alles was hier drin steht, wird an die Linkpartner weitergegeben, welche es wiederum an alle ihre Linkpartner mitteilen usw. Fehler verteilen sich somit im Ganzen HAMNET.

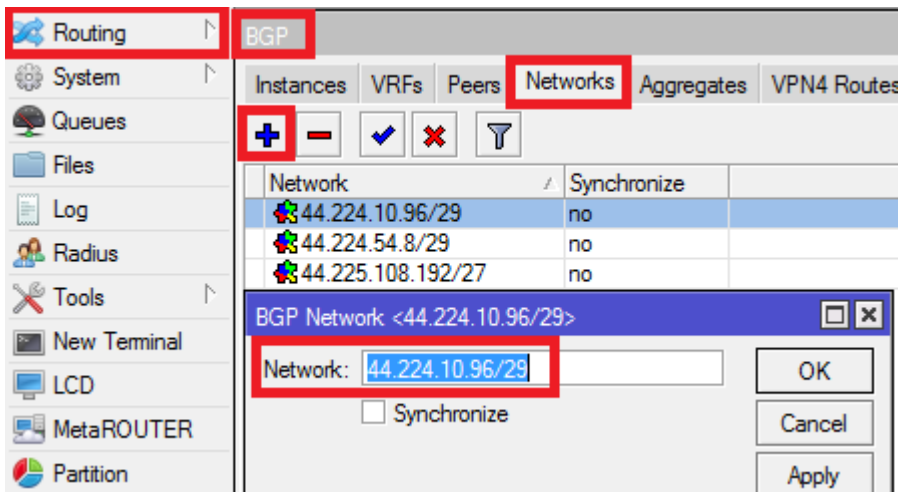
Wenn man ein Subnetz NICHT im Hamnet veröffentlichen möchte, darf es hier nicht eingetragen werden. Zu beachten ist, dass diese Liste nicht mit der Routing-Tabelle abgeglichen wird. Es sind also alle Subnetze hier nochmals einzutragen, sofern sie bekannt gemacht werden sollen.

Die Option „Synchronize“ dient lediglich dazu, den jeweiligen Networks Eintrag nochmal mit der eigenen Routing-Tabelle abzugleichen. Nur wenn ein Subnetz auch physikalisch erreichbar ist, wird dieses ggf. über BGP veröffentlicht. Viele Sysops aktivieren diese Option bei den Transfernetzen, zwingend notwendig ist es aber nicht.

Wenn man keinen Haken setzt, könnte man damit theoretisch „Geisternetze“ veröffentlichen. Man kann dies z.B. für Tests machen, um zu sehen ob die Verteilung der Routen korrekt funktioniert.

Bei DB0DAH werden folgende Netze veröffentlicht:

- 44.224.10.96/29 (Link zu DB0TVM)
- 44.224.54.8/29 (Link zu DB0ZKA)
- 44.225.108.192/27 (User- und Servicenetz)



12.4. BGP Instanz (32 Bit) einrichten

12.4.1. 32 bit BGP

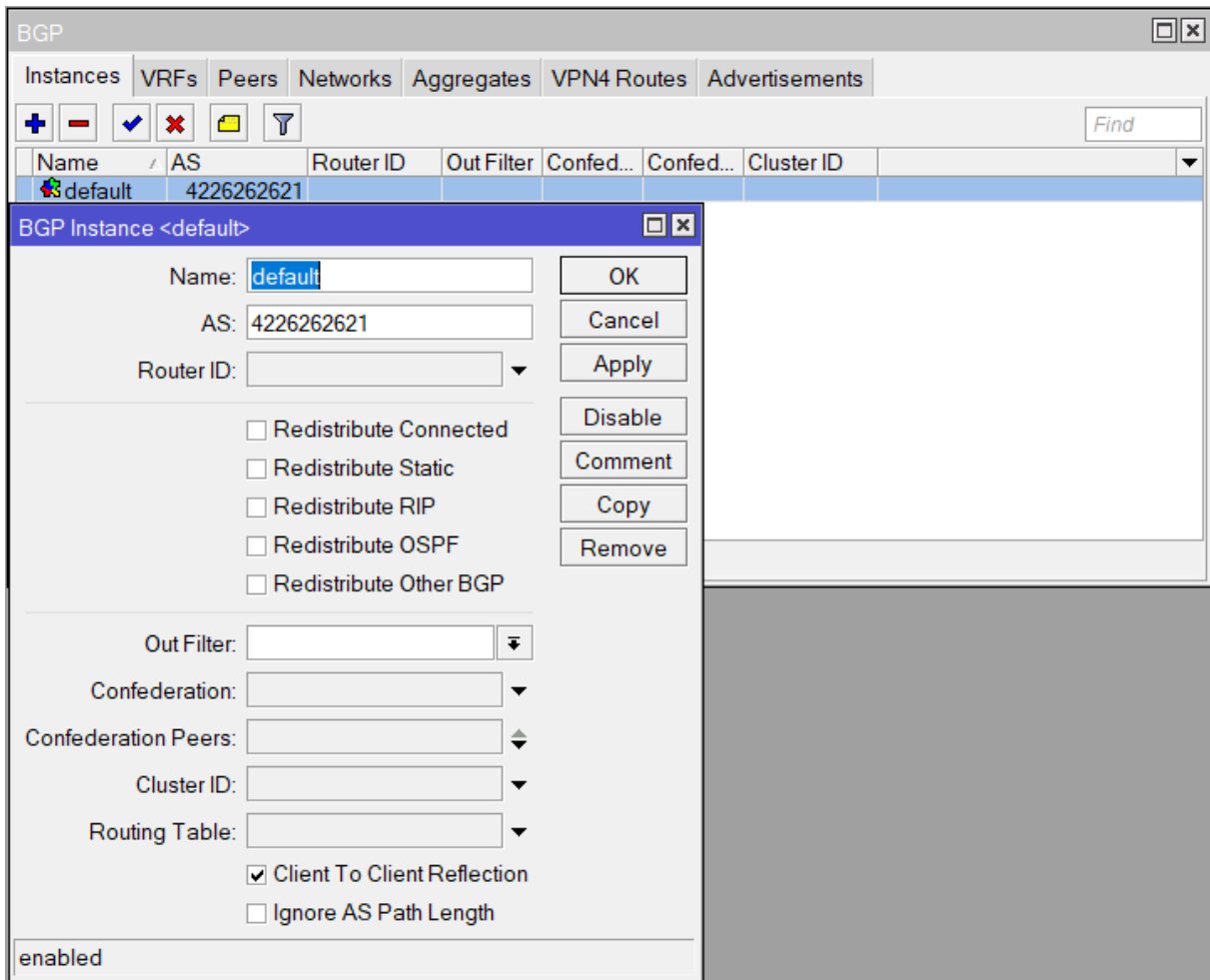
Die Unterschiede bei den 32 Bit Routingnetzen sind:

- Es gibt keine „Confederations“ mehr. Jeder Knoten hat seine eigene „externe“ AS Nummer und verbindet sich „direkt“ mit den Nachbar-AS
- 32 bit AS Nummern sind 10-stellig

Die 32 Bit Konfiguration wird anhand des Links DB0UC-DB0NU beschrieben.

ROUTING > BGP

Man passt sich am besten die „Default“-Instanz für seine Zwecke an:



- Unter „Name“ steht der Name der Instanz, i.d.R. bleibt es bei „default“.
- Im Feld „AS“ steht die eigene AS-Nummer
- „Client to Client Reflection“ wird aktiviert

12.4.2. Peers einrichten

The screenshot shows the BGP configuration interface. At the top, there are tabs for 'Instances', 'VRFs', 'Peers', 'Networks', 'Aggregates', 'VPN4 Routes', and 'Advertisements'. Below these are buttons for '+', '-', '✓', '✗', a folder icon, a filter icon, 'Refresh', 'Refresh All', 'Resend', and 'Resend All'. A 'Find' input field is also present.

Name	Instance	Remote Addr	Remote	M...	R...	T	Remote ID	Uptime	Prefix C...	State
peer-db0adb	default	44.224.12.169	42262664	no	no	d...	44.225.178.	5d 09:2...	1318	establi...
peer-db0nu	default	44.224.12.129	42262626	no	no	d...	44.225.26.97	10:57:56	403	establi...

Below the table is the 'BGP Peer <peer-db0nu>' configuration window. It has tabs for 'General', 'Advanced', and 'Status'. The 'General' tab is active, showing the following fields:

- Name: peer-db0nu
- Instance: default
- Remote Address: 44.224.12.129
- Remote Port: (empty)
- Remote AS: 4226262615
- TCP MD5 Key: (empty)
- Nexthop Choice: force self
- Multihop
- Route Reflect
- Hold Time: 180 s
- Keepalive Time: (empty)
- TTL: default
- Max Prefix Limit: (empty)
- Max Prefix Restart Time: (empty)
- In Filter: (empty)
- Out Filter: (empty)
- AllowAS In: (empty)
- Remove Private AS
- AS Override
- Default Originate: never
- Passive
- Use BFD

At the bottom of the window, there are two status indicators: 'enabled' and 'established'.

- Unter „Name“ erhält der Peer einen eindeutigen Namen
- Unter „Instance“ muss die zuvor eingerichtete Instanz ausgewählt sein, i.d.R. „default“. Wurde vorher eine neue Instanz mit eigenem Namen erstellt, ist diese auszuwählen.
- „Remote Address“ ist die IP-Adresse, unter der wir den Linkpartner erreichen können (IP-Adresse aus dem Transfernetz)
- „Remote AS“ ist die AS Nummer des Linkpartners
- Das Feld „Nexthop Choice“ wird auf „force self“ gestellt
- Die „Hold Time“ bleibt auf 180
- TTL bleibt auf „default“

Alle anderen Parameter bleiben wie sie sind.

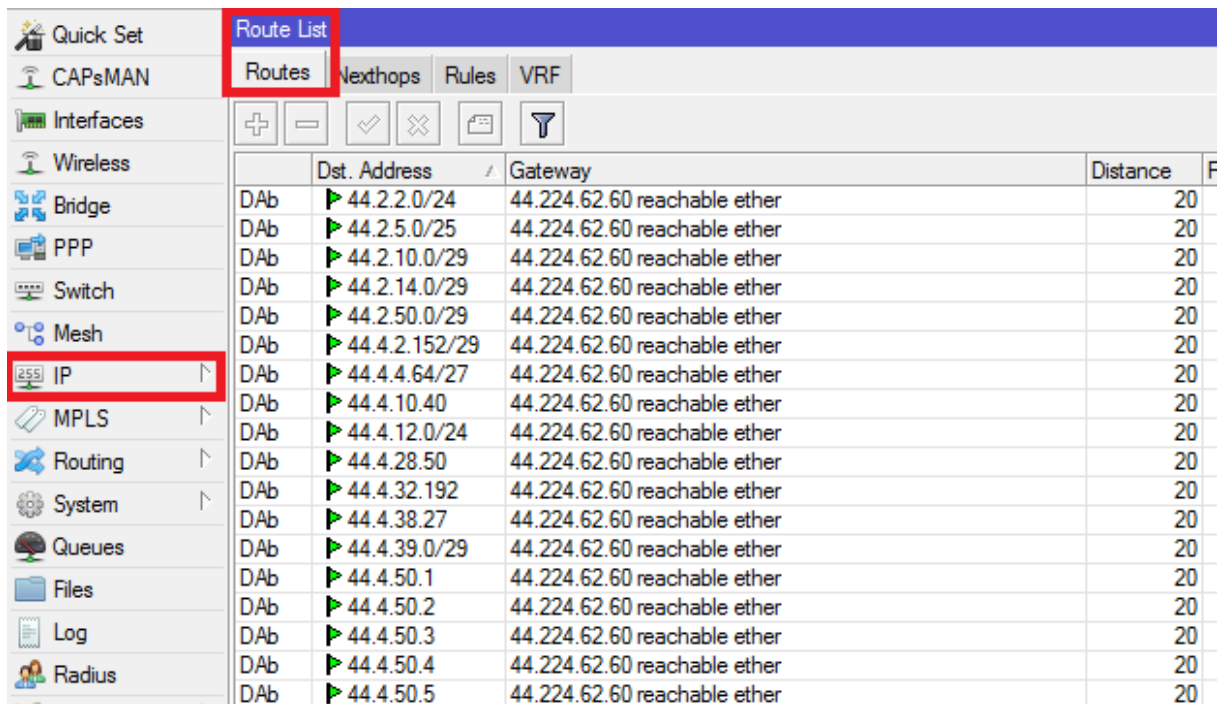
12.4.3. Eintragungen im Reiter „Networks“

Dies geschieht analog zur 16bit Variante, siehe Punkt 11.3.3

12.5. Kontrolle

IP > ROUTES

Mit einem Blick in die Routingtabelle kann man nun kontrollieren ob schon Routen von den Linkpartnern übermittelt wurden. Übermittelte Routen/Subnetze erkennt man am angehängten kleinen „b“ des Routentyps in der ersten Spalte. Das „b“ steht für „BGP“.



	Dst. Address	Gateway	Distance	F
DAb	▶ 44.2.2.0/24	44.224.62.60 reachable ether	20	
DAb	▶ 44.2.5.0/25	44.224.62.60 reachable ether	20	
DAb	▶ 44.2.10.0/29	44.224.62.60 reachable ether	20	
DAb	▶ 44.2.14.0/29	44.224.62.60 reachable ether	20	
DAb	▶ 44.2.50.0/29	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.2.152/29	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.4.64/27	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.10.40	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.12.0/24	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.28.50	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.32.192	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.38.27	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.39.0/29	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.50.1	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.50.2	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.50.3	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.50.4	44.224.62.60 reachable ether	20	
DAb	▶ 44.4.50.5	44.224.62.60 reachable ether	20	

PS: Der Screenshot stammt nicht von DB0DAH, sondern von einem anderen Knoten. Dürfte aber überall gleich aussehen.

Mehr zum BGP Routing findet man auch hier: <http://wiki.oevsv.at/images/d/da/BGPtb38.pdf>

13.Sende- und Strahlungsleistungen im Hamnet

Im Amateurfunk sind im 13, 9 und 6cm grundsätzlich 75 Watt Senderausgangsleistung erlaubt, was für den normalen OM völlig ausreichend ist. Leider gilt dies nicht für unbemannte automatische Stationen. Hier hat der Gesetzgeber eine Strahlungsleistung von 15 Watt ERP (entspricht 24,6 EIRP) als maximale Strahlungsleistung festgesetzt. Bei den hohen Antennengewinnen der WLAN-Antennen, kommt man daher schnell an die gesetzlichen Grenzen. Bei Hochgewinnantennen muss daher für den regelkonformen Betrieb die maximale Sendeleistung reduziert werden. Im Folgenden ist eine Tabelle, aus der man abhängig vom Antennengewinn (dBi) die maximale Sendeleistung (dBm) herauslesen kann, die für einen regelkonformen Amateurfunkbetrieb gilt. **Bei MIMO/dual-polarity Betrieb (also H und V gleichzeitig) ist darauf zu achten, dass sich diese Angaben auf die Summe beider Signale beziehen. Die Eingabe in RouterOS bezieht sich immer auf eine einzelne Chain, so dass der Eingabewert dann 3 dB unterhalb des Wertes in der Tabelle liegen muss.**

G Ant (dBi)	Hamnet			Beispielantennen
	P Out (dBm)	P Out (W)	P Out ERP	
2	42	15,849	15,3	
3	41	12,589	15,3	
4	40	10,000	15,3	
5	39	7,943	15,3	
6	38	6,310	15,3	
7	37	5,012	15,3	
8	36	3,981	15,3	Ubiquity Nanostation M2 Loco
9	35	3,162	15,3	
10	34	2,512	15,3	Mikrotik SXT2
11	33	1,995	15,3	Ubiquity Nanostation M2
12	32	1,585	15,3	
13	31	1,259	15,3	Ubiquity Nanostation M5 Loco
14	30	1,000	15,3	
15	29	0,794	15,3	
16	28	0,631	15,3	Ubiquity Nanostation M5, Mikrotik SXT5
17	27	0,501	15,3	
18	26	0,398	15,3	Mikrotik SEXTANT G
19	25	0,316	15,3	
20	24	0,251	15,3	
21	23	0,200	15,3	MikroTik Disc Lite5
22	22	0,158	15,3	Ubiquity Powerbeam M5-300
23	21	0,126	15,3	Mikrotik QRT5, Ubiquity Airgrid 5G23, Ubiquity Litebeam M5-23
24	20	0,100	15,3	Mikrotik Light Head Grid LHG5
25	19	0,079	15,3	Ubiquity Powerbeam M5-400
26	18	0,063	15,3	
27	17	0,050	15,3	Ubiquity Airgrid 5G27
28	16	0,040	15,3	
29	15	0,032	15,3	Ubiquity Powerbeam M5-620
30	14	0,025	15,3	Mikrotik mANT30

14. Sendebetrieb mit ISM Parametern

Manchmal kann es sinnvoll oder auch notwendig sein, auf HF Ebene mit ISM Parametern zu arbeiten.

14.1. Wann ist ISM Betrieb notwendig bzw. sinnvoll?

Vorteile und wann macht es Sinn?

- Kurze Strecken, die überbückt werden müssen (< 10 km)
- ISM Betrieb ist Anmelde- und Genehmigungsfrei (Keine Rufzeichenzuteilung notwendig)
- Höhere Bandbreiten als 5 bzw. 10 MHz möglich (20,40,80,160 MHz usw.) und dadurch höherer Datendurchsatz
- Weitere Frequenzen außerhalb des Amateurfunkspektrums nutzbar, falls 5 GHz Spektrum schon ausgeschöpft ist an einem Standort
- Klasse E Stationen in DL dürfen auf ISM Frequenzen senden und damit am Hamnet über HF teilnehmen. Seit 2017 ist in DL die Nutzung von 13cm und 6cm durch Inhaber der Klasse E geduldet, allerdings immer jährlich befristet. Eine dauerhafte Freigabe ist geplant.

Bekannte Nachteile:

- Geringere Reichweiten bedingt durch begrenzte Strahlungsleistung (max. 1000mW EIRP)
- Frequenzen werden mit anderen Teilnehmern geteilt, Störungen sind nicht ausgeschlossen
- Hierbei handelt es sich NICHT um Amateurfunk, da keine AFU Frequenzen benutzt werden!

Die Rahmenbedingungen müssen in jedem Fall eingehalten werden! Insbesondere ist im 5 GHz Bereich darauf zu achten, dass das Wetterradar um 5,6 GHz nicht gestört wird. Dafür müssen die Geräte die Radarerkennung unterstützen und bei Kollisionen einen automatischen Frequenzwechsel durchführen ([DFS - Dynamic Frequency Selection](#)). Auch „[Transmit Power Control \(TPC\)](#)“ müssen die 5 GHz Router unterstützen, damit die volle Strahlungsleistung von 1000mW EIRP benutzt werden darf. Das bedeutet, dass bei starken Signalen die Sendeleistung automatisch reduziert wird. Werden TPC und DFS nicht unterstützt, ist eine maximale Strahlungsleistung von 200mW (23 dBm) auf 5 GHz erlaubt. Fehlt nur TPC, darf 500mW abgestrahlt werden (27 dBm). Die Angabe der Sendeleistung in dBm bezieht sich dabei immer auf die Summe der Signale eines Senders, bei Dual-Polarity Betrieb also auf beide Signale („Total TX Power“). Diese liegt i.d.R. auch 3 dB höher als eingetragen (zumindest bei Mikrotik).

14.2. ISM Sendeparameter Allgemein

ISM Betrieb ist in Deutschland unter denen in der Norm ETSI EN 301 893 festgelegten Parametern möglich:

2,4 GHz:

2,3995 bis 2,4835 GHz mit maximal 100mW EIRP

5 GHz:

5,15 bis 5,25 GHz mit maximal 200mW EIRP in geschlossenen Räumen

5,25 bis 5,35 GHz mit maximal 200mW EIRP in geschlossenen Räumen und unter Beachtung von TPC und DFS.

5,47 bis 5,725 GHz mit maximal 1000mW EIRP in geschlossenen Räumen und im Freien und unter Beachtung von TPC und DFS. Ohne TPC sind nur 500mW EIRP erlaubt. Das Wetterradar auf 5,59 bis 5,65 MHz darf nicht gestört werden.

RouterOS von Mikrotik und AirOS von Ubiquity unterstützen beide kein TPC und regulieren ihre Strahlungsleistung daher automatisch auf 500mW EIRP.

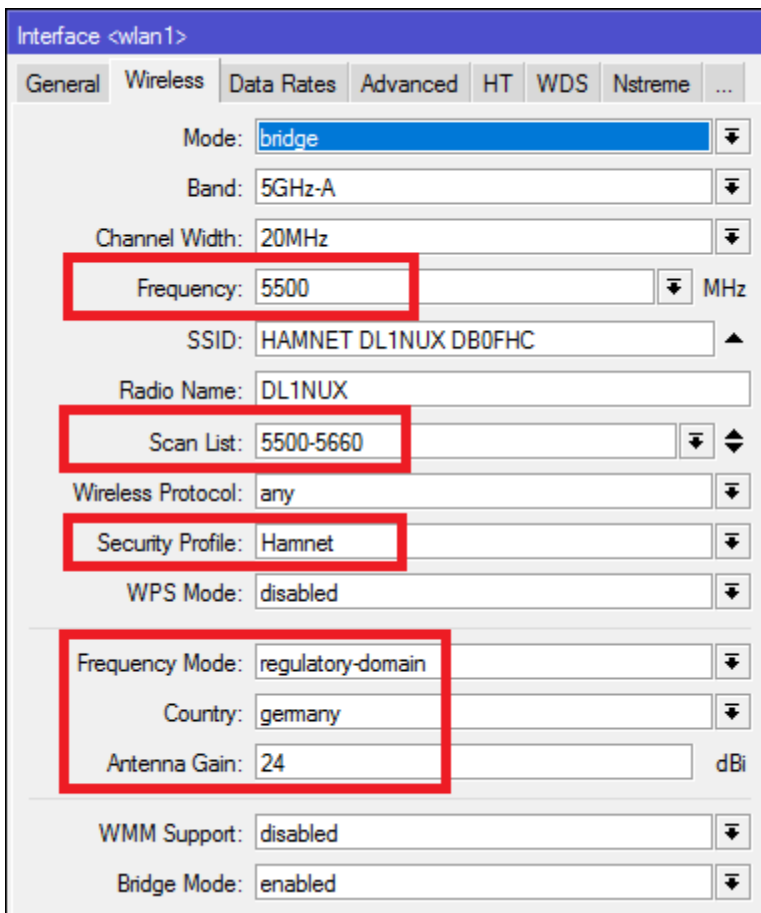
Bei Geräten, welche TPC unterstützen, kann folgende Tabelle zur Ermittlung der maximalen Sendeleistung (1000mW bzw. 1W) unter Beachtung des Antennengewinns herangezogen werden. Bei Geräten ohne TPC muss die Sendeleistung um weitere 3 dB reduziert werden, um 500mW nicht zu überschreiten. Bei MIMO natürlich wiederum um weitere 3 dB.

ISM			
G Ant (dBi)	P Out (dBm)	P Out (W)	P Out EIRP
0	30	1,0000	1,0
1	29	0,7943	1,0
2	28	0,6310	1,0
3	27	0,5012	1,0
4	26	0,3981	1,0
5	25	0,3162	1,0
6	24	0,2512	1,0
7	23	0,1995	1,0
8	22	0,1585	1,0
9	21	0,1259	1,0
10	20	0,1000	1,0
11	19	0,0794	1,0
12	18	0,0631	1,0
13	17	0,0501	1,0
14	16	0,0398	1,0
15	15	0,0316	1,0
16	14	0,0251	1,0
17	13	0,0200	1,0
18	12	0,0158	1,0
19	11	0,0126	1,0
20	10	0,0100	1,0
21	9	0,0079	1,0
22	8	0,0063	1,0
23	7	0,0050	1,0
24	6	0,0040	1,0
25	5	0,0032	1,0
26	4	0,0025	1,0
27	3	0,0020	1,0
28	2	0,0016	1,0
29	1	0,0013	1,0
30	0	0,0010	1,0

14.3. ISM Parameter bei Mikrotik RouterOS

Folgende Wireless-Parameter müssen bei Mikrotik RouterOS beachtet werden. Achtung, der folgende Screenshot zeigt RouterOS Version 6.37.2. auf einem „Light Head Grid LHG5“. Ab RouterOS Version 6.37 sind auf 5 GHz die DFS Einstellungen in der Übersicht verschwunden. Sie werden automatisch angewandt, sobald ein Land ausgewählt wird wo dies gefordert wird. Außerdem ist zu beachten, dass RouterOS kein TPC beherrscht, und daher die Strahlungsleistung automatisch auf 500mW (27 dBm) begrenzt. Wenn man 1000mw EIRP erreichen will, muss man die Sendeleistung manuell einstellen bzw. den eingetragenen Antennengewinn um 3 dB reduzieren (das wäre aber nicht mehr regelkonform).

- a) Frequency: Frequenz, auf der gesendet wird, falls kein Frequenzwechsel durch DFS angeordnet wird
- b) Scan List: Frequenzbereich von/bis, in dem die Frequenz gewechselt werden kann. Überschneidungen mit im Amateurfunk genutzten Frequenzen ab 5670 MHz sind zu vermeiden
- c) Security Profile: Im ISM Betrieb **darf und sollte auch verschlüsselt werden**, da sonst „Nachbarn“ das Netzwerk sehen und sich verbinden können
- d) Frequency Mode: Die Einstellung „regulatory-domain“ sorgt dafür, dass die Sendeleistung anhand des angegebenen Antennengewinns und den Gesetzen des ausgewählten Landes automatisch reduziert wird.
- e) Country: Das Land, indem wir uns befinden. Hier unbedingt nur „Germany“ auswählen. Die Länder „Germany 5.8...“ sind für kommerzielle [BFWA](#) Anwender vorgesehen, welche bei 5.8 GHz senden.
- f) Antenna Gain: Antennengewinn in dBi
- g) DFS Mode (nur bei Versionen bis 6.36.4): „radar detect“ aktiviert die Radarerkennung.



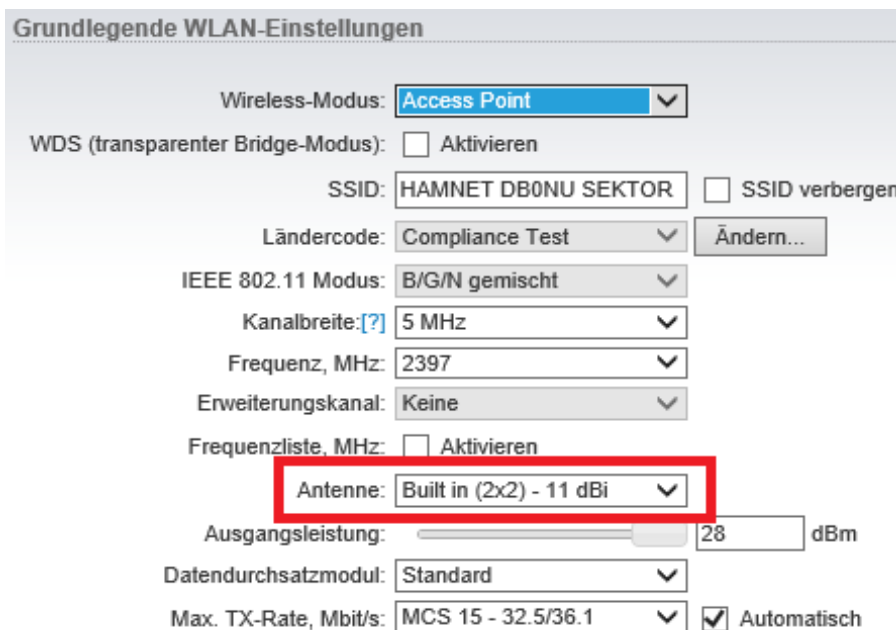
14.4. ISM Parameter bei Ubiquity AirOS V

Für den ISM Betrieb mit Ubiquity AirOS V muss bei der Ersteinrichtung nur das richtige Land ausgewählt werden.



Wenn man „Germany“ auswählt, werden die Sendeparameter gleich passend eingestellt. Weitere Einstellungen sind nicht mehr notwendig. Auch lässt sich die Sendeleistung nicht erhöhen, wenn dies die zulässige Strahlungsleistung überschreitet.

Je nach AirOS Version und verwendeter Antenne muss aber ggf. noch in den „Wireless“ Einstellungen der Antennentyp ausgewählt werden:



15.VPN Server (PPTP) einrichten

15.1. Voraussetzungen und IP-Einstellungen

Ein Hamnet-Standort mit Internetanbindung kann auch als VPN Server für die Einwahl von OMs über das Internet genutzt werden, wenn keine HF-Anbindung möglich ist.

- Ausreichend Download- und Upload-Bandbreite am Internetanschluss
- Ein entsprechend großes Subnetz für die Zuteilung von dynamischen IP-Adressen.
- Portweiterleitung am DSL-Router/Internetgateway für Port 1723 (TCP) zum Mikrotik Router im LAN (Portforwarding).
- Ggf. dyndns Domain einrichten, falls keine fixe öffentliche IPv4-Adresse am Internetanschluss vorhanden ist.

Folgendes Konfigurationsbeispiel (DB0TEST) wird für die folgende Anleitung vorausgesetzt:

Site-Network: 44.225.240.0/28 auf LAN3 (Nutzbare Adressen: x.1 bis x.14)

- 44.225.240.1 router.DB0TEST
- 44.225.240.2 hamserverpi.DB0TEST (Beispiel)

PPTP-Subnetz: 44.225.241.0/24 (Nutzbare Adressen: x.1 bis x.254)

- 44.225.241.1 pptp-gw.DB0TEST
- 44.225.241.2 bis x.254 PPTP DHCP Range

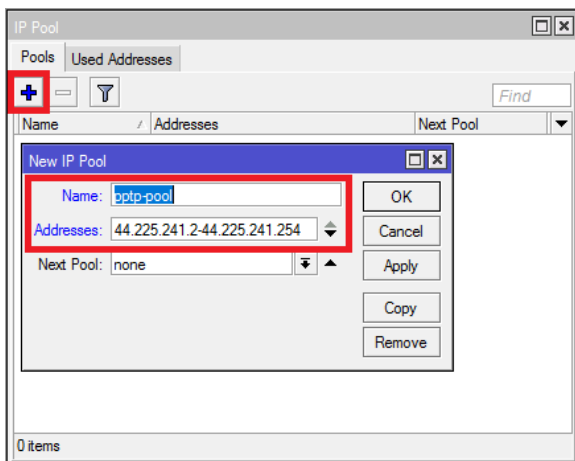
Internetzugang über LAN1

- 10.0.0.20/24 IP-Adresse am LAN1 Port
- 10.0.0.2 Internet Gateway & DNS-Server (z.B. FritzBox)

15.2. PPTP Server in RouterOS konfigurieren

Servicenetz mit Internetzugang wurden bereits konfiguriert, die Konfiguration wird nicht separat beschrieben.

a) Als erstes wird der Adresspool für die Adressvergabe der PPTP-Clients festgelegt

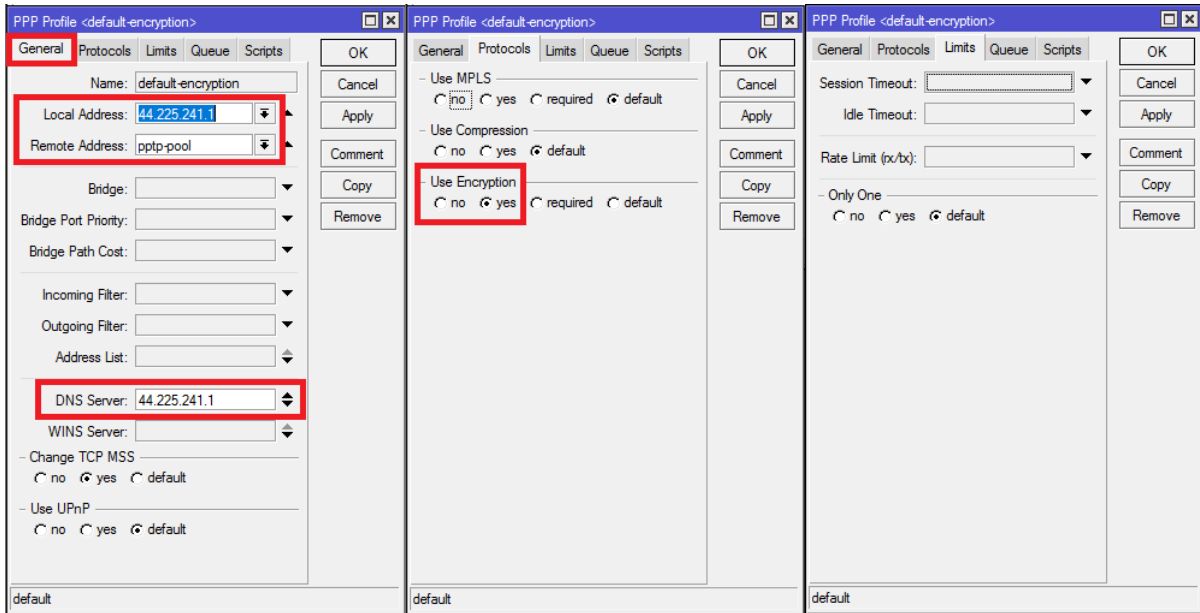


IP > IP Pool

- Definieren eines Namens für den Pool
- Eingabe der Adressen, die dynamisch vergeben werden sollen

b) Nun erstellt man ein PPP Profil

VPN Server (PPTP) einrichten

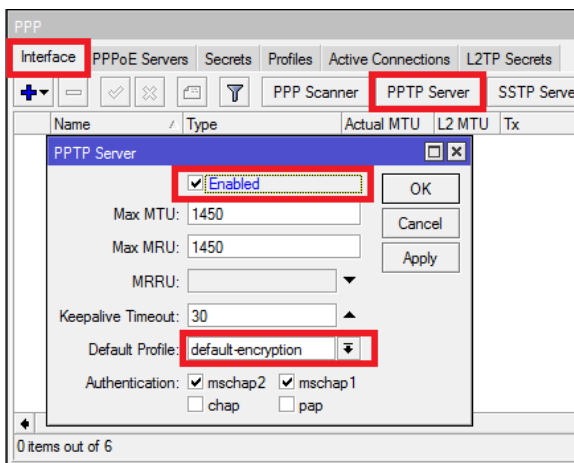


PPP > Profiles

Idealerweise modifiziert man eines der standardmäßig vorhandenen Profile, z.B. „default-encryption“, dann ist es grundsätzlich schon verschlüsselt.

- „Local Address“ bezeichnet die Gateway-Adresse des PPTP Servers, in der Regel also die erste nutzbare Adresse im PPTP Subnetz.
- Unter „Remote Address“ wählt man den entsprechenden IP Adresspool, der für PPTP Verbindungen vorgegeben wurde.
- Als „DNS-Server“ nimmt man wieder die IP Adresse des PPTP Servers
- Im Reiter „Protocols“ sollte „Use encryption“ auf „yes“ stehen, damit die Verbindung auch verschlüsselt wird.
- Im Reiter „Limits“ kann man optional ein Session Timeout oder auch eine Begrenzung der Dantentransferrate pro Client definieren.

c) Nun aktiviert man den PPTP Server

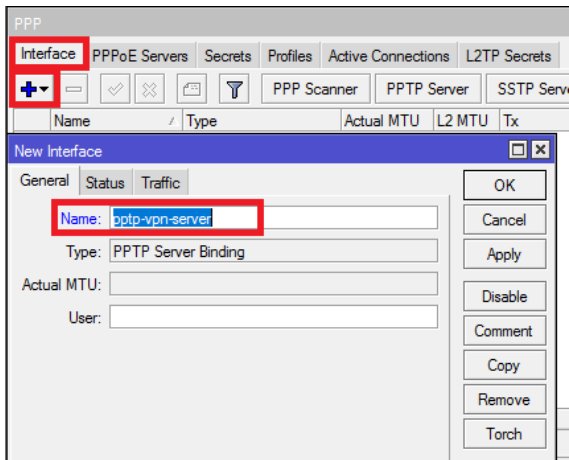


PPP > Interface > PPTP Server

- Den Haken bei „enabled“ setzen

- Unter „Default Profile“ das zuvor erstelle oder modifizierte Profil auswählen

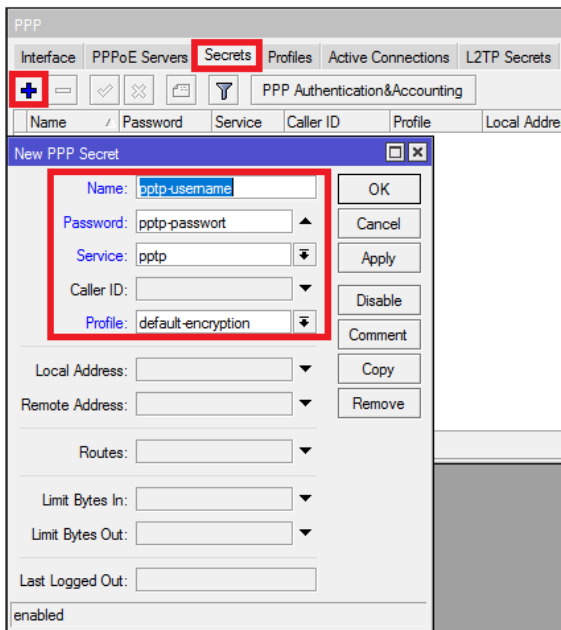
d) PPTP Interface einrichten



PPP > Interface

Damit nun das Ganze auch funktioniert, muss noch ein passendes Interface vom Typ „PPTP Server Binding“ erzeugt werden.

e) PPTP User anlegen



PPP > Secrets

Die Anlage der User erfolgt im „Secrets“ Abschnitt in den PPP Einstellungen.

- Angabe des Login-Namens unter „Name“
- Angabe des Login-Passworts unter „Password“
- Unter „Service“ wird „pptp“ ausgewählt
- Unter „Profile“ wird das passende Profil ausgewählt

16. Sonderfälle beim RSSI-Monitoring

In Kapitel 4 und 8 wurde erklärt, wie man das RSSI Monitoring für die HamnetDB aktiviert. Allerdings gibt es auch ein paar Sonderfälle, die einer genaueren Betrachtung bedürfen. Die Infos stammen direkt von der DL-IP-Koordination (Jann DG8NGN) und werden hier 1:1 übernommen.

Beim System „Mikrotik“ ist bereits eine Fehlerquelle identifiziert worden, die nur in wenigen Fällen auftritt. Dafür steht leider nur ein Workaround und keine Fehlerbehebung zur Verfügung. In diesem Fall ist nicht sichergestellt, dass SNMP-Anfragen an eine Ziel-IP-Adresse auch von dieser

Ziel-IP-Adresse wieder beantwortet werden. Das SNMP-Antwort-Paket wird bei jeder Anfrage neu generiert und im Standardfall als Quell-IP-Adresse diejenige verwendet, die zum Ziel in der Routing-Tabelle passt. Das Monitor-System kann keine zugehörige SNMP-Antwort erkennen und verwirft das Paket.

Beispiel Fall #1 (Linkdevice Point-to-Point-Link DB0ZB → DB0HHB):

Die Linkeinheit hat zwei IP-Adressen (1x Sitenetwork / 1x Backbone-Network) und hat die Defaultroute über das Sitenetwork gesetzt.

The screenshot shows two windows from Mikrotik WinBox. The top window is 'Address List' and the bottom is 'Route List'.

Address List		
Address	Network	Interface
44.224.64.52/29	44.224.64.48	bridge1
44.225.27.132/27	44.225.27.128	ether1

Route List					
Routes	Nexthops	Rules	VRF		
Dist. Address	Gateway	Distance	Routing Mark	Pref.	Source
AS 0.0.0.0/0	44.225.27.129 reachable ether1	1			
DAC 44.224.64.48/29	bridge1 reachable	0		44.224.64.52	
DAC 44.225.27.128/27	ether1 reachable	0		44.225.27.132	

Die SNMP-Anfrage an 44.224.64.52 wird in diesem Fall mit einer SNMP-Antwort von 44.225.27.132 beantwortet. Für diesen Fall kann ab RouterOS 6.40 die SNMP-Source-Address im Dialog „IP → SNMP“ händisch gesetzt werden (letzte Zeile):

The screenshot shows the 'SNMP Settings' dialog box. The 'Enabled' checkbox is checked. The 'Src. Address' field is set to 44.224.64.52.

Enabled	OK
Contact Info:	Cancel
Location:	Apply
Engine ID:	Communities
Trap Target:	
Trap Community: public	
Trap Version: 1	
Trap Generators:	
Trap Interfaces:	
Src. Address: 44.224.64.52	

Beispiel Fall #2 (Linkdevice Point-to-Multipoint-Link DB0ZB → DB0TAW/DB0UC):

Address List			
Address	Network	Interface	
44.224.12.42/29	44.224.12.40	bridge2	
44.224.12.154/29	44.224.12.152	bridge1	
44.225.27.131/27	44.225.27.128	ether1	

In diesem Fall muss die Linkeinheit die SNMP-Abfragen im Fall DB0ZB → DB0TAW mit der IP-Adresse 44.224.12.42 und im Fall DB0ZB → DB0UC mit der IP-Adresse 44.224.12.154 beantworten. Dies ist nur möglich, wenn man für beide abgehenden IP-Adresse eine eigene IP-Regel definiert.

Route List						
Routes						
#	Src. Address	Dst. Address	Routing Mark	Interface	Action	Table
0	44.224.12.154				lookup	Ink-db0uc
1	44.224.12.42				lookup	Ink-db0taw

Für den Fall, dass ein Paket mit der Source-IP-Adresse 44.224.12.154 abgeschickt werden soll, soll in die Routing-Tabelle „Ink-db0uc“ geschaut werden. Für den Fall, dass ein Paket mit der Source-IP-Adresse 44.224.12.42 abgeschickt werden soll, soll in die Routing-Tabelle „Ink-db0taw“ geschaut werden.

Die entsprechenden Default-Gateways sind für die einzelnen Source-IP-Adressen in der Routing-Tabelle definiert:

Route List						
Routes						
	Dst. Address	Gateway	Distance	Routing Mark	Pref.	Source
AS	0.0.0.0/0	44.225.27.129 reachable ether1	1			
AS	0.0.0.0/0	44.224.12.153 reachable bridge1	1	Ink-db0uc		
AS	0.0.0.0/0	44.224.12.41 reachable bridge2	1	Ink-db0taw		
DAC	44.224.12.40/29	bridge2 reachable	0			44.224.12.42
DAC	44.224.12.152/29	bridge1 reachable	0			44.224.12.154
DAC	44.225.27.128/27	ether1 reachable	0			44.225.27.131

Beispiel Fall #3 (Linkdevice und BGP-Router DB0ADB → DB0UC):

Contains the following hosts:

Host-IP	M	Hostname	Type	Site
44.224.12.169	●	bb-db0uc.db0adb	Routing-Radio	db0adb
44.224.12.173	●	Ink-db0adb.db0uc	Service	db0uc
44.224.12.174	●	bb-db0adb.db0uc	Routing-Radio	db0uc

3 entries.

Bei DB0ADB ist ein BGP-Router mit WLAN-Karten im Einsatz (keine spezielle Linkeinheit). Die Linkstrecke DB0ADB ↔ DB0UC hat also nur drei Hosts im Transfernetzwerk 44.224.12.168/29:

Im Falle von DB0ADB ist für 44.224.12.169 in der HamnetDB das Monitor-Flag zu setzen. Der Router DB0ADB hat aber mehrere Linkstrecken und es ist aufgrund von asynchronem Routing möglich, dass die Antwort zum Monitoring-Host über ein anderes Interface gehen kann als es empfangen wurde. Damit hat das Paket wieder eine falsche Source-IP-Adresse und wird vom Monitoring-System verworfen.

In diesem Fall hat es nur geholfen auf der richtigen Seite der Linkstrecke das /29-
Tranfernetzannouncement in den BGP-Networks zu deaktivieren (im Standardfall wird das
Tranfernetz von beiden Seiten announced).

Problematisch könnte sich eine Änderung in der Topologie auswirken.

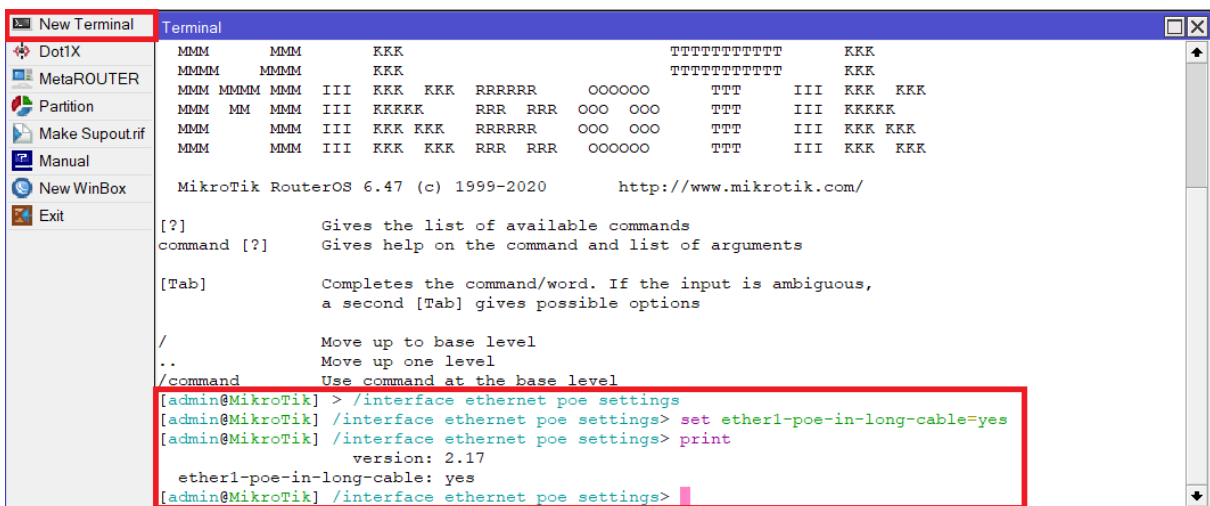
17. PoE Stromversorgung einer Powerbox und ähnliche PoE Switches

An dieser Stelle noch ein Hinweis zur Verwendung der Powerbox (Pro) oder anderen Geräten mit mehreren Anschlüssen, die per LAN-Kabel mit PoE versorgt werden und den Strom auch an mehrere angeschlossene Geräte weitergeben.

Mikrotik Geräte haben auf PoE Leitungen eine Kurzschlussprüfung, welche die PoE Stromversorgung deaktiviert, sollte ein Kurzschluss festgestellt werden. Leider löst auch die Kurzschlussprüfung aus, wenn ein langes Kabel zur PoE Versorgung auf ether1 genutzt wird. Dann werden die Geräte an den anderen Ports (ether2 bis 5 z.B.) nicht mehr mit Strom versorgt. Man wundert sich dann nur dass nichts funktioniert.

Dazu muss im betroffenen Gerät, z.B. die Powerbox, der PoE-long-cable-support eingeschaltet werden. Dadurch wird die Kurzschlussprüfung deaktiviert und die angeschlossenen Geräte zuverlässig mit Strom versorgt. Die Befehle können nur über die RouterOS Konsole oder per SSH eingegeben werden, in der grafischen Oberfläche in der WinBox oder WebFig gibt es dazu aktuell keine Möglichkeit mehr.

```
/interface ethernet poe settings  
Set ether1-poe-in-long-cable=yes
```



```
New Terminal Terminal
DotIX
MetaROUTER
Partition
Make Supoutrif
Manual
New WinBox
Exit

MMM   MMM   KKK   TTTTTTTTTT   KKK
MMMM  MMMM  KKK   TTTTTTTTTT   KKK
MMM MMMM MMM III KKK KKK RRRRRR   OOOOOO   TTT   III KKK KKK
MMM MM  MMM III KKKKK RRR RRR   OOO OOO   TTT   III KKKKK
MMM   MMM   III KKK KKK RRRRRR   OOO OOO   TTT   III KKK KKK
MMM   MMM   III KKK KKK RRR RRR   OOOOOO   TTT   III KKK KKK

MikroTik RouterOS 6.47 (c) 1999-2020      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]        Completes the command/word. If the input is ambiguous,
              a second [Tab] gives possible options

/            Move up to base level
..          Move up one level
/command    Use command at the base level

[admin@MikroTik] > /interface ethernet poe settings
[admin@MikroTik] /interface ethernet poe settings> set ether1-poe-in-long-cable=yes
[admin@MikroTik] /interface ethernet poe settings> print
              version: 2.17
ether1-poe-in-long-cable: yes
[admin@MikroTik] /interface ethernet poe settings>
```

Mit dem Befehl „print“ kann man kontrollieren, ob die Einstellung übernommen wurde.

Diese Einstellungen sind an allen Geräten möglich, welche mehrere PoE Ausgänge besitzen, z.B. Powerbox (Pro), HEX PoE (Lite), OmniTik PoE und ähnliche.