

Пакети Wireless и WiFi, CAPsMAN

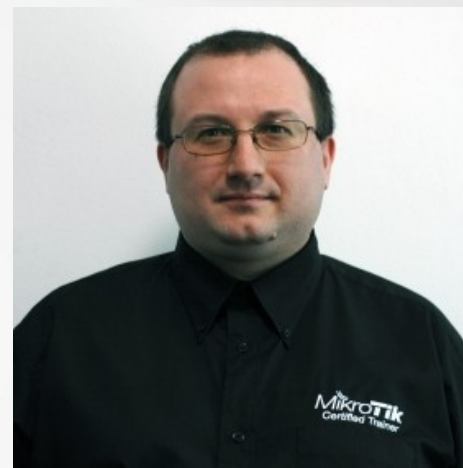
MikroTik Net Camp 2024, гр. Смолян

Съдържание

- Имало едно време (ретроспекция)
- Текущо състояние по отношение на безжичната функционалност
- Пакети wireless и wifi, сравнение
- Съществени разлики при CAPsMAN в двата пакета
- Съществени разлики и особености при CAP с различните пакети
- Демонстрация на CAPsMAN и CAP

За мен - Петър Димитров

- MikroTik Trainer: от 2013 г.
- Предлагани обучения:
 - Въведение в компютърните мрежи
 - Мониторинг с The Dude
 - MTCNA, MTCSWE, MTCRE, MTCINE, MTCWE, MTCEWE, MTCTCE, MTCUME, MTCSE, MTCIPv6E



Имало едно време (ретроспекция)

- Преди много, много години, имало един пакет wireless и всичко било много просто.
- Един прекрасен мартенски ден в далечната 2014-та година MikroTik пуснали RouterOS v6.11, където за първи път имало CAPsMAN и в този ден всички станали много щастливи.
- Не след дълго (още в края на същата 2014-та година) в RouterOS v6.22 се появил нов и по-добър CAPsMAN v2, който бил несъвместим с CAPsMAN v1, та... пакетите станали два: wireless (с CAPsMAN v1) и wireless-cm2 (с CAPsMAN v2)

Имало едно време (ретроспекция)

- В някакъв момент (Април 2016-та) дошло време и за по-нови драйвери за Atheros чиповете и в RouterOS v6.35 се появил нов пакет - wireless-rep (а името дошло от repeater, тази зла мисъл, прокрадваща се в умовете на някои човеци, вече била осъществима с новите драйвери) и... пакетите станали три :)
- Това сложно състояние не продължило дълго - още същата есен 2016-та MikroTik решили да върнат хармонията в света на хората и обявили, че от RouterOS v6.37 ще има само един пакет wireless (това бил всъщност наследника на wireless-rep, с новите драйвери и CAPsMAN v2, а CAPsMAN v1 окончателно бил забравен)

Имало едно време (ретроспекция)

- И ето че пак всичко било много просто, имало един пакет wireless и всички били (почти) щастливи.
- Защо почти? Защото хората са любопитни, виждат 802.11ac wave2 функционалността и се чудят - чиповете я поддържат, кога ще я имаме?
- Времето минавало, нищо не се случвало, някои се отказали, други ставали нетърпеливи.
- Докато един декемврийски ден през 2021-ва най-накрая дошъл Единорога - официално излязъл RouterOS v7.1 stable! И с него освен пакета wireless се появил изцяло нов, с нови драйвери и възможности, с нова логика и нова конфигурация пакет wifiwave2... и пакетите пак станали два

И в наши дни:

- До края на 2023-та пакетите wireless и wifivave2 съдържаха безжичната функционалност и драйвери за чиповете.
 - Пакета wireless нямаше развитие от години
 - Драйвери за 802.11ax (WiFi6) чиповете логично имаше само във wifivave2
 - Някои функционалности бяха несъвместими между двата пакета
 - Пакета wifivave2 можеше да се ползва само с новите ax чипове и с две и половина устройства от старите (Audience, hAP ac³ и RB4011iGS+5HacQ2HnD-IN)

И в наши дни:

- Голямата промяна настъпи в RouterOS v7.13 (Декември 2023 г.):
 - пакета wireless вече не е част от комбинирания пакет routeros
 - пакета wifivave2 се разделя на две части
 - пакет wifi, осигуряващ безжична функционалност, включително CAPsMAN, който вече е част от комбинирания пакет routeros (за почти всички архитектури)
 - отделни пакети, осигуряващи драйвери за различни чипове, за употреба с пакета wifi

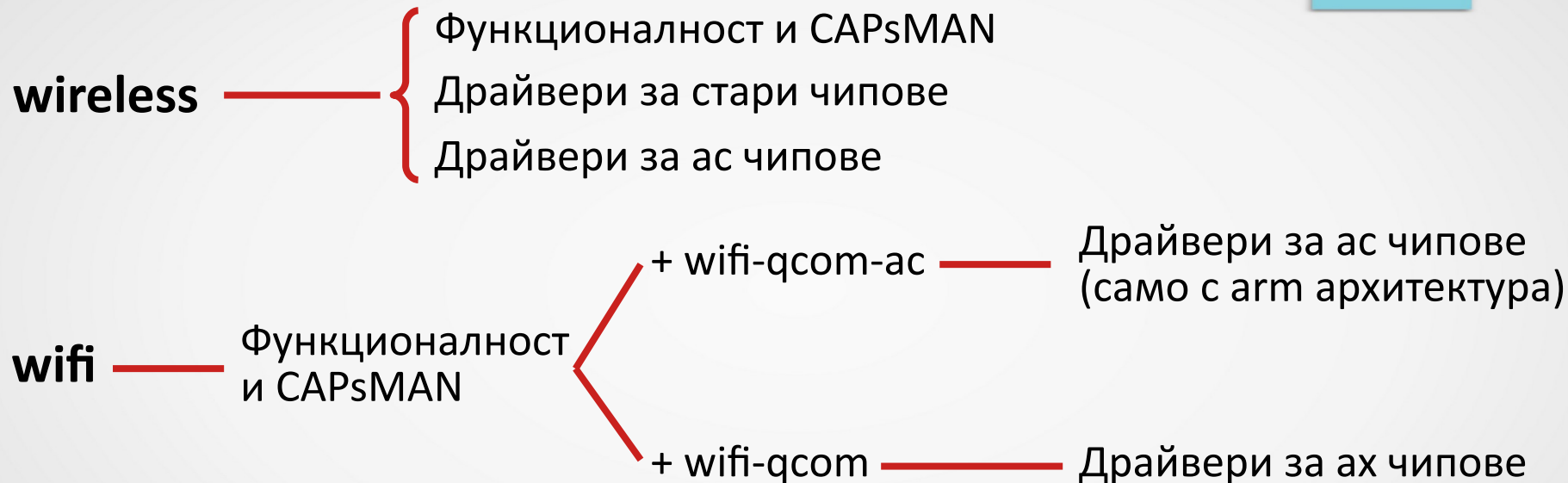
RouterOS пакет wireless

- Стария пакет за поддръжка на безжична функционалност
- Поддържа a, b, g, n и ac wave 1 функционалност, 60GHz (ad/ay)
- Поддържа режими с пренос на 4 MAC адреса, позволяващи прозрачен wireless bridge, **не са съвместими с пакет wifi**
- Може да се използва с всички по-стари безжични карти - без поддръжка на ax (WiFi6)
- **CAPsMAN и CAP функционалностите от този пакет не са съвместими с тези от пакет wifi**

RouterOS пакет wifi

- Поддържа a, g, n, ac (wave 1 и wave 2) и ah функционалност
- Поддържа режим с пренос на 4 MAC адреса (station-bridge), позволяващ прозрачен wireless bridge, **не е съвместим с пакет wireless**
- Пакета wifi съдържа само функционалност и контролер. За поддръжка на локални физически интерфейси допълнително се качва пакет с подходящи (в зависимост от чипа) драйвери.
- **CAPsMAN и CAP функционалностите от този пакет не са съвместими с тези от пакет wireless**

RouterOS пакети за безжични мрежи



Пакета **wifi** е част от **routeros** (комбинирания пакет). При добавяне на пакет **wireless** разполагаме с двете функционалности/двата CAPsMAN-а едновременно, т. е. една машина може да работи като двата контролера.

Сравнение на пакети wireless и wifi

	пакет wireless	пакет wifi
поддържани чипове	всичко преди 802.11ax	802.11ac с ARM архитектура, всички нови (ax) чипове
автентикация	open, WPA/WPA2 PSK/EAP	open, OWE, WPA/WPA2/WPA3 PSK/EAP, WPA3 EAP 192
криптиране	TKIP, AES CCM	TKIP, AES CCMP/GCMP/CCMP 256/GCMP 256
Management Protection	собствена (между RouterOS у-ва)	стандартна 802.11w
802.11ac wave2 функционалност	липсва	MU-MIMO, beamforming
MikroTik протоколи	Nstreme, Nv2	липсват
Механизми за fast roaming / steering	липсват	802.11r, 802.11k, 802.11v

Съществени разлики при CAPsMAN

- При пакета wireless данните от безжичните мрежи могат както да останат за обработка локално в CAP-а, така и да бъдат пренесени протоколно до CAPsMAN, докато при пакета wifi данните могат единствено да останат за обработка локално в CAP-а
- При пакета wireless CAPsMAN може да управлява локални физически интерфейси, докато при пакета wifi CAPsMAN НЕ управлява локални интерфейси (има начин локалните интерфейси да подлежат на правилата за провизиране, но не чрез CAP)
- При пакета wireless настройките (каналы, security, ...) и registration table са отделни за CAPsMAN и за локалните интерфейси, при пакета wifi настройките са едни и могат да се ползват за всичко

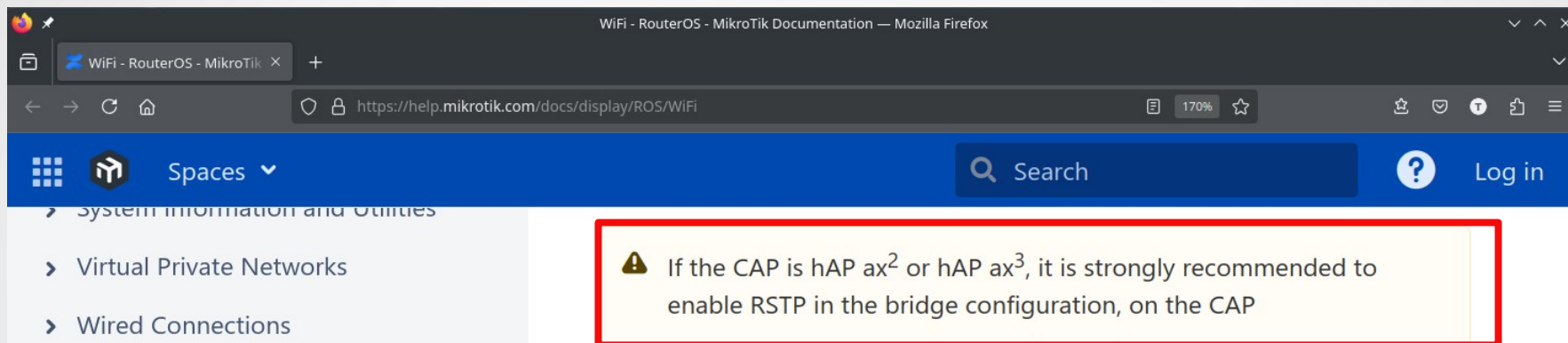
Съществени разлики при CAP

- При пакета wireless на CAP се указва bridge, в който влизат физическите и виртуалните интерфейси, докато при пакета wifi на CAP се указва slaves-datarath, който се прилага само за виртуалните интерфейси
 - Същия или друг datarath можем да укажем и на физическите интерфейси, ако искаме да използваме еднакъв datarath, достатъчно е да се укаже на физическите интерфейси, виртуалните го наследяват
- При пакета wireless на CAP се указва кои интерфейси се предоставят на CAPsMAN, докато при пакета wifi на всеки интерфейс се указва configuration.manager
 - configuration.manager=capsman-or-local позволява активиране на локалната конфигурация на интерфейса при липса на връзка с CAPsMAN

Особености при CAP

- AC чиповете, използващи пакета `wifi + wifi-qcom-ac`, не поддържат работа с VLAN-и директно чрез безжичния интерфейс, което не позволява провизиране на конфигурации с VLAN-и
- За заобикаляне на ограничението се създават и провизират конфигурации без VLAN-и, като на CAP
 - се указва `slaves-static=yes`
 - `bridge-a` се конфигурира с `vlan-filtering`
 - ръчно се добавят безжичните интерфейси със съответните `rvid` като портове на `bridge-a`

Особености при CAP



- За какво ли става въпрос тук, защо се препоръчва RSTP?
- А ако не сте с тези устройства, а ползвате сАР ах?

Особености при CAP

- Отговори на въпросите от предния слайд:
 - MikroTik имат проблем с използваните суич чипове в някои устройства, така че **ако имате Hardware Offload, дори само на ether1, няма да работите коректно с VLAN-и**
 - (R)STP не се поддържа и изключва Hardware Offload
 - Същото се отнася за vlan-filtering
 - Или просто изключват Hardware Offload на порта (hw=no)
 - Това важи с пълна сила и за CAP ах



Следва демонстрация на конфигуриране на
CAPsMAN на пакети wireless и wifi и
конфигурация на CAP с пакети
wireless, wifi + wifi-qcom и wifi + wifi-qcom-ac



Обобщение

Въпроси



Благодаря за вниманието!

Допълнение: използвани конфигурации



- На CAPsMAN:

```
/interface ethernet
set [ find default-name=ether1 ] name=ether1-trunk
set [ find default-name=ether2 ] name=ether2-inet
/interface vlan
add interface=ether1-trunk name=vlan10-mgmt vlan-id=10
add interface=ether1-trunk name=vlan20-corp vlan-id=20
add interface=ether1-trunk name=vlan30-guest vlan-id=30
/ip dhcp-client
add interface=ether2-inet
/ip firewall nat
add action=masquerade chain=srcnat comment="Masquerade traffic to Internet" \
  out-interface=ether2-inet
```

Допълнение: използвани конфигурации



```
/ip address
add address=10.10.10.254/24 interface=vlan10-mgmt network=10.10.10.0
add address=10.10.20.254/24 interface=vlan20-corp network=10.10.20.0
add address=10.10.30.254/24 interface=vlan30-guest network=10.10.30.0
/ip pool
add name=dhcp_pool-mgmt ranges=10.10.10.101-10.10.10.200
add name=dhcp_pool-corp ranges=10.10.20.101-10.10.20.200
add name=dhcp_pool-guest ranges=10.10.30.101-10.10.30.200
/ip dhcp-server
add address-pool=dhcp_pool-mgmt interface=vlan10-mgmt lease-time=2h name=dhcp-mgmt
add address-pool=dhcp_pool-corp interface=vlan20-corp lease-time=2h name=dhcp-corp
add address-pool=dhcp_pool-guest interface=vlan30-guest lease-time=2h name=dhcp-guest
/ip dhcp-server network
add address=10.10.10.0/24 caps-manager=10.10.10.254 comment=mgmt dns-server=\
    8.8.8.8,1.1.1.1 gateway=10.10.10.254
add address=10.10.20.0/24 comment=corp dns-server=8.8.8.8,1.1.1.1 gateway=10.10.20.254
add address=10.10.30.0/24 comment=guest dns-server=8.8.8.8,1.1.1.1 gateway=10.10.30.254
```

Допълнение: използвани конфигурации



```
/caps-man datapath
add client-to-client-forwarding=yes local-forwarding=yes name=datapath-corp \
    vlan-id=20 vlan-mode=use-tag
add local-forwarding=yes name=datapath-guest vlan-id=30 vlan-mode=use-tag
/caps-man security
add authentication-types=wpa2-psk name=security-corp passphrase=*****
add name=security-guest
/caps-man configuration
add datapath=datapath-corp mode=ap name=cfg-corp security=security-corp ssid=\
    corp-old
add datapath=datapath-guest mode=ap name=cfg-guest security=security-guest \
    ssid=guest-old
/caps-man provisioning
add action=create-dynamic-enabled master-configuration=cfg-corp name-format=\
    identity slave-configurations=cfg-guest
/caps-man manager set enabled=yes
```

Допълнение: използвани конфигурации



```
/interface wifi datapath
add disabled=no name=datapath-corp vlan-id=20
add client-isolation=yes disabled=no name=datapath-guest vlan-id=30
add disabled=no name=datapath-corp-ac
add client-isolation=yes disabled=no name=datapath-guest-ac
/interface wifi security
add authentication-types=wpa2-psk,wpa3-psk disabled=no ft=yes ft-over-ds=yes \
  name=sec-corp passphrase=*****
add disabled=no ft=yes ft-over-ds=yes name=sec-guest
/interface wifi configuration
add country=Bulgaria datapath=datapath-corp disabled=no mode=ap name=\
  cfg-corp-ax security=sec-corp ssid=corp
add datapath=datapath-guest disabled=no mode=ap name=cfg-guest-ax security=\
  sec-guest ssid=guest
```


Допълнение: използвани конфигурации



```
add country=Bulgaria datapath=datapath-corp-ac disabled=no mode=ap name=\
  cfg-corp-ac security=sec-corp ssid=corp
add datapath=datapath-guest-ac disabled=no mode=ap name=cfg-guest-ac \
  security=sec-guest ssid=guest
/interface wifi provisioning
add action=create-dynamic-enabled disabled=no master-configuration=\
  cfg-corp-ax name-format=%I slave-configurations=cfg-guest-ax \
  supported-bands=5ghz-ax
add action=create-dynamic-enabled disabled=no master-configuration=\
  cfg-corp-ax name-format=%I slave-configurations=cfg-guest-ax \
  supported-bands=2ghz-ax
add action=create-dynamic-enabled disabled=no master-configuration=\
  cfg-corp-ac name-format=%I slave-configurations=cfg-guest-ac
/interface wifi capsman set enabled=yes
```

Допълнение: използвани конфигурации



- На CAP с пакет wireless:

```
/interface bridge
add name=bridge-all protocol-mode=none
/interface bridge port
add bridge=bridge-all interface=ether1
/interface vlan
add interface=bridge-all name=vlan10-mgmt vlan-id=10
/ip dhcp-client add interface=vlan10-mgmt
/interface wireless cap
set bridge=bridge-all enabled=yes interfaces=wlan1,wlan2
```



- На CAP с пакет wifi-qcom-ac:

```
/interface bridge
add name=bridge-all protocol-mode=none vlan-filtering=yes
/interface vlan
add interface=bridge-all name=vlan10-mgmt vlan-id=10
/ip dhcp-client add interface=vlan10-mgmt
/interface wifi
set [ find default-name=wifi1 ] configuration.manager=capsman disabled=no
set [ find default-name=wifi2 ] configuration.manager=capsman disabled=no
add configuration.mode=ap disabled=no master-interface=wifi1 name=wifi3
add configuration.mode=ap disabled=no master-interface=wifi2 name=wifi4
```

Допълнение: използвани конфигурации



```
/interface bridge port
add bridge=bridge-all interface=ether1
add bridge=bridge-all frame-types=admit-only-untagged-and-priority-tagged \
  interface=wifi1 pvid=20
add bridge=bridge-all frame-types=admit-only-untagged-and-priority-tagged \
  interface=wifi2 pvid=20
add bridge=bridge-all frame-types=admit-only-untagged-and-priority-tagged \
  interface=wifi3 pvid=30
add bridge=bridge-all frame-types=admit-only-untagged-and-priority-tagged \
  interface=wifi4 pvid=30
/interface bridge vlan
add bridge=bridge-all comment=mgmt tagged=ether1,bridge-all vlan-ids=10
add bridge=bridge-all comment=corp tagged=ether1 vlan-ids=20
add bridge=bridge-all comment=guest tagged=ether1 vlan-ids=30
/interface wifi cap set enabled=yes slaves-static=yes
```

Допълнение: използвани конфигурации



- На CAP с пакет wifi-qcom:

```
/interface bridge add name=bridge-all protocol-mode=none
/interface vlan add interface=bridge-all name=vlan10-mgmt vlan-id=10
/interface bridge port add bridge=bridge-all hw=no interface=ether1
/ip dhcp-client add interface=vlan10-mgmt
/interface wifi datapath add bridge=bridge-all disabled=no name=dp-all
/interface wifi
set [ find default-name=wifi1 ] configuration.manager=capsman datapath=dp-all disabled=no
set [ find default-name=wifi2 ] configuration.manager=capsman datapath=dp-all disabled=no
/interface wifi cap set enabled=yes slaves-datapath=dp-all
(понеже datapath е същия като на физическите интерфейси, може да се наследи от тях,
при което е достатъчно /interface wifi cap set enabled=yes)
```