

800 registered for the MUM



When we announced the MUM in Czech Republic, we expected 700 people to register, yet beyond all expectations, already 800 people are registered from 70 countries, and it's still two weeks until the event. Due to this we have arranged more discounted rooms with the hotel, and extended the free registrations until this Friday, 6:00PM

MUM will take place **February 27-28, 2009**.
Training before MUM will take place the same week.

More information on <http://mum.mikrotik.com> and <http://training.mikrotik.com>



RB1000 encryption engine

In RouterOS v3.20 we have added support for the RB1000 encryption hardware, that is already built into your device. Just a simple software upgrade, and your performance will **increase** an unbelievable 10x, compare these results:

v3.20:	v3.19:
AES128: 510Mbps	AES128: 79Mbps
3DES: 500Mbps	3DES: 45Mbps

The RB1000 even outperforms a top of the line dual-core PC that we also tested, the PC managed to get 300Mbps with AES128 enabled, which is still 200Mbps less than our RB1000.

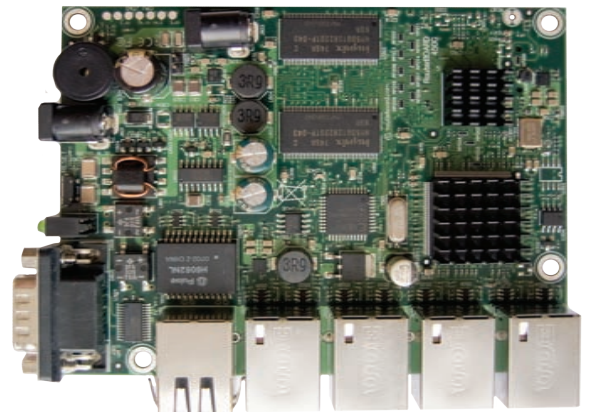
More info about RB1000:

<http://www.routerboard.com/pdf/rb1000brochure.pdf>

RouterBOARD RB450G

We are happy to announce a new product that, among others, will be demonstrated at the upcoming MikroTik User Meeting (MUM) in two weeks, the RB450G.

Comparing to the RB450, the RB450G not only includes five gigabit ethernet ports, but also 256Mb of RAM for full BGP and metaROUTER support, a faster CPU and a microSD card slot for file storage. The device is powered by a fast AR7161 680MHz Atheros CPU, and also includes a temperature sensor and voltage monitor.



Management frame protection

Ever wonder how to protect your wireless AP from hackers that clone MAC addresses or use deauthentication attacks to disrupt, or gain access to your network? Encryption and authentication is not always an option, as disruptions due to disassociation attacks could still be possible.

If you use MikroTik client devices, turn on the **management frame protection** in your wireless settings, if you also have other brand clients in your network set it to **allowed** instead of **required**. Recently introduced, it inserts a special keyphrase into some management frames that are exchanged between the client and the AP, so that the AP always knows which one is the real client.

```
/interface wireless security-profiles> set default  
management-protection=required
```

v3.20 wireless-test package required. More info:
http://wiki.mikrotik.com/wiki/Wireless_Development