MikroTik és RouterOS

Dr. Répás Sándor

Történelem

- SIA Mikrotīkls
- 1996-ban alakult
- Lettország (Riga)
- RouterOS (1997 óta)
- 2002 óta saját hardver is, RouterBoard néven
- Több mint 140 munkavállaló
- A Wireless ISP-k körében nagyon népszerű

RouterBoard

- WiFi és Ethernet interfészek
- Intel, MIPS, ARM, PPC és TILE architektúra
- Moduláris és fix eszközök
- Rack, desktop, „csupasz” és kültéri eszközök

hEX lite – RB750r2

- 5 db Ethernet port
- 1 magos QCA9533 (ARM) CPU, 850MHz
- 64MB RAM, 16MB Flash
- Akár 493Mbps továbbítás
- 2W
- ~12.000Ft

hEX – RB750Gr3

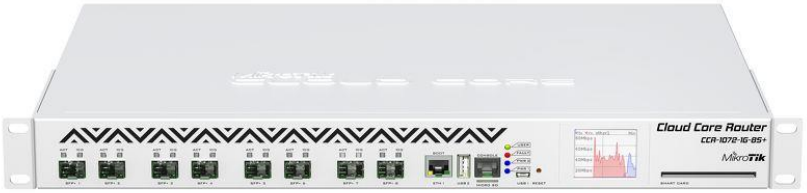
- 5 db Gb Ethernet port
- 2 magos, 4 szálas MT7621A (MMIPS) CPU, 880MHz
- 256MB RAM, 16MB Flash
- MicroSD, USB
- Akár 2Gbps továbbítás
- IPsec támogatás (~470Mbps)
- 10W
- ~17.000Ft

RB3011UiAS-RM

- 10 db Gb Ethernet port (1 SFP)
- 2 magos IPQ-8064 (ARM) CPU, 1,4GHz
- 1GB RAM, 128MB Flash
- USB 3.0, LCD
- Akár 4Gbps továbbítás
- IPsec támogatás (~790Mbps)
- 10W
- ~50.000Ft

CCR1072-1G-8S+

- 8 db 10Gb Ethernet port (SFP+)
- 1 db Gb Ethernet port
- 72 magos TLR4-07280 (TILE) CPU, 1GHz
- 16GB RAM, 128MB Flash
- MicroSD, 2 db M.2, 2 db USB, LCD
- Akár 79Gbps továbbítás
- IPsec támogatás (~10Gbps)
- 125W
- ~850.000Ft

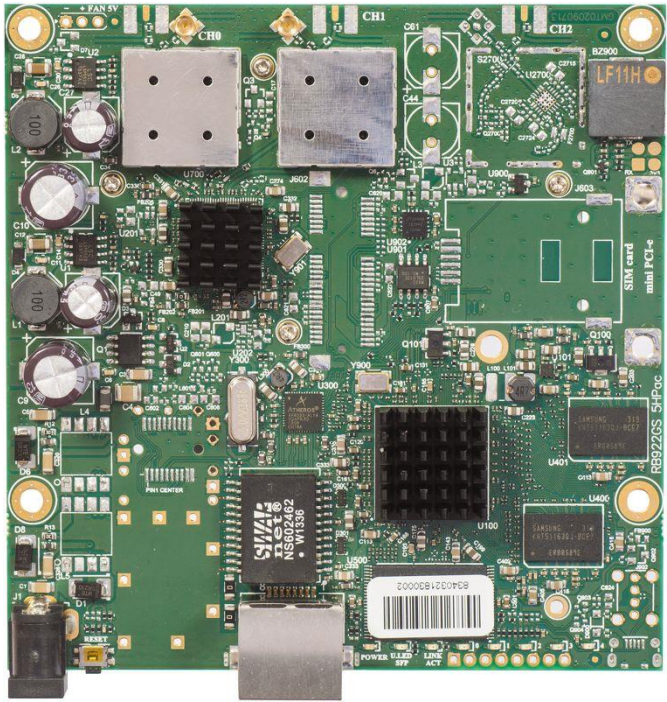


hAP ac²

- 5 db Gb Ethernet port
- 1db 802.11b/g/n
- 1db 802.11a/n/ac, 2 chains
- 4 magos IPQ-4018 (ARM) CPU, 716MHz
- 128MB RAM, 16MB Flash
- USB
- Akár 2Gbps továbbítás
- IPsec támogatás (~424Mbps)
- 16W
- ~20.000Ft

RB911G-5HPacD

- 1 db Gb Ethernet port
- 1db 802.11a/n/ac, 2 chains
- 1 magos QCA9557 (MIPS) CPU, 720MHz
- 128MB RAM, 16MB Flash
- 12W
- ~22.000Ft



DynaDish 5

- 1 db Gb Ethernet port
- 1db 802.11a/n/ac, 2 chains, 2dBi antenna
- 1 magos QCA9557 (MIPS) CPU, 720MHz
- 128MB RAM, 16MB Flash
- 9W
- ~44.000Ft

RouterOS

- 1997 óta
- Eleinte csak i386
- Linux alapú, de rengeteg saját fejlesztéssel
- Linux ismeretek kicsit segítenek, de saját konfigurációs felületek
- Licensz vásárolható i386 számítógépekre és virtualizált környezetbe (Cloud Hosted Router, CHR)
- A RouterBoard eszközökhöz jár valamilyen licensz, ami szükség esetén „upgradelhető”

RouterOS licenszelés

Level number	0 (Trial mode)	1 (Free Demo)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	volume only	$45	$95	$250
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h trial	-	-	yes	yes	yes
Wireless Client and Bridge	24h trial	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h trial	-	yes(*)	yes	yes	yes
EoIP tunnels	24h trial	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h trial	1	200	200	500	unlimited
PPTP tunnels	24h trial	1	200	200	500	unlimited
L2TP tunnels	24h trial	1	200	200	500	unlimited
OVPN tunnels	24h trial	1	200	200	unlimited	unlimited
VLAN interfaces	24h trial	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h trial	1	1	200	500	unlimited
RADIUS client	24h trial	-	yes	yes	yes	yes
Queues	24h trial	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h trial	-	yes	yes	yes	yes
User manager active sessions	24h trial	1	10	20	50	Unlimited
Number of KVM guests	none	1	Unlimited	Unlimited	Unlimited	Unlimited

Cloud Hosted Router (CHR)

- Támogatott virtualizációs platformok:
  - VirtualBox 5
  - VMWare ESXi/Workstation/Fusion
  - Qemu
  - Hyper-V on Windows Server 2012
  - Citrix XenServer
  - Microsoft Azure
  - Amazon Web Services (AWS)
- Licenszelés interfész sávszélesség alapján:
  - Trial regisztrációval: 60 napig ingyenes, a megadott sávszélességgel, utána nincs upgrade
    - Érdemes kipróbálni. Tanuláshoz ideális.
  - Trial limited: 1Mbps limittel bármeddig
  - P1: 1Gbps/interfész; 45 USD
  - P10: 10Gbps/interfész; 95 USD
  - P-Unlimited; 250 USD

Kezdeti konfiguráció

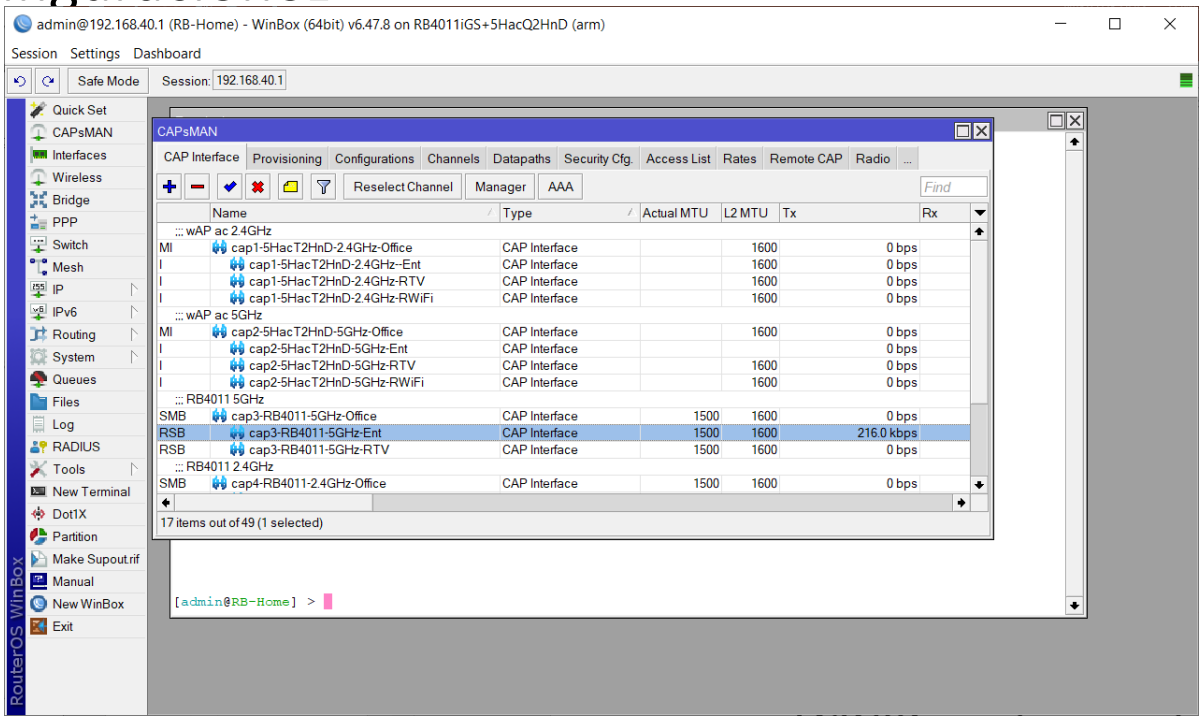
- Az első bekapcsoláskor alapértelmezett konfiguráció töltődik be
- Ez eszköztípusonként eltér
- Az első belépéskor felajánlja a lehetőséget a konfigurációs beállítások törlésére
- Amivel a legtöbbször találkozunk, az a CPE konfiguráció:
  - Az első ethernet port a WAN, a többi LAN, WiFi esetén nincs hitelesítés, titkosítás!
  - Eszköz LAN IP címe: 192.168.88.1/24
  - DHCP szerver és DNS szerver is fut
  - Alap tűzfalbeállítások
  - WAN porton DHCP kliensként, de ez könnyen átállítható PPPOE-re

Felügyelet, konfiguráció

- Soros porton keresztül, konzol:
  - Eszköztől függően:
  - 0, 1, vagy 2 darab soros port
  - RJ45 (mint a Cisco eszközök), vagy DB9 csatlakozó
- Telnet: nem biztonságos
- Mac-Telnet:
  - MikroTik saját megoldása
  - Nincs szükség hozzá IP címre. L2 felett működik!
  - Nem biztonságos.
- SSH
- Winbox: grafikus felület
- Webfig: A Winboxhoz hasonlóra kialakított webfelület

Winbox

- GUI
- Win32 program, de Wine segítségével Linux és MacOS.
- AES128-CBC-SHA titkosítással kommunikál
- TCP/IP segítségével a TCP 8291 portján kommunikál
- Képes Mac-telnet szerű kommunikációra is (L2!), általában kezdeti konfigurációhoz



Alapvető beállítások

- IP cím
- Átjáró
- DNS kliensként
- DNS szerverként
- DHCP szerverként
- NAT
- Firewall
- WiFi

IP cím

- IP címek kiíratása

```
ip address print
```

- IP címek interfészhez rendelése

```
ip address add interface=ether1 address=80.64.65.22/24
ip address add interface=ether2 address=192.168.32.1/24
```

- IPv6 címek kiíratása

```
ipv6 address print
```

- IPv6 címek interfészhez rendelése

```
ipv6 address add interface=ether1 address=2a02:d400:0:a401::2
ipv6 address add interface=ether2 address=2a02:d500:0:1::1
```

IP routing

- IP routing tábla kiíratása

```
ip route print
```

- IP routing tábla bejegyzés hozzáadása

```
ip route add dst-address=0.0.0.0/0 gateway=80.64.65.1
```

- IPv6 routing tábla kiíratása

```
ipv6 route print
```

- IPv6 routing tábla bejegyzés hozzáadása

```
ipv6 route add dst-address=::/0 gateway=2a02:a50::1
```

DNS beállítások

```
ip dns set servers=185.143.48.16,8.8.8.8 \
 allow-remote-requests=yes
```

- A `servers` adja meg, hogy az eszköz a névfeloldáshoz mely DNS szervereket veszi igénybe
- Az `allow-remote-request` engedélyezi, hogy kleinsektől érkező névfeloldási kérésekre válaszoljon. (cache only DNS szerver)
  - Fontos, hogy ha ezt engedélyezzük, úgy tűzfalszabályokkal védjük a routerünket, az internet felől érkező kérésektől, mert DDoS támadásokra jól használható a védtelen eszköz.

DHCP szerver beállítása

- IP pool létrehozása a kliensek számára

```
ip pool add name=DHCP-hez ranges=192.168.32.32/27
```

- IP alhálózat létrehozása, melyben megadhatjuk a különböző DHCP options beállításokat

```
ip dhcp-server network add address=192.168.32.0/24 \
 dns-server=192.168.32.1,8.8.8.8 gateway=192.168.32.1 \
 netmask=24
```

- IP alhálózat létrehozása, melyben megadhatjuk a különböző DHCP options beállításokat

```
ip dhcp-server add interface=ether2 address-pool=DHCP-hez \
 lease-time=1h
```

Tűzfal beállítások

- IP forrás cím NAT

```
ip firewall nat add action=src-nat chain=srcnat \
src-address=192.168.32.0/24 to-addresses=80.64.65.22
```

- IP forrás cím masquerade

```
ip firewall nat add action=masquerade chain=srcnat \
src-address=192.168.32.0/24
```

- Különböző címről érkező csomagok szűrése

```
ip firewall filter add src-address=1.2.3.4/32 chain=input \
 action=drop
ip firewall filter add src-address=1.2.3.4/32 chain=forward \
 action=drop
```

Hálózat összefoglalás

- Csak az alapvető parancsokat ismertettük
- Azoknak is csak a legfontosabb lehetőségeit
- Különösen a tűzfalszabályok esetében szembetűnő, hogy a rendszer működése és paraméterezése nagyon hasonlít a Linuxra

WiFi parancsok

```
interface wireless security-profiles add \
 authentication-types=wpa2-psk name=profile1 \
 wpa2-pre-shared-key=AABBCCDDEE!
interface wireless set wlan1 band=2ghz-b/g/n \
 channel-width=20/40mhz-Ce disabled=no distance=indoors \
 frequency=2412 mode=ap-bridge security-profile=profile1 \
 ssid=TESTWIFI wireless-protocol=802.11
```