MikroTik RouterOS - Basic configuration

Help and Support

Help Desk

Homepage

SERVER MANAGEMENT

Managed Service Provider | Network Solutions | Information Systems | IT Projects | www.serman.ee

Overview

> This article is written by Server Management Inc. IT systems administrator Timo Puistaja - 19.04.2017, Tartu, Estonia.

Need help configuring your device? Contact us

info@serman.ee

We have built several different networking systems all over EU. This is the main step-by-step overview of MikroTik RouterOS configurations we are using. This is the basics - everything you need to do when you just want to get the internet up and running but also know how to secure your router from potetial threats. In this scenario im going to use RB3011Ui-AS running Router OS 6.3.7.3 as example.

Basic Configurations

WAN/UPLINK/ISP Connection (ether1 on MT)

Usually there are 3 ways of getting cable internet to your home or office:

1. Dynamic IP from ISP: *IP - DHCP Client - Add:* ether1; Use peer DNS and NTP;
2. Static IP from ISP: *IP - Addresses - Add:* fill in the address from the info ISP gave you; use Interface: ether1. **NB!** Dont forget to manually add the default route and let your router know where is the gateway (usually ISP router): /ip route add distance=1 gateway=ISP device IP)
3. PPPoE uplink: *PPP - Add:* PPPoE Client - Interface: ether1; Dial Out window: fill in the username and password fields; usually you don´t need to touch anything else.

LAN (ether2 - 10 on MT)

Usually we setup bridge and add all ports to bridge. Give this bridge IP (this will be the GW; DHCP and DNS server for local PC´s). Configure IP Pool and then make DHCP Server to serve addresses from the pool.

1. *Bridge - Add*: bridge_LAN; Admin MAC Addres: 00:BB:01:32:00:00 (or use any of the ports ether2 -10 MAC for bridge MAC)
2. *IP Addresses - Add*: 192.168.x.x/24; network: 192.168.x.0; interface: bridge_LAN;
3. *IP - Pool - Add:* DHCP_pool: 192.168.x.100 - 192.168.x.150 for example (you will be serving 50 IP addresses to you network users).
4. *IP - DHCP Server - Add:* DHCP_server; Interface: bridge_LAN; Lease time 8h; Address pool: DHCP_pool; Networks: Add: Address: 192.168.x.1/24; Gateway: 192.168.x.1; DNS Servers: 192.168.x.1)
5. *IP - DNS - Allow Remote Requests*
6. *Now add you ether2-10 ports to new bridge_LAN: Brigne - Ports - Add: Interface: ether2: Bridge: bridge_LAN - OK.* ***Do this for all ports that are meant for LAN connection.***

NAT

Now we need to Masquerade our LAN and WAN networks, so they can talk in the default route (0.0.0.0/0) - our clients can access internet.

1. *IP - Firewall - NAT - Add:* SCRNAT; Scr. Adr.: 192.168.x.0/24; Dst. Adr.: 0.0.0.0/0; Action: Masquerade;

Firewall

This is one of the best firewalls we have seen in the years. More info: MikroTik RouterOS - Best practice firewall

As you noticed before we did allow our router to answer DNS requests. Its good idea to make MikroTik you internal DNS server - you can make fake DNS records. (for example elephant.monkey.com = 192.168.x.100). But we need to Drop the DNS requests coming from outside (WAN) otherwise our router will be Open DNS Resolver and sooner or later will be used to attack some other DNS servers.

Our firewalls idea is to block everything coming from outside (WAN) and then start allowing only needed traffic (for example you put up Webserver - then you allow port 80 towards your IP/router and make port forward in NAT to reach the server in your internal network)

Here is the export of our most used firewall, comments showing what each line is for:

/ip firewall filter

add action=drop chain=input comment="Drop DNS requests from public" connection-state=new dst-port=53 in-interface=ether1 protocol=tcp

add action=drop chain=input comment="Drop DNS requests from public" connection-state=new dst-port=53 in-interface=ether1 protocol=udp

add action=drop chain=input comment="Disallow weird packets" connection-state=invalid

add action=accept chain=input comment="Allow LAN access to router and Internet" connection-state=new in-interface=bridge1-LAN

add action=accept chain=input comment="Allow connections that originated from LAN" connection-state=established

add action=accept chain=input comment="Allow connections that originated from LAN" connection-state=related

add action=accept chain=input comment="Allow ping ICMP from anywhere" protocol=icmp

add action=accept chain=input comment="Allow WAN access to router" dst-port=8291 protocol=tcp

add action=drop chain=input comment="Disallow anything from anywhere on any interface"

add action=drop chain=forward comment="Disallow weird packets" connection-state=invalid

System/Varia configurations

1. *System - Identity* - For example: HOMEROUTER or BERLINOFFICE
2. *System - Password* - ADD EXTRA STRONG PASSWORD (Example of strong password: B__7A=:J[g'^JF9D)
3. *IP - Services* - Disable everything BUT Winbox (so you know that only Winbox access to router is enabled, you can enable services later, if needed)
4. *LCD* **-** Disable Touchscreen (you dont want people who have access to the network rack to track any configurations from the LCD panel)
5. *Tools - MAC Server - Telnet Interfaces* - **ONLY bridge_LAN (**you dont want people be able to access your router from external using MAC address)
6. *IP Firewall - Service Ports* - DISABLE ALL!

Monitoring your MikroTik

By default you should configure some graphing - whenever you or your PC users feel like the internet is slow - you can check out whether MikroTik is out of resources (CPU; Mem) or the uplink speed is not enough.

Ofcouse for bigger infrastructures its recommended to use SNMP monitoring softwares (Cacti/Observium/The Dude or something similar). Next step from SNMP monitoring is Packet Flow monitoring to monitor WHO is using the resource.

To setup basic graphing:

1. *Tools - Graphing - Queue Rules - Add:* Interface: ether1 (our uplink); Allow Address (from witch IP people can view the graphs); Store on Disk =YES (we dont want to keep our useful graphs on the HDD of MikroTik)
2. *Tools - Graphing - Queue Rules - Add:* Interface: bridge_LAN (our whole LAN); Allow Address (from witch IP people can view the graphs); Store on Disk =YES (we dont want to keep our useful graphs on the HDD of MikroTik)
3. *Tools - Graphing - Resource Rules - Add:* Allow Address (from witch IP people can view the graphs); Store on Disk =YES (we dont want to keep our useful graphs on the HDD of MikroTik)

You can View your graphs from the same menu OR enable WWW from *IP - Services* and go to you MikroTiks webpage/panel.

Logging

This is **VERY important** - by default MikroTik holds its logs on RAM which means if you reboot the device when you are in trouble - you will lose all the logs. We will setup MikroTik to keep logs on Disk:

1. *System - Logging:* switch warning; error, critical and info topics to action TO disk, this mean they will be saved on Disk.
2. Go to Actions menu and configure Disk to save lots of logs: Lines Per File 50000; File Count 10; Stop on Full = NO!

Configuration backups

We usually keep configs in .rsc format. Its really easy to export and import them between routers. We make manual backups form devices after every bigger change. Note that this method doesnt export MAC addresses and admin password - perfect for import-export between 2 different routers.
Open terminal and write *export file=filenamehere* and press Enter on your keyboard.

The backup file is now in the Files menu - go and download it to your PC. (Your backup file is useless if the MikroTik is dead or corrupted and its only stored on the MikroTik itself)

Thats it - your basic configuration is now done as professional networking engineer would do it.

Need help configuring your device? Contact us info@serman.ee