

Dreiländereck-Sysop-Treffen in Engen am 10. Februar 2024

Thomas Osterried DL9SAU

IP-Koordination DL



(c) 2024-02-10 Thomas Osterried DL9SAU <dl9sau@darc.de>

Version 1.00

License: CC-BY-SA

Weniger Vortrag, eher offene Fragerunde.

Folien hatte ich dieses mal keine; ich zeigte <https://vpn.hc.r1.ampr.org> und <https://www.de.ampr.org/hamnet/bgp-mikrotik> am Beamer

Dieses Dokument fasst v.a. die Rückmeldungen und Erkenntnisse zusammen.

Die Themen:

1. HAMNET-Tagung
 2. VPN in die HamCloud
 3. HamCloud-Dienste
 4. WiFi-Chips mit 10 MHz Bandbreite
 5. ROSv7
 - 5.1 pro/contra
 - 5.2 BGP-Konfiguration in ROSv7: was ist zu beachten
 - 5.3 Kompatibilität
 - 5.4 Diskussion
- Anhänge

1. HAMNET-Tagung

Interesse an einer HAMNET-Tagung ist gross.

Wir sollten 2025 ins Auge fassen. → Vorgemerkt: Planungen ab Herbst 2024. ;))

2. VPN in die HamCloud

Das VPN in die HamCloud (<https://vpn.hc.r1.ampr.org>) wurde von Jann, DG8NGN, letztes Jahr vorgestellt; es hatte gerade den Regelbetrieb aufgenommen.

Ich bat um feedback.

Anwesende: einige (aber nicht viele) Nutzer nutzen das VPN; sie hatten Probleme bei der Einrichtung.

Ein OM fragte, ob er von der RWTH wechseln müsse. → Nein, das dafür gibt es keinen Grund. Aachen ist ähnlich in der HamCloud verankert und verwendet ebenso einen entsprechenden IP-Adressraum.

Was unser VPN attraktiv macht ist der self-Service (initiale Autorisierung LotW-TLS-Zertifikat, oder DARC-Login).

3. HamCloud-Dienste

In Berlin haben wir seit ende 2023 immer wieder Probleme bei DMR (Brandmeister) und FM-funknetz zu deren Servern in der HamClpid. Die Verbindungsabbrüche und Sprachaussetzer konnten auch nach Umstellung auf einen dritten DSL-Anbieter (Uplink-Standort-Wechsel, zuletzt nur ein Hop entfernt, bei gutem HF-Link) nicht zufriedenstellend behoben werden..

Von den Anwesenden meinte ein OM, seit etwa seit 2 Monaten hatte er sowas auch schon bei seiner Brandmaster-Relaisverbindung festgestellt. Das würde sich in etwa mit unseren Erfahrungen decken. Wie man das Problem eingrenzen kann ist eine gute Frage, denn ping / mtr zeigten keine Auffälligkeiten.

→ Ggf. braucht es ein etwas aufwändigeres und permanentes Monitoring an Übergabe zur „Wolke“.

Artem (Brandmeister-Entwickler) schlug vor, man könne auch im Brandmeister-Webinterface für sein Relais mit dem Einstellungen für den jitterbuffer experimentieren.

Jann, DG8NGN, wies in einer Besprechung nochmal darauf hin, dass wir im HAMNET Nstreme (bei Mikrotik) bzw. AirMax (bei Ubiquiti) einschalten sollten. Damit arbeitet WiFi in festen Zeitslots, das Jitter minimiert. Siehe auch:

<https://help.mikrotik.com/docs/display/ROS/Wireless+Interface#WirelessInterface-Nstreme>

[Die Nstreme-Parameter sind die Vorgabe für den AP. Der Client muss nur Nstreme können, braucht aber nicht weiter eingestellt werden. Nstreme funktioniert nicht im Modus WDS]

4. WiFi-Chips mit 10 MHz Bandbreite

Jann, DG8NGN, meinte die Tage, dass es auch WiFi-Hardware mit 802.11ac (oder vielleicht sogar -ax) gäbe, die man auf 10 MHz Bandbreite einstellen könne.

→ Ich erwähnte dies und es gab eine Rückmeldung:

bei manchen Gräten läßt es sich im GUI sogar einstellen, dann funktioniert das WLAN aber nicht (oder sendet weiter mit 20 MHz Bandbreite?).

Ein anwesender OM meinte: Mikrotik's Dokumentation ist idR. Outdated, oder sie stimmt nicht (– das ist auch unsere Erfahrung). Er hat sich an Mikrotik gewendet, aber die Dokumentation wurde nicht verbessert. Vor einigen Jahren hatte sich auch Jann, DG8NGN, an Mikrotik gewendet (es wurden dann zumindest einige Angaben korrigiert).

Es kam die Frage auf, ob wir das selbst irgendwo dokumentieren.

Mein Vorschlag: im Wiki auf de.ampr.org.

Ich warb darum, das bei passender Gelegenheit zu testen:

Wer neue Geräte gerade einrichtet, könnte die 10-MHz-Bandbreitenfähigkeit testen, und so ergibt sich im Laufe der Zeit hoffentlich ein guter Gesamtüberblick der Produktpalette.

Am besten Rückmeldung an die IP-Koordination DL geben (damit richtig getestet ist und die genaue Beschreibung von WiFi-Chip und Hardware/Software-Version vor liegt; insbesondere auch, weil mit RouterOS 7.13.x noch eine weiterer Faktor hinzu, der evtl. wieder Unterschiede bringt).

Von Jann, DG8NGN, erfuhr ich nach der Tagung:

Der „Dyna Dish 5“ ist ac-fähig, **kann** aber mit 10 MHz betrieben werden (dann natürlich mit 802.11n).

Davon abgesehen: werden zwei benachbarte Frequenzen beantragt (wird auch genehmigt), stellt sich die 10 MHz-Frage nicht mehr vordringlich (außer bei Nutzerzugängen).

Auch erwähnte ich, dass man die Frequenz doppelt belegen kann

(vert. + horiz. == MIMO) → 4-fache Übertragungsrate.

Allerdings: es gibt schon Gegenden wo dadurch keine freien Frequenzen mehr verfügbar sind.

Später im persönlichen Gespräch meinte ein OM, dass er Tests mit 802.11ac gemacht hat, und seiner Meinung nach der Link schlechter lief als unter 802.11n.

Ich meinte, er könne das ggf. testen ohne Hardware umzubauen, indem er die Karte auf 802.11n einstellt und vergleicht.

Bei 802.11ac (und noch mehr bei 802.11ax) wurde gem. der Standard das „guard-interval“ optimiert, und die Komplexität der Modulation erhöht (n-QAM).

Die max. Bitraten eines Streams gingen mit jedem neuen Standard stets etwas höher:

von 54 MBit auf 58.5 (n und ac) auf 77.4 MBit

[Da sich max-QAM von 64 auf 256 erhöhte und auch die coding rate von 3/4 auf 5/6 sich änderte (und guard-interval 0.4us nur bei 802.11n zu finden ist), vergleiche ich im Beispiel nur 64-QAM mit GI 0.8us bei CR 3/4]

[Nachgelesen:

The default guard interval is 0.8 microseconds.

However, 802.11ax extended the maximum available guard interval to 3.2 microseconds, in order to support Outdoor communications, where the maximum possible propagation delay is larger compared to Indoor environments.

Und: GI 0.4us gab es nur in 802.11n und 802.11ac. Ab 802.11ax: GI 0.8us, 1.6us und 3.2us. Demzufolge sollten 802.11ax-Geräte für stabilere Links sorgen]

5. ROSv7

5.1 pro/contra

Das Interesse an ROSv7 ist gross.

Benötigt wird es aber nur für neue features wie „wireguard“-VPN, oder bei neuer Hardware welche nicht mehr unter ROSv6 läuft.

Ansonsten gibt es aber keinen zwingenden Grund für ein Update von ROSv6 auf ROSv7, weil es nach wie vor supported ist (inkl. Sicherheitsupdates).

Unsere Empfehlung ist nach wie vor, bei ROSv6 zu bleiben.

Ein anwesender warnte: seit ROSv7.13 Mikrotik ist der WLAN-Treiber optional (weil Mikrotik RAM-Verbrauch sparen mussten für ältere Geräte).

Wer also seine Linkeinheit unbedingt auf diese Version oder neuer upgraden will, ist gut beraten, einen Ethernet-Weg zum Gerät zu haben, falls die Installation des WiFi-Treibers schief läuft ;) Vermutlich kommen deshalb neuere firmwares nicht mehr automatisch (automatische updates gehen nur bis zur Version-vor-7.13), sondern nur wenn man es manuell anschiebt.

Siehe [Anhang 1](#).

5.2 BGP-Konfiguration in ROSv7: was ist zu beachten

Eine Übersicht zu den Konfigurationsunterschieden für BGP in ROSv6 gegenüber ROSv7 haben wir zusammengestellt.

Unsere Mikrotik-Beschreibung zu BGP ROSv7:

<https://www.de.ampr.org/hamnet/bgp-mikrotik>

Der Text auf unserer Wiki-Seite beschreibt die Unterschiede detailliert und vollständig. Eine Migration von ROSv6 zu ROSv7 sollte deshalb keine große Herausforderung sein.

Das mit ROSv7 eingeführte *bgp-template* ist seit einigen ROSv7-Versionen nicht mehr nötig.

Damit wird die Konfiguration überschaubarer – aber auch fehlerträchtiger, z.B. wenn man sich bei dann für jedes peer anzugebene „own-AS“ vertippt.

Wir werden unsere Beschreibung im Wiki aktualisieren.

An dieser Stelle noch der u.E. wichtige Hinweis:

„routentables klein halten“

Bei ROSv6 konnte man sein /27 (auch wenn man es in mehrere Unternetze aufteilte) mit routing bgp network add network=.... synchronize=no en-block annoucen.

ROsv7 announced nur noch aktive Routen. Deshalb muß man das Netz als Blackhole-Route konfigurieren.

Details sie im Konfigurationsbeispiel in [Anhang 2](#).

5.3 Kompatibilität

Ich berichtete von einem BGP-Problem zwischen zwei Knoten in Berlin, wo das ROSv7-System Routen, welche von einem ROSv6-Partner gelernt wurden, zwar zu einem anderen Linkpartner weiterleitete, aber aus der eigenen Routing-Table entfernte (!) → er wurde zum blackhole. Reboot tat gut.

5.4 Diskussion

Es kam wieder mal die Frage auf weshalb wir heute noch ROSv6 empfehlen?

Irgendwann hat man doch ein altes System das nicht mehr updated wird. Ich sagte ROSv7 hatte lange Zeit immer wieder neue bugs. Zudem gibt es für ROSv6 immer noch Sicherheitsupdates.

Manche berichteten von Stabilitätsproblemen mit dem WLAN-Treiber.

Ferner erwähnte ich, dass ich wegen „[wireguard](#)“-VPN-testen einen alten rb750 upgradete. In den ersten ROSv7-Versionen war die CPU-Last > 100% und die Kiste rebootete ständig mangels RAM. Das Gerät ist auch heute noch nicht so performant und stabil wie unter ROSv6.

Eine Auffälligkeit sah ich neulich, dass eine BGP-Session bei ROSv7 deutlich mehr Daten überträgt. Das sieht man in ROSv7 in den Details der laufenden Session zum Peer.

Anhang 1

Automatische Updates nur bis vor ROS v7.13

<https://mikrotik.com/download/changelogs>

Release 7.13.3

2024-01-25

Notice - Starting from RouterOS version 7.13, significant changes have been made to the RouterOS wireless packages. This is done due to a new product development which will require more disk space for hardware drivers so we had to split it in order to maintain old products alongside the new ones. More wireless packages are yet to come.

1. When upgrading by using "check-for-updates", all versions earlier than 7.12 will display 7.12 as the latest available version. Upgrade from v7.12 to v7.13 or later versions must be done through 7.12 in order to convert wireless packages automatically. Fresh installation with Netinstall or manual package installation works in the same manner as always

[...]

3. The existing "wifivave2" package has been divided into distinct packages: "wifi-qcom" and "wifi-qcom-ac", and the necessary utilities for WiFi management are now included in the RouterOS bundle. RouterOS and "wifi-qcom-ac" packages alongside each other now fit into 16MB flash memory.

Anhang 2

BGP Beispiel mit ROSv7 ohne Verwenden eines “templates“.
Own-AS und die seit ROSv7 wichtige **blackhole-Route** (denn ROSv7 announced nur aktive Routen) sind **fett** markiert.

Unterstrichen markiert ist das in der adress-list angegebene user/services-Netz 44.149.76.128/27, das en-block (ungeachtet lokaler Unterteilungen wie 44.149.76.129/28 für das service-Netz und 44.149.76.145/28 für das user-Netz) announced wird, weil dank der Blackhole-Route eine Route (also ein exakt-match, das /27) existiert.

Beachte auch den Notations-Unterschied in /routing bgp connection:

„as“: .xxx ist ein Subvariable, der die auf die zuvor verwendete (hier remote, durch remote.address) bezieht → .as an dieser Stelle läßt sich auch als „remote.as“ schreiben.

Wer Sub-Variablen verwendet, muß die Reihenfolge einhalten. Ein Umstellen zu as=4226263904 .as=4226263902 wäre **falsch!**

```
/interface bridge port
add bridge=bridge-service interface=ether5
add bridge=bridge-service interface=ether6
add bridge=bridge-service interface=ether7
add bridge=bridge-user interface=ether4
add bridge=bridge-service interface=ether1
add bridge=bridge-service interface=sfp-sfpplus1
add bridge=bridge-service interface=ether3
/ip address
add address=44.148.38.57/29 interface=ether2 network=44.148.38.56
add address=44.148.38.121/29 interface=ether8 network=44.148.38.120
add address=44.149.76.129/28 interface=bridge-service network=44.149.76.128
add address=44.149.76.145/28 interface=bridge-user network=44.149.76.144
/ip dhcp-server network
add address=44.149.76.128/28 dns-server=44.149.76.129 gateway=44.149.76.129
add address=44.149.76.144/28 dns-server=44.149.76.145 gateway=44.149.76.145
/ip dns
set allow-remote-requests=yes servers=44.149.28.10,8.8.8.8
/ip firewall address-list
add address=44.149.76.128/27 list=bgp-advertise
add address=44.148.38.120/29 list=bgp-advertise
add address=44.148.38.56/29 list=bgp-advertise
/ip route
add blackhole disabled=no dst-address=44.149.76.128/27 gateway="" \
routing-table=main suppress-hw-offload=no
add check-gateway=ping disabled=no distance=1 dst-address=0.0.0.0/0 gateway=\
44.148.38.126 pref-src="" routing-table=main scope=30 \
suppress-hw-offload=no target-scope=10 vrf-interface=ether8
/routing bgp connection
add as=4226263904 disabled=no local.role=ebgp name=DB0W0 nexthop-choice=\
force-self output.network=bgp-advertise remote.address=44.148.38.126 .as=\
4226263901
add as=4226263904 disabled=no local.role=ebgp name=DB0EMS nexthop-choice=\
force-self output.network=bgp-advertise remote.address=44.148.38.62 .as=\
4226263902
```