



Какво ново от MikroTik

MikroTik Net Camp 2018

Троян

Петър Димитров

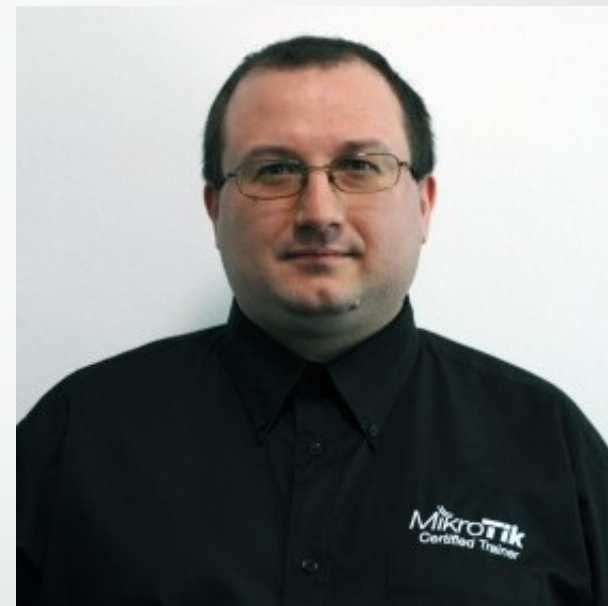
За мен:

- ❖ Име: Петър Димитров
- ❖ MikroTik Trainer: от 2013 г.
- ❖ Ubiquiti Trainer: от 2018 г.
- ❖ Предлагани обучения:

Въведение в компютърните мрежи

MTCNA, MTCWE, MTCRE, MTCTSE, MTCUME, MTCIPv6E, MTCINE

UBWS, UBWA, UBRSS, UBRSA, UEWA



Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO

RouterOS

ПОСЛЕДНИ ПРОМЕНИ

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO

Лято 2015 - Лято 2016

- ❖ Cloud Hosted Router (CHR)
- ❖ Възобновена поддръжка на The Dude
- ❖ Нова безжична функционалност с wireless-rep
- ❖ Промени във firewall

Cloud Hosted Router (CHR)

- ❖ От RouterOS 6.31 има нова версия на RouterOS, предназначена за работа като виртуален рутер
- ❖ CHR е 64-битов, с поддръжка на специфичен за виртуалните среди хардуер
- ❖ Различен модел на лицензиране - без ограничения на брой връзки и функционалност, но с различен лимит за изходящ трафик през интерфейс

The Dude

- ❖ Софтуер за наблюдение на мрежата, разработен от MikroTik. Предоставя множество уникални възможности за управление на RouterOS устройства
- ❖ Работата по The Dude е възобновена от RouterOS 6.34
- ❖ Сървъра работи на RouterOS (CCR, ARM, MMIBS, CHR или x86)
- ❖ Клиента работи под Windows (също под Linux и OS X с Wine)

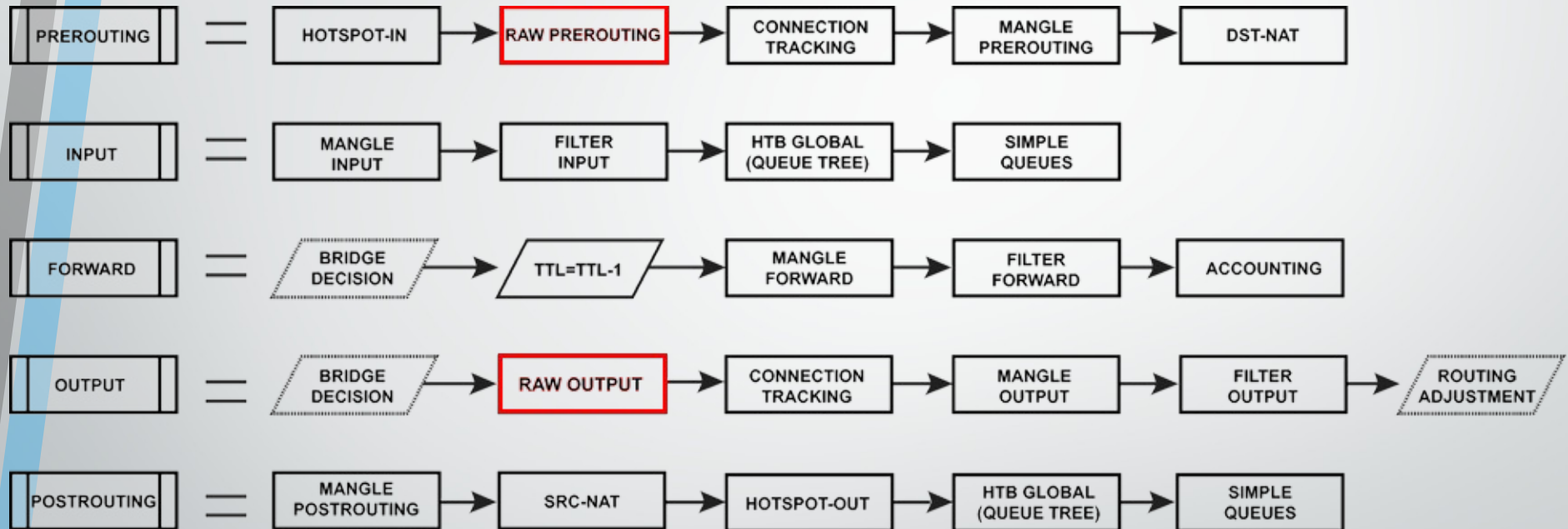
wireless-rep (от RouterOS 6.35)

- ❖ Виртуални безжични интерфейси включително и в режим station, създаване на wireless repeater
- ❖ Инструмента scan поддържа фонов режим (802.11 protocol), поддържа rounds и записване на резултата във файл
- ❖ Поддръжка на roaming в режим station (802.11 protocol). Поддръжка на клиент за wps. Поддръжка на указване на стъпка в scan-list

Промени във firewall

- ❖ Нова таблица "raw" (от RouterOS 6.36) - филтри преди пакетите да стигнат до системата за проследяване на връзките (Connection Tracking)
- ❖ Веригите по подразбиране са две - prerouting и output
- ❖ Няма условия, зависещи от Connection Tracking
- ❖ Може значително да намали натоварването на рутера

Промени във firewall



Промени във firewall

- ❖ Ново меню `/interface list` (от RouterOS 6.36) за групиране на интерфейси, което да улесни работата с firewall и други
- ❖ Нови условия `In Interface List` и `Out Interface List` (от RouterOS 6.36), позволяващи задаване на условия по група интерфейси, дефинирана в `/interface list` (подобно на `Src/Dst Address List`)

Други промени

- ❖ от RouterOS 6.33 - инструмента email може да работи с имена/fqdn
- ❖ от RouterOS 6.33 - всички тунели поддържат DNS имена за remote address
- ❖ от RouterOS 6.33 - on-up и on-down скриптове в PPP профилите

Други промени

- ❖ от RouterOS 6.34 - промяна в условие limit - освен packet rate вече се поддържа bit rate, промяна в синтаксиса (limit=5,5 вече трябва да бъде limit=5,5:packet). Поддръжка инверсия.
- ❖ от RouterOS 6.35 - добавена опция bucket-size към опашките
- ❖ от RouterOS 6.35 - добавено действие "route" в mangle prerouting

Други промени

- ❖ от RouterOS 6.35 - добавена политика romon за потребители
- ❖ от RouterOS 6.36 - възможност за добавяне на DNS име към address-lists
- ❖ от RouterOS 6.36 - добавени NAT Helpers за udplite, dccp и sctp

Лято 2016- Лято 2017

- ❖ От версия 6.37 има един wireless пакет, който е наследника на wireless-ger
- ❖ Премахната е настройка DFS, режима на работа е DFS с Radar Detect
- ❖ Добавена функционалност loop-protect за интерфейси, пренасящи Ethernet

Лято 2016- Лято 2017

- ❖ От версия 6.38 е добавена поддръжка за IKEv2
- ❖ От версия 6.38 е добавена функционалност за използване на хардуерната поддръжка на (R)STP за switch chip-овете
- ❖ От версия 6.38 е премахната поддръжката на IKEv1 ah+esp
- ❖ Възможност за убиване на конкретен ipsec peer

Лято 2016- Лято 2017

- ❖ Във версия 6.39 е решен out-of-order проблема с хардуерния AES при CCR, също са направени и оптимизации в използването на хардуерното ускорение за AES
- ❖ Във версия 6.39 е добавена поддръжка за aes-ni на i386 и x64
- ❖ Добавена поддръжка на fast-forward - специален вариант на fastpath за bridge с 2 порта

Лято 2016- Лято 2017

- ❖ Преработена имплементация на MPLPPP, използва вътрешен механизъм за промяна на MSS - не се създават динамични mangle правила
- ❖ Възможност за добавяне на VPN интерфейси динамично към interface list
- ❖ Възможност за конфигуриране на L2TP клиента и L2TP сървъра да изискват IPsec

Лято 2016- Лято 2017

- ❖ От версия 6.40 IPsec политиките нямат параметър приоритет, но вече са подредени - обхождат се последователно
- ❖ Добавен tr069-client
- ❖ Премахнато условие p2p от firewall

Лято 2016- Лято 2017

- ❖ Добавена възможност за коментари в switch менюто
- ❖ Добавена поддръжка на LLDP
- ❖ Добавен режим local-proxy-arp за интерфейсите

Лято 2016- Лято 2017

- ❖ В Nv2 включена възможност за управление на разпределението на времето за up и down
- ❖ Възможност за синхронизация на слотовете на Nv2 точки за достъп, които се виждат (не е обвързано с GPS синхронизация)
- ❖ Имплементирана опция "caps-mode" при нулиране на конфигурацията с отделен скрипт за първоначална базова конфигурация

Лято 2016- Лято 2017

- ❖ От версия 6.40 на RouterOS /walled garden ip поддържа address-list
- ❖ Нова опция terse при export, с помощта на която дългите редове не се пренасят
- ❖ Имплементирани базови филтри в /ipv6 firewall в конфигурацията по подразбиране. Изисква пакета IPv6 да е разрешен по време на нулиране на конфигурацията!

Лято 2017- Лято 2018

Версия 6.41 на RouterOS ◀◀

- ❖ Нова имплементация на Bridge
- ❖ Използване на интерфейсни листи за Neighbor Discovery и за MAC сървър
- ❖ Ново условие "tls-host" във firewall
- ❖ Поддръжка на DNS имена за IPsec "remote-peer"

Лято 2017- Лято 2018

Версия 6.41 на RouterOS ◀◀

- ❖ Промени в меню lte
- ❖ Промени в меню w60g
- ❖ Възможност за автоматично изпълняване на скриптите или инсталиране на пакети чрез качване по ftp
- ❖ Оправен процеса по избиране на DR в OSPF

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO

Лято 2017- Лято 2018

- ❖ Разширяване на употребата на интерфейсни листи – wireless access list, CAPsMAN access list, bridge port
- ❖ Пакет userman вече и за ARM и MMIPS бордове
- ❖ Уеднаквяване на версиите на boot loader с тези на RouterOS. Опция за автоматичен ъпгрейд на boot loader (влиза в сила след следващ рестарт)

Лято 2017- Лято 2018

- ❖ Разработване на /ip kid-control
- ❖ От версия 6.42 потребителски опции и за DHCPv6 сървърите
- ❖ Нова концепция за условието сила на сигнала в access list-ите за wireless.
- ❖ Решени съществени проблеми в сигурността.

Нова имплементация на Bridge

- ❖ Поддръжка на MSTP, IGMP snooping и VLAN операции, управление на broadcast/multicast
- ❖ За да се използва switch chip за препращане на трафик между портове, вместо (вече липсващия) master-port, портовете се вкарват с hw=yes в Bridge.
- ❖ Ползването на switch chip-а се активира автоматично, ако конфигурацията позволява, иначе всичко се случва софтуерно.

Bridge- поддръжка на VLAN-и

Interface <bridge1>

General STP **VLAN** Status Traffic

VLAN Filtering

PVID: 1

Bridge Port <ether3>

General STP **VLAN** Status

PVID: 10

Frame Types: admit all

Ingress Filtering

enabled

enabled inactive Hw. Offload

Bridge VLAN <10>

Bridge: bridge1

VLAN IDs: 10

Tagged: ether5

Untagged: ether3

Current Tagged:

Current Untagged:

enabled

Bridge- MSTP

- ❖ STP и RSTP поддържат едно Spanning Tree в рамките на физическа топология, без значение от използваните vlan-и
- ❖ При Multiple Spanning Tree Protocol в рамките на един region може да има няколко MSTIs (Multiple Spanning Tree Instances), към които да са причислени различни vlan-и.
- ❖ Чрез различни активни връзки за отделните MSTIs може да се оптимизира топологията.

Neighbor Discovery и MAC сървър

The screenshot shows the Mikrotik WinBox interface. On the left, the 'Tools' menu is open, and 'Neighbors' is highlighted. The main window displays the 'Neighbor List' table. A 'Discovery Settings' dialog box is open, showing the 'Interface' dropdown set to 'dynamic'.

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6	Ag
ether1	10.0.0.249	00:0C:42:92:1E:2C	250GS-tmk	MikroTik	1.17	BB250GS	no	
ether1	10.0.0.248	E4:8						
ether1	10.0.0.254	64:D						
ether1	10.0.0.251	E4:8						
ether1	10.0.0.253	D4:C						
ether1	10.0.0.17	00:0						
ether1	10.0.0.252	00:5						
ether1		D0:5						
ether1		88:A						

The screenshot shows the Mikrotik WinBox interface. On the left, the 'Tools' menu is open, and 'MAC Server' is highlighted. The main window displays the 'MAC Server' configuration dialog. The 'MAC Telnet Server' and 'MAC WinBox Server' tabs are visible. The 'Allowed Interface List' dropdown is set to 'none' for the MAC Telnet Server and 'all' for the MAC WinBox Server.

Interface	Src. Address	Uptime
MAC Telnet Server		
Allowed Interface List:	none	

Interface	Src. Address	Uptime
MAC WinBox Server		
Allowed Interface List:	all	

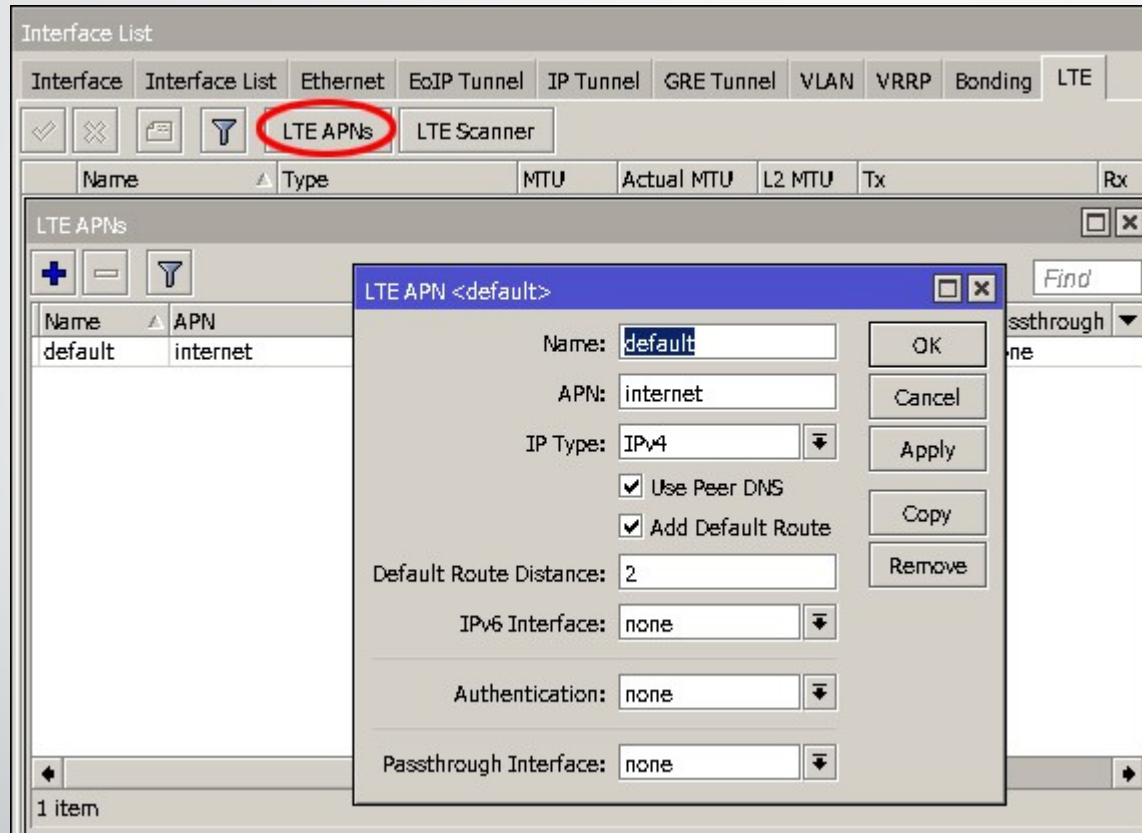
Какво ново от Mikrotik, Петър Димитров

© PG.NET.PRO

tls-host

- ❖ Използва некриптираната заявка към https сървър, указваща име на търсения сървър чрез Server Name Indication допълнението на SSL
- ❖ Удобен инструмент за блокиране на определени https сайтове
- ❖ Работи само при използване на SNI (rfc3546) и ако заявката не е фрагментирана

Промени в меню Ite



Промени за w60g

- ❖ Поддръжка на Point to Multipoint (до 8 клиента)
- ❖ Промяна на наименованията на режимите на работа - вече се използват познатите "bridge", "ap-bridge" и "station-bridge"
- ❖ Клиентите се третират като отделни интерфейси, с възможност за динамично добавяне в bridge
- ❖ Изоляция между клиентите

Файлове, качвани по FTP

- ❖ При качване на скрипт с име, завършващо на ".auto.rsc", скрипта се изпълнява автоматично. Резултата от изпълнението се записва във файл.
- ❖ При качване на пакет с име, завършващо на ".auto.npk", рутера се рестартира, при което пакета се инсталира

Опции за DHCPv6 сървърите

- ❖ От версия 6.42 има възможност за дефиниране на потребителски опции, които да бъдат давани от DHCPv6 сървърите
- ❖ Това дава възможност за указване на произволен DNS сървър, включително самия рутер, с което се избягва ограничението да бъдат давани само сървърите от `/ip dns`, например:

```
dhcp option 23
```

```
0x2001486048600000000000000000000008888200148604860000000000000000008844
```

Сила на сигнала в access list

Wireless Tables

WiFi Interfaces | W60G Station | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | Channels

#	MAC Address	Interface	Signal Str...	Authentication	Forwarding
0	C4:17:FE:8E:40:64	all	-120..120	no	no
1	C4:17:FE:8E:40:64	all	-120..120	yes	yes
2	C4:17:FE:8E:40:64	all	-120..120	yes	yes

AP Access Rule <C4:17:FE:8E:40:64>

MAC Address: C4:17:FE:8E:40:64

Interface: all

Signal Strength Range: -120..120

Allow Signal Out Of Range: 00:00:10

AP Tx Limit: []

Client Tx Limit: []

Authentication

Forwarding

VLAN Mode: no tag

VLAN ID: 1

Private Key: none 0x []

Private Pre Shared Key: []

Management Protection Key: []

Time: 00:00:00 - 1d 00:00:00

Days: sun mon tue wed thu fri sat

enabled

Решени проблеми в сигурността

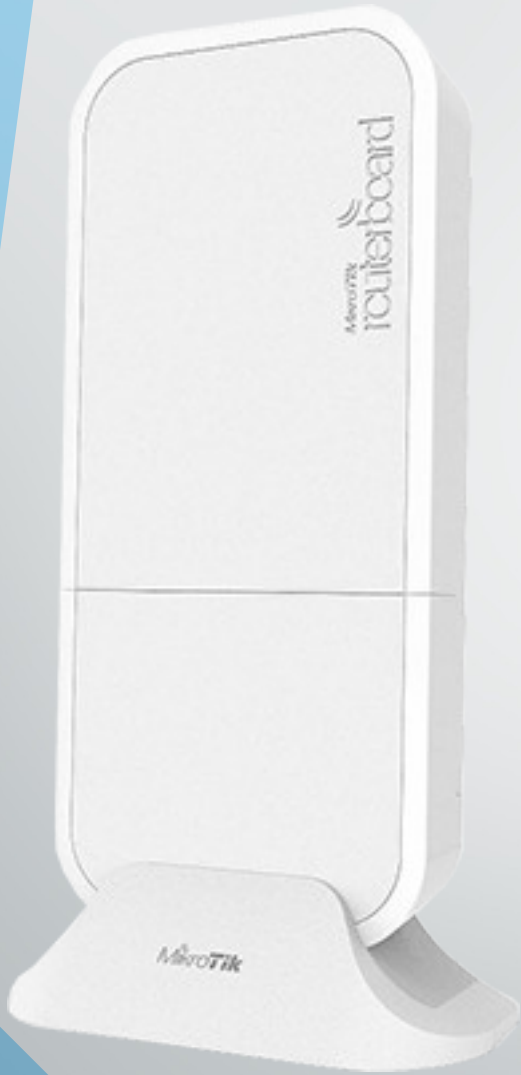
- ❖ За последната година имаше няколко сериозни проблема, които MikroTik отстраниха - с http/https услугата, със SMB услугата и с winbox услугата
- ❖ В резултат от лоша поддръжка (оставяне на стари версии в употреба, липса на смислен firewall или твърде либерални правила във firewall) множество рутери бяха хакнати, най-вече през отворен порт 8291.

Хардуер

Какво ново от MikroTik, Петър Димитров

© PG.NET PRO

WAP LTE



- ❖ "Бисквитка" с RouterOS
- ❖ Жичен и безжичен интерфейс
- ❖ Възможност за мобилни офиси, с достъп до корпоративни ресурси по сигурен начин и без нужда потребителите да достъпват и конфигурират рутера

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO

hAP ac²



- ❖ Мощ четириядрен рутер с хардуерен AES за Ipsec
- ❖ Компактен и красив
- ❖ Гигабитови интерфейси
- ❖ 802.11 a/b/g/n/ac

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO

Dual Band Aps- wAP ac и cAP ac



- ❖ wAP ac е първия dual band AP, два отделни чипа за 2.4 и 5 GHz, сензори температура и напрежение
- ❖ cAP ac е по-новото и по-бюджетно решение с един чип, работещ едновременно на 2.4 и 5 GHz, без сензори

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO

RB1100x4



- ❖ Съвременното устройство от серията 1100
- ❖ Резервирано с 2 захранвания
- ❖ Мощен четериядрен процесор и разбира се хардуерен AES за IPsec

Какво ново от MikroTik, Петър Димитров

© PG.NET PRO

RB450Gx4



- ❖ Интересен наследник на RB450G/RB850Gx2
- ❖ Четериядрен процесор и хардуерен AES за IPsec
- ❖ 1GB памет

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO

60GHz-ad устройства



- ❖ Една платка с две различни антени - wAP 60G за къси и LHGG-60ad за по-дълги разстояния
- ❖ Пренос над 1Gbps
- ❖ Beamforming

Какво ново от Mikrotik, Петър Димитров

© PG.NET PRO

Комутатори CRS 3-та серия

- ❖ Новата 3-та серия switch-ове от MikroTik са с по-проста конфигурация спрямо 1-ва и 2-ра серия
- ❖ Поддържат Dual Boot - можете да ги ползвате под RouterOS или SwOS
- ❖ Постепенно изместват устройствата от по-старите серии с аналогични портове

Комутатори CRS 3-та серия

- ❖ Менюто Switch е с минимална функционалност - аналогично на бордовете с прост switch chip
- ❖ Конфигурацията на vlan-и се случва в Bridge, като това не изключва Hardware Offload
- ❖ Почти всички анонсирани нови switch-ове са 3-та серия

Новите модели комутатори

❖ CRS326-24G-2S+RM/CSS326-24G-2S+RM

❖ CRS317-1G-16S+RM

❖ CRS112-8P-4S

❖ CRS328-24P-4S+RM

❖ CRS328-4C-20S-4S+RM

Предстоят: CRS305-1G-4S+IN, CRS309-1G-8S+PC, CRS332-32S+RM,
CRS312-4C+8XG, CRS354-48G-4S+2Q+, CRS354-48P-4S+2Q+

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO

LtAP mini с LTE



- ❖ За монтаж в превозни средства
- ❖ С LTE и GPS
- ❖ Жичен и безжичен порт
- ❖ Възможност за външни антени за LTE и GPS

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO


wsAP ac lite



- ❖ Първото In-Wall решение, подходящо за изграждане на безжична мрежа в хотели и други публични сгради
- ❖ Dual Band 2.4 и 5 GHz
- ❖ Допълнителни портове

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO



Благодаря за
вниманието!

Какво ново от MikroTik, Петър Димитров

© PG.NET.PRO