

# TE PUNOSH ME MIKROTIK

# IMPLEMENTIMI I SIGURISE

## Do te flasim per

### Hapat baze te punes me MikroTik

Cfare eshte MikroTik RouterOS, RouterBoard, si lidhemi me ta, pamja e jashtme, resurset, zgjedhja e ruterbordit specifik per detyra specifike, upgrade, konfigurimi, monitorimi, CLI, etj

### Implementimi I sigurise ne ruter

Implementimi I sigurise eshte nje nga proceset kyce te ndertimit te nje rrjeti kompjuterik. Meqenese nje ruter eshte porta hyrese per nje rrjet, ateherë vete ruteri duhet te konfigurohet ne menyra te tilla qe te jete sa me I mbrojtur. Nje sulm nga jashte dhe marja eventuale ne kontroll e ruterit, I siguron sulmuesit edhe kontrollin ndaj rrjetit.



# TUNGJATJETA!

**Quhem: Erion Demiri**

Email:  
[edemiri@ens-al.com](mailto:edemiri@ens-al.com)

- ▶ 1999 – Pergjegjes per rrjetet LAN, Infosoft.
- ▶ 2001 – IBM Netfinity Servers
- ▶ 2001 – Omega Networking and Service
- ▶ 2006 – ENS, Easy Network Solutions
- ▶ 2007 – MUM Egypt, MTCNA
- ▶ 2011 – MUM Budapest, MTCRE

## ENS – EASY NETWORK SOLUTIONS

- ▶ Rrjeta kompjuterike te permasave te ndryshme
- ▶ Zgjidhje per sigurine, mbrojtje antivirale
- ▶ Rrjeta wireless te permasave te medha
- ▶ Sisteme survejimi IP.
- ▶ Sisteme VPN.
- ▶ Etj...

## WIFI







OmniTIK5  
3G TIM Usb Key  
SIEMENS PLC

# MOBILE VPN



1.

# MikroTik - RouterOS

Pse MikroTik?



“

*MikroTik RouterOS eshte nje sistem operativ i dizenuar per ruterat, i bazuar ne Linux, me nje game te gjere funksionesh, qe i japin nje inxhinieri rrjetesh, mundesi per konfigurime nga me te ndryshmet.*

”

## Versionet

- ▶ Versioni i pare i leshuar ne 1997
- ▶ RouterBoard i pare ne 2002
- ▶ Vers.2.7 dhe 2.9.27
- ▶ 3.0 (Janar 2008)
- ▶ 4.0 (Tetor 2009)
- ▶ 5.0 (Maj 2010)
- ▶ 6.0 (Maj 2013)
- ▶ Vers aktual: 6.43.4 (17 Tet 2018)

# Versionet

https://mikrotik.com/download



Search



Home About Buy Jobs Hardware Software Support Training Account

## Software

Downloads Changelogs Download archive RouterOS The Dude

## RouterOS



|                 | 6.42.9 (Long-term)                                                                                                                                                                                                | 6.43.4 (Stable)                                                                    | 6.44beta20 (Testing)                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <b>MIPSBE</b>   | CRS1xx, CRS2xx, DISC, hAP, hAP ac, hAP ac lite, LDF, LHG, mANTBox, mAP, NetBox, NetMetal, PowerBox, QRT, RB9xx, cAP, hEX Lite, RB4xx, wAP, BaseBox, DynaDish, RB2011, SXT, OmniTik, Groove, Metal, Sextant, RB7xx |                                                                                    |                                                                                      |
| Main package    |                                                                                                                                  |   |   |
| Extra packages  |                                                                                                                                  |   |   |
| <b>SMIPS</b>    | hAP mini, hAP lite                                                                                                                                                                                                |                                                                                    |                                                                                      |
| Main package    |                                                                                                                                  |   |   |
| Extra packages  |                                                                                                                                  |   |   |
| <b>TILE</b>     | CCR                                                                                                                                                                                                               |                                                                                    |                                                                                      |
| Main package    |                                                                                                                                  |   |   |
| Extra packages  |                                                                                                                                  |   |   |
| The Dude server |                                                                                                                                 |  |  |

# Arkitektur

- ▶ **MIPS (MIPSBE, SMIPS, MIPSLE, MMIPS)**

**MIPSBE:** RS1xx, CRS2xx, DISC, hAP, hAP ac, hAP ac lite, LDF, LHG, OmniTik, etj

**SMIPS:** hAP mini, hAP lite

**MMIPS:** hEX (RB750Gr3), RBMxx

- ▶ **TILE – seria CCR**

- ▶ **PPC**

RB3xx, RB600, RB8xx, RB1100AHx2, RB1100AH, RB1100, RB1200

- ▶ **ARM**

cAP ac, hAP ac<sup>2</sup>, LDF ac, LHG ac, SXTsq (ac series), Wireless Wire, CRS3xx, RB3011, RB1100AHx4, RB450Gx4

- ▶ **X86**

- ▶ X86 Pentium III Router



## Cloud Hosted Router

### CHR

- ▶ VMWare ESX
- ▶ Hyper-V
- ▶ Qemu/KVM
- ▶ Xen
- ▶ VirtualBox



## 2. Hapat e pare

# RouterBoard

## Kutia e cudirave

### hAP Mini – RB931-2nd

SMIPS, 650 MHz, 3 Ethernet, 32 MB Ram, 16 MB Flash, Dual Chain 802.11b/g/n.

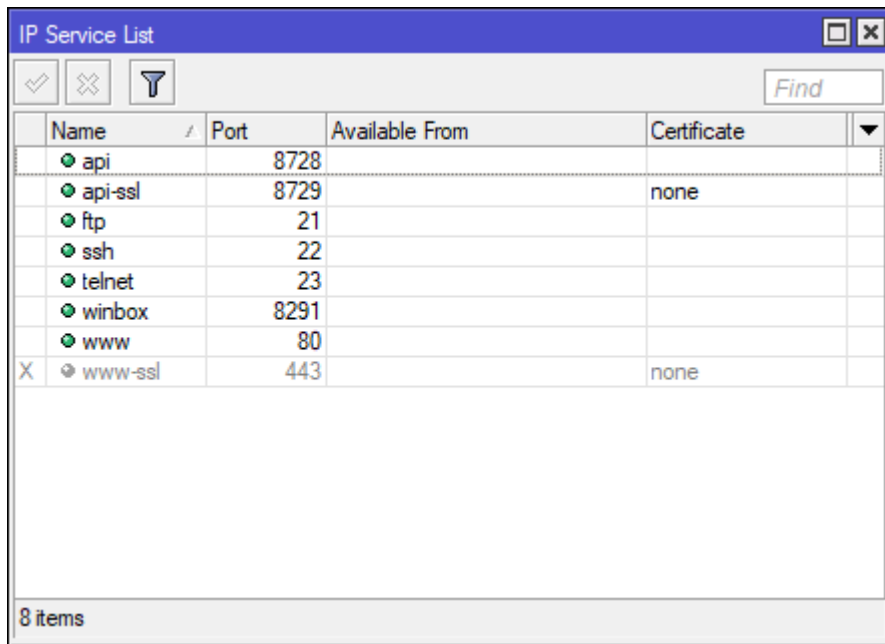
|                            | 1518 byte |       | 64 byte |      |
|----------------------------|-----------|-------|---------|------|
|                            | kpps      | Mbps  | kpps    | Mbps |
| Routing<br>25 simple queue | 24.4      | 296.3 | 151.6   | 77.6 |



# RouterBoard

- ▶ Winbox
- ▶ SSH
- ▶ Telnet
- ▶ Serial
- ▶ API
- ▶ FTP
- ▶ WWW

## Menyrat e lidhjes



|   | Name    | Port | Available From | Certificate |
|---|---------|------|----------------|-------------|
|   | api     | 8728 |                |             |
|   | api-ssl | 8729 |                | none        |
|   | ftp     | 21   |                |             |
|   | ssh     | 22   |                |             |
|   | telnet  | 23   |                |             |
|   | winbox  | 8291 |                |             |
|   | www     | 80   |                |             |
| X | www-ssl | 443  |                | none        |

8 items

[Home](#) [About](#) [Buy](#) [Jobs](#) [Hardware](#) [Software](#) [Support](#) [Training](#)

## Software

[Downloads](#) [Changelogs](#) [Download archive](#) [RouterOS](#) [The Dude](#)

## Upgrading RouterOS

If you are already running RouterOS, upgrading to the latest version can be done by clicking on **"Check For Updates"** in **QuickSet** or **System > Packages** menu in WebFig or WinBox.

See the [documentation](#) for more information about upgrading and release types.

To manage your router, use the web interface, or download the maintenance utilities. Winbox to connect to your device, Dude to monitor your network and Netinstall for recovery and re-installation.

WinBox ▾

The Dude ▾

Netinstall ▾

WinBox 3.18



# Winbox

WinBox v3.18 (Addresses)

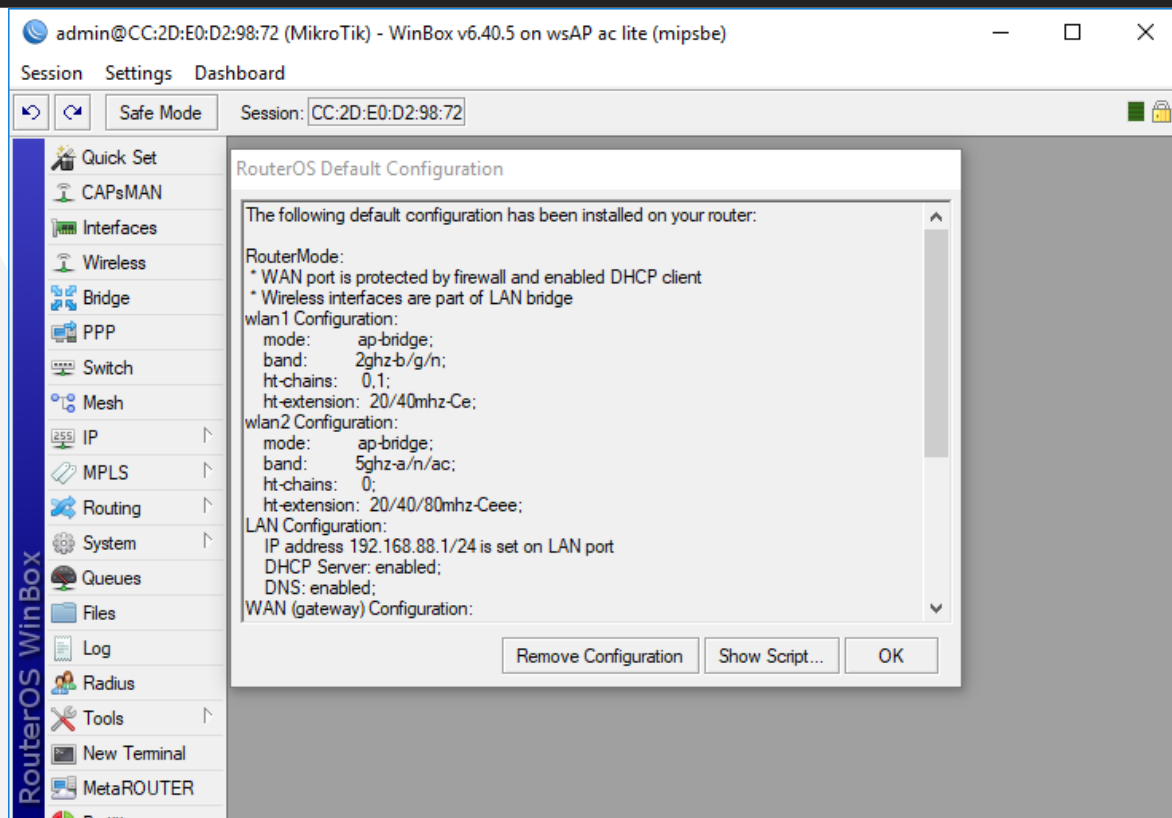
File Tools

Connect To:  ☒ Keep Password  
Login:  ☐ Open In New Window  
Password:

Managed Neighbors

| MAC Address       | IP Address | Identity | Version       | Board         | Uptime   |  |
|-------------------|------------|----------|---------------|---------------|----------|--|
| CC:2D:E0:D2:98:72 | 0.0.0.0    | MikroTik | 6.40.5 (st... | RBwsAP5Hac2nD | 00:01:36 |  |

# Winbox



# Upgrade

admin@CC:2D:E0:D2:98:72 (MikroTik) - WinBox v6.40.5 on wsAP ac lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: CC:2D:E0:D2:98:72

Quick Set  
CAPsMAN  
Interfaces  
Wireless  
Bridge  
PPP  
Switch  
Mesh  
IP  
MPLS  
Routing  
System  
Queues  
Files  
Log  
Radius  
Tools  
New Terminal  
MetaROUTER  
Partition  
Make Spout.rtf  
Manual  
New WinBox

File List

| File Name   | Type      | Size | Creation Time |
|-------------|-----------|------|---------------|
| flash       | disk      |      |               |
| flash/skins | directory |      | Jan/01/15     |

Package List

Check for Updates

| Name            | Version | Creation Time        |
|-----------------|---------|----------------------|
| routeros-mipsbe | 6.40.5  |                      |
| advanced+       | 6.40.5  | Oct/31/2017 13:05:15 |
| dhcp            | 6.40.5  | Oct/31/2017 13:05:15 |
| hotspot         | 6.40.5  | Oct/31/2017 13:05:15 |
| ipv6            | 6.40.5  | Oct/31/2017 13:05:15 |
| mpls            | 6.40.5  | Oct/31/2017 13:05:15 |
| ppp             | 6.40.5  | Oct/31/2017 13:05:15 |
| routing         | 6.40.5  | Oct/31/2017 13:05:15 |
| security        | 6.40.5  | Oct/31/2017 13:05:15 |
| system          | 6.40.5  | Oct/31/2017 13:05:15 |
| wireless        | 6.40.5  | Oct/31/2017 13:05:15 |

2 items 10.8 MiB of 16.0 MiB used 32% free

11 items

all\_packages-mipsbe-6.43.4.zip

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

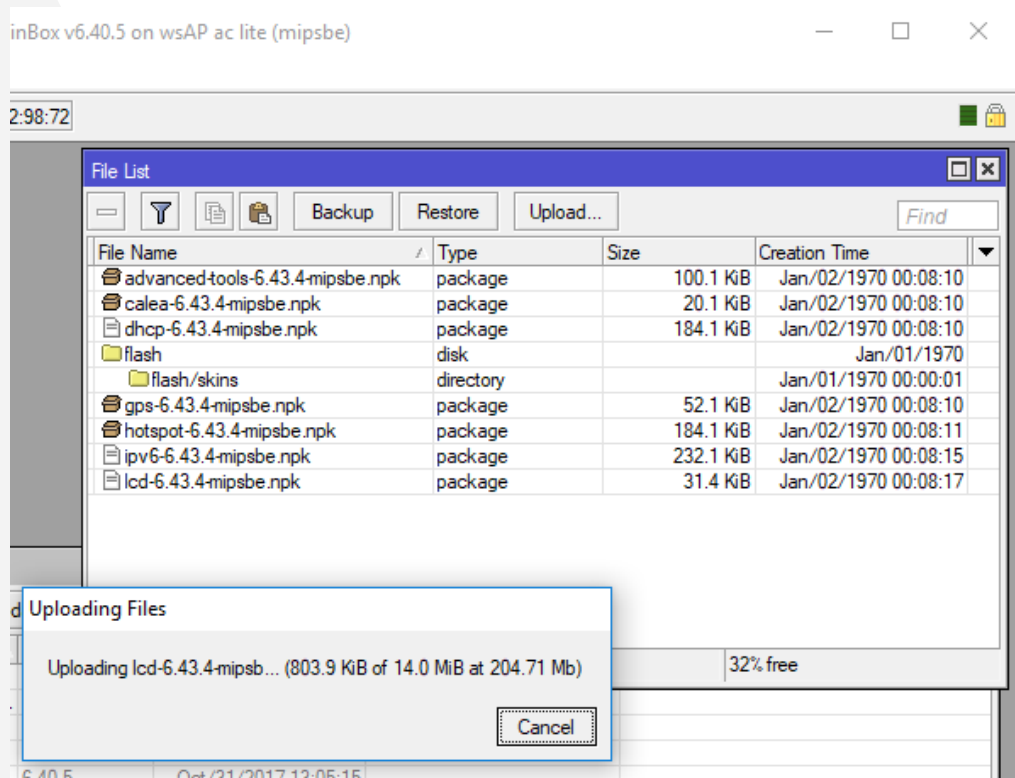
all\_packages-mipsbe-6.43.4.zip - ZIP archive, unpacked size 14,663,958 bytes

| Name                             | Size      | Packed    | Type     | Modified          | CRC32    |
|----------------------------------|-----------|-----------|----------|-------------------|----------|
| Local Disk                       |           |           |          |                   |          |
| advanced-tools-6.43.4-mipsbe.npk | 102,481   | 95,298    | NPK File | 10/18/2018 9:2... | 4FB30837 |
| calea-6.43.4-mipsbe.npk          | 20,561    | 15,814    | NPK File | 10/18/2018 9:2... | 79D73518 |
| dhcp-6.43.4-mipsbe.npk           | 188,497   | 182,396   | NPK File | 10/18/2018 9:2... | CC50A951 |
| gps-6.43.4-mipsbe.npk            | 53,329    | 45,861    | NPK File | 10/18/2018 9:2... | 7C572EA0 |
| hotspot-6.43.4-mipsbe.npk        | 188,497   | 180,631   | NPK File | 10/18/2018 9:2... | 456DAEF0 |
| ipv6-6.43.4-mipsbe.npk           | 237,649   | 232,732   | NPK File | 10/18/2018 9:2... | 31602BB0 |
| lcd-6.43.4-mipsbe.npk            | 57,425    | 51,181    | NPK File | 10/18/2018 9:2... | 598687D4 |
| lte-6.43.4-mipsbe.npk            | 1,990,737 | 1,985,757 | NPK File | 10/18/2018 9:2... | E3CCABA6 |
| mpls-6.43.4-mipsbe.npk           | 98,385    | 90,901    | NPK File | 10/18/2018 9:2... | 34C2BA4D |
| multicast-6.43.4-mipsbe.npk      | 73,809    | 67,107    | NPK File | 10/18/2018 9:2... | 7E635687 |
| ntp-6.43.4-mipsbe.npk            | 266,321   | 260,441   | NPK File | 10/18/2018 9:2... | 9DB37B1A |
| openflow-6.43.4-mipsbe.npk       | 77,905    | 71,318    | NPK File | 10/18/2018 9:2... | 2CA9B3F4 |
| ppp-6.43.4-mipsbe.npk            | 311,377   | 304,530   | NPK File | 10/18/2018 9:2... | DCAE8329 |
| routing-6.43.4-mipsbe.npk        | 122,961   | 118,775   | NPK File | 10/18/2018 9:2... | 942CA188 |
| security-6.43.4-mipsbe.npk       | 335,953   | 328,998   | NPK File | 10/18/2018 9:2... | 28E19981 |
| system-6.43.4-mipsbe.npk         | 7,600,915 | 7,510,043 | NPK File | 10/18/2018 9:2... | 62123090 |
| tr069-client-6.43.4-mipsbe.npk   | 139,345   | 133,530   | NPK File | 10/18/2018 9:2... | 73505232 |
| ups-6.43.4-mipsbe.npk            | 65,617    | 59,532    | NPK File | 10/18/2018 9:2... | 37EFF481 |
| user-manager-6.43.4-mipsbe.npk   | 868,433   | 861,628   | NPK File | 10/18/2018 9:2... | 569410F6 |
| wireless-6.43.4-mipsbe.npk       | 1,863,761 | 1,856,878 | NPK File | 10/18/2018 9:2... | 647E4F8D |

Total 14,663,958 bytes in 20 files



# Upgrade



## Upgrade

- ▶ Shkarkojme paketat nga MikroTik
- ▶ I hedhim tek "files"
- ▶ Restartojme ruterin

# Upgrade

98:72 (MikroTik) - WinBox v6.43.4 on wsAP ac lite (mipsbe)

board

Session: CC:2D:E0:D2:98:72

File List

File Name / Type Size Creation Time

|                             |           |          |                      |
|-----------------------------|-----------|----------|----------------------|
| flash                       | disk      |          | Jan/01/1970 02:00:07 |
| flash/skins                 | directory |          | Jan/01/1970 02:00:01 |
| flash/user-manager          | directory |          | Jan/02/1970 02:13:14 |
| flash/user-manager/logsqldb | file      | 6.0 KiB  | Jan/01/2002 03:00:03 |
| flash/user-manager/sqlqldb  | file      | 80.0 KiB | Jan/01/2002 03:00:09 |
| um-before-migration.tar     | tar file  | 17.0 KiB | Jan/01/2002 03:00:09 |

Routerboard

☒ Routerboard

Model: RouterBOARD wsAP 5Hac2nD

Serial Number: 925C0853DF23

Firmware Type: qca9531L

Factory Firmware: 3.41

Current Firmware: 3.41

Upgrade Firmware: 6.43.4

OK

Upgrade

Settings

USB Power Reset

Mode Button

Package List

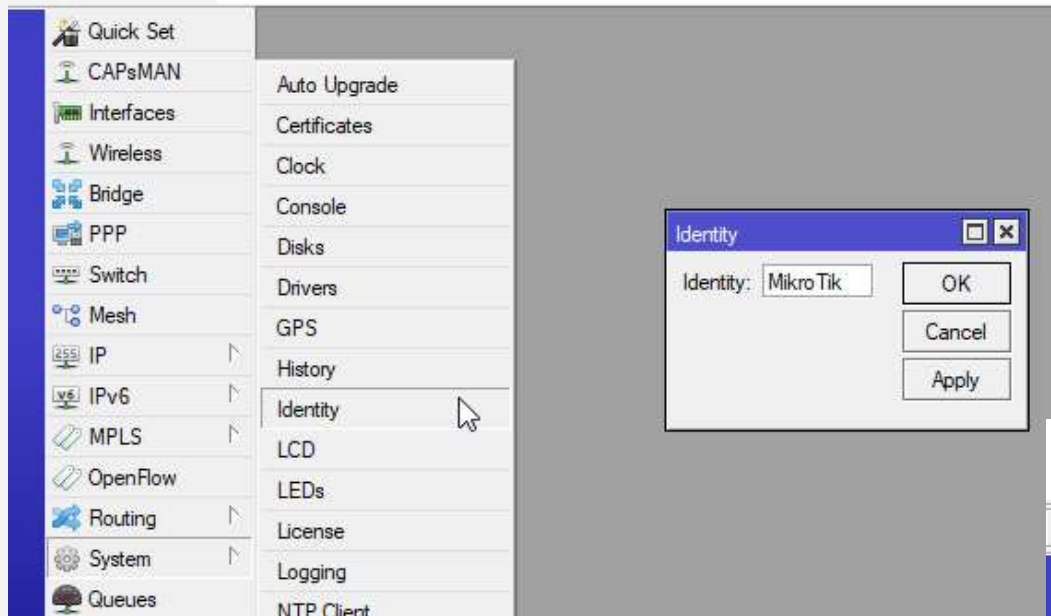
Check For Updates

| Name           | Version |
|----------------|---------|
| advanced-tools | 6.43.4  |
| calea          | 6.43.4  |
| dhcp           | 6.43.4  |
| gps            | 6.43.4  |
| hotspot        | 6.43.4  |
| ipv6           | 6.43.4  |
| lcd            | 6.43.4  |
| lte            | 6.43.4  |
| mpls           | 6.43.4  |

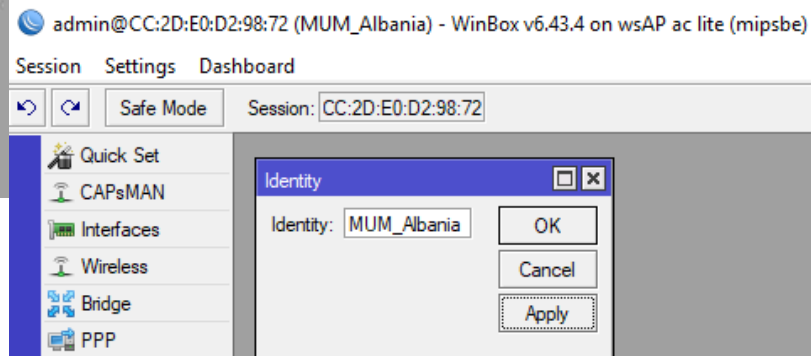
## Upgrade firmware

- ▶ Shkojme tek System – Routerboard
- ▶ Japim “Upgrade”

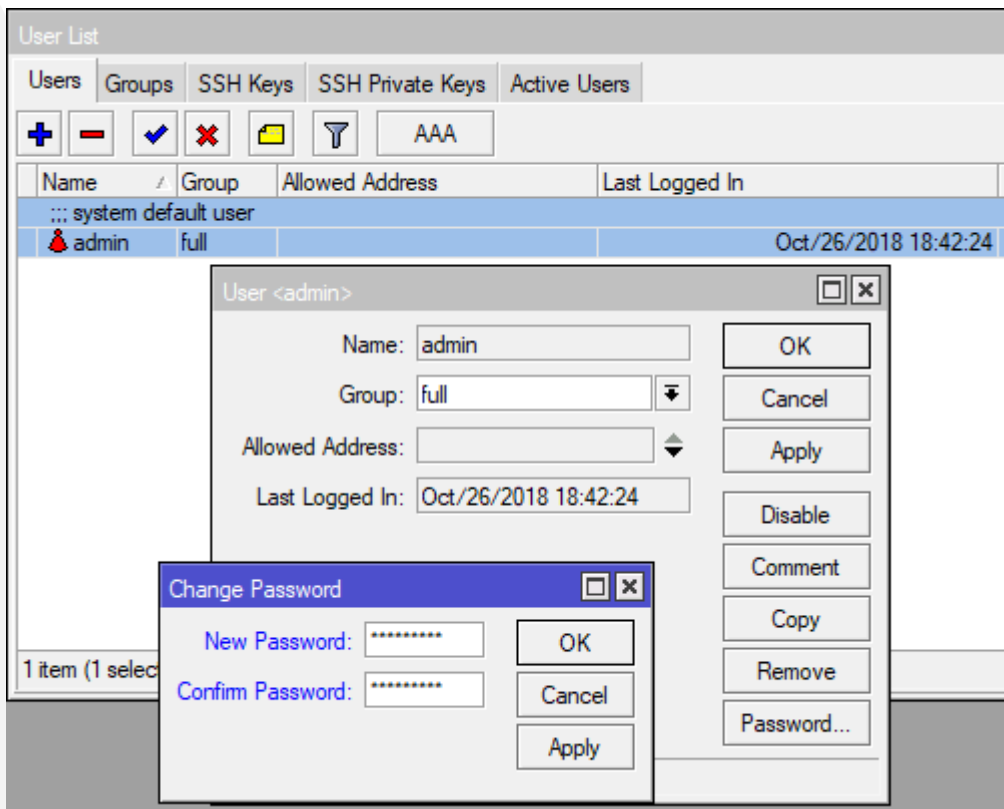
# Identiteti



- ▶ Shkojme tek System - Identity
- ▶ Vendosim identitetin



# Perdoruesit e sistemit - Users



- ▶ Shkojme tek System – Users
- ▶ Double click mbi perdoruesin
- ▶ Klikojme mbi password
- ▶ Vendosim Passwordin
- ▶ OK

# Interfaces

admin@CC:2D:E0:D2:98:72 (MUM\_Albania) - WinBox v6.43.4 on wsAP ac lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: CC:2D:E0:D2:98:72

Quick Set  
CAPsMAN  
Interfaces  
Wireless  
Bridge  
PPP  
Switch  
Mesh  
IP  
IPv6  
MPLS  
OpenFlow

### Interface List

Interface Interface List Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding ...

+ - [ ] [X] [ ] [ ] Detect Internet Find

|   | Name   | Type                     | Actual MTU | L2 MTU | Tx        | Rx |
|---|--------|--------------------------|------------|--------|-----------|----|
| R | ether1 | Ethernet                 | 1500       | 1598   | 57.6 kbps |    |
|   | ether2 | Ethernet                 | 1500       | 1598   | 0 bps     |    |
|   | ether3 | Ethernet                 | 1500       | 1598   | 0 bps     |    |
| X | wlan1  | Wireless (Atheros AR9... | 1500       | 1600   | 0 bps     |    |
| X | wlan2  | Wireless (Atheros AR9... | 1500       | 1600   | 0 bps     |    |

5 items

# Adresat IP

admin@CC:2D:E0:D2:98:72 (MUM\_Albania) - WinBox v6.43.4 on wsAP ac lite (mipsbe)

Session Settings Dashboard

Safe Mode Session: CC:2D:E0:D2:98:72

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- IPv6
- MPLS
- OpenFlow
- Routing
- System
- Quotas

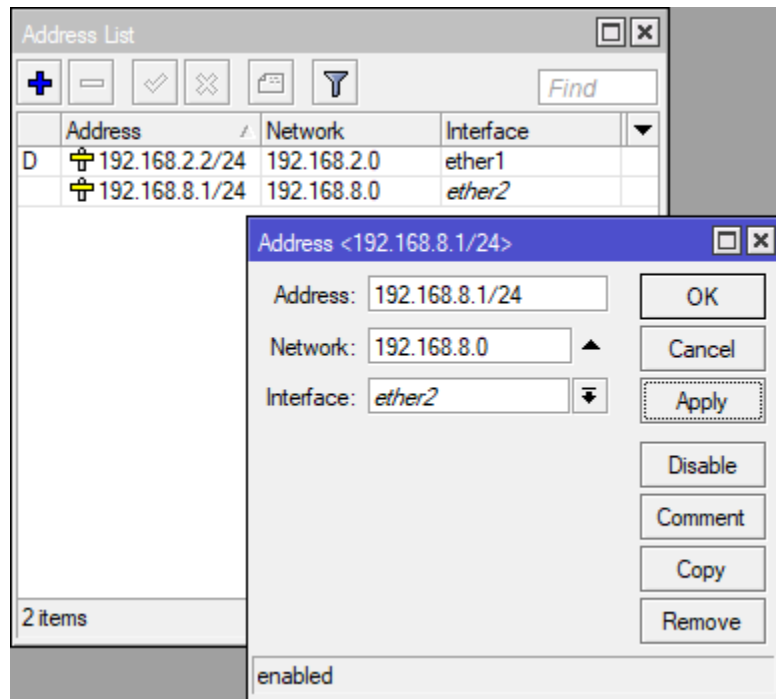
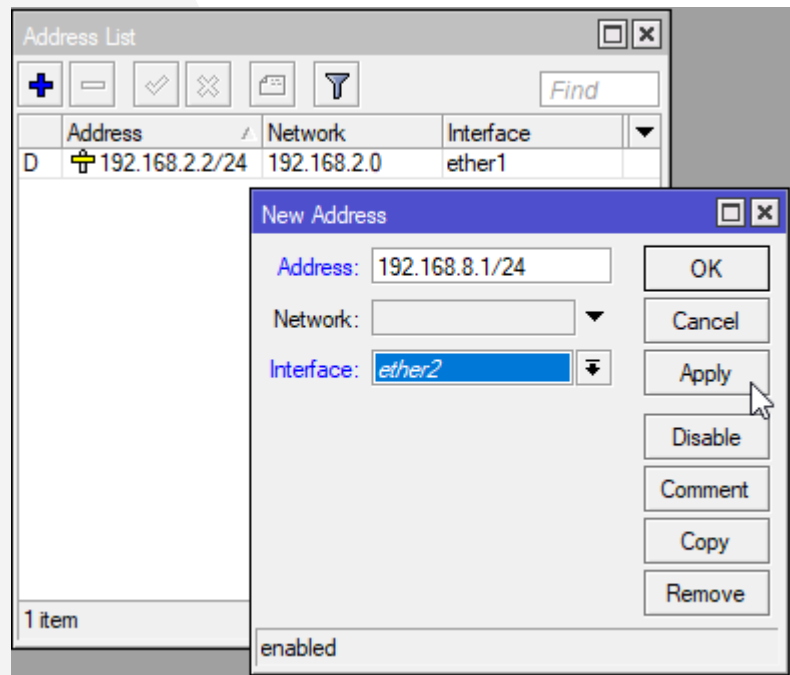
- ARP
- Accounting
- Addresses
- Cloud
- DHCP Client
- DHCP Relay
- DHCP Server
- DNS
- Firewall

### Address List

|   | Address        | Network     | Interface |  |
|---|----------------|-------------|-----------|--|
| D | 192.168.2.2/24 | 192.168.2.0 | ether1    |  |

1 item

# Adresat IP - Statike



# Adresat IP - Statike

**Network and Subnet Helper**

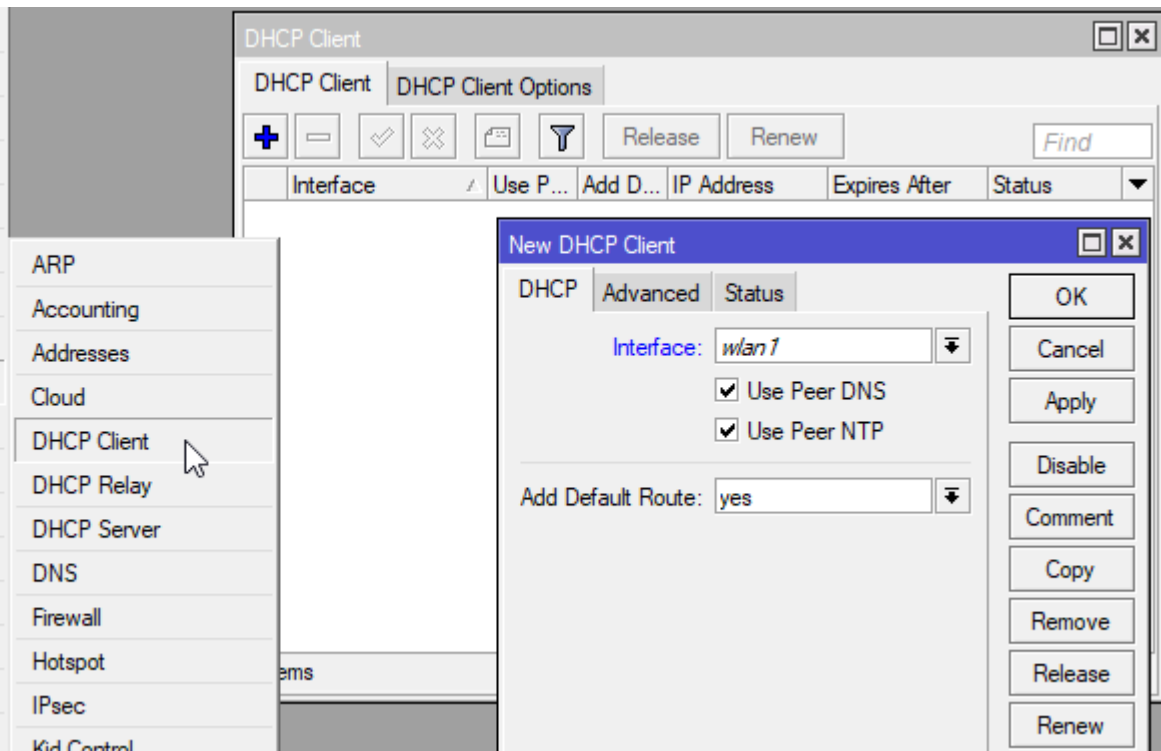
| MASK (DEC):  |              | .252 |    | .248 |    | .240 |    | .224 |   | .192 |   | .128 |   | .0  |   |
|--------------|--------------|------|----|------|----|------|----|------|---|------|---|------|---|-----|---|
| MASK (BITS): |              | /30  |    | /29  |    | /28  |    | /27  |   | /26  |   | /25  |   | /24 |   |
| SUBNET BITS: |              | 2    |    | 3    |    | 4    |    | 5    |   | 6    |   | 7    |   | 8   |   |
| N=Network:   | B=Broadcast: | N    | B  | N    | B  | N    | B  | N    | B | N    | B | N    | B | N   | B |
| 00000000     | 00000011     | 0    | 3  | 0    |    | 0    |    | 0    |   | 0    |   | 0    |   | 0   |   |
| 00000100     | 00000111     | 4    | 7  |      | 7  |      |    |      |   |      |   |      |   |     |   |
| 00001000     | 00001011     | 8    | 11 | 8    |    |      |    |      |   |      |   |      |   |     |   |
| 00001100     | 00001111     | 12   | 15 |      | 15 |      | 15 |      |   |      |   |      |   |     |   |
| 00010000     | 00010011     | 16   | 19 | 16   |    | 16   |    |      |   |      |   |      |   |     |   |
| 00010100     | 00010111     | 20   | 23 |      | 23 |      |    |      |   |      |   |      |   |     |   |

**Shembull:** Nje IP 80.78.74.13 me subnet 255.255.255.240, do te vendoset ne MikroTik si 80.78.74.13/28, do te kete si network: 80.78.74.0, si broadcast: 80.78.74.15, si gateway: 80.78.74.1

**Shembull 2:** Nje IP 80.89.45.11 me subnet 255.255.255.248, do te vendoset ne MikroTik si.....

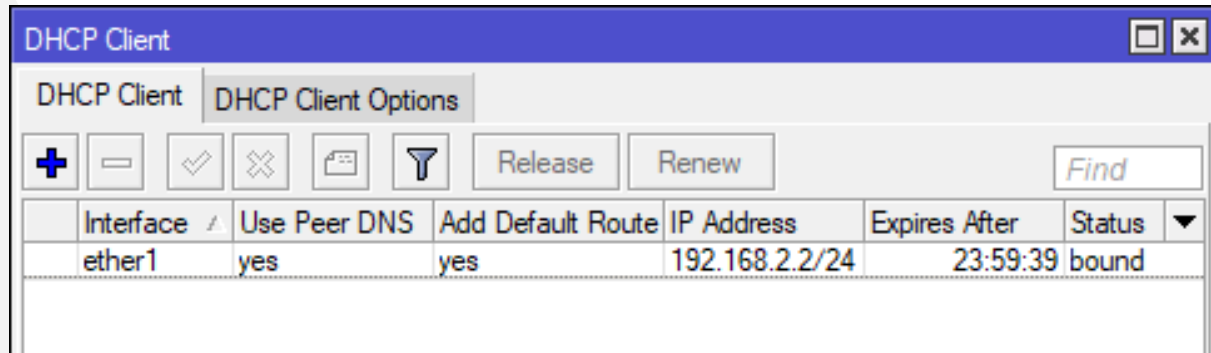


# Adresat IP - Dinamike



- ▶ IP – DHCP Client
- ▶ Japim +
- ▶ Zgjedhim Nderfaqjen
- ▶ Japim OK

# Adresat IP - Dinamike



# Routes

The screenshot shows two windows from a network management application. The 'Route List' window in the background displays a table of routes:

|     | Dst. Address   | Gateway                       | Distance | Rd |
|-----|----------------|-------------------------------|----------|----|
| DAS | 0.0.0.0/0      | 192.168.2.1 reachable bridge1 | 1        |    |
| DAC | 192.168.2.0/24 | bridge1 reachable             | 0        |    |

The 'New Route' window in the foreground is open, showing the 'General' tab. The fields are configured as follows:

- Dst. Address: 0.0.0.0/0
- Gateway: 192.168.2.1
- Check Gateway: (dropdown menu)
- Type: unicast
- Distance: (dropdown menu)
- Scope: 30
- Target Scope: 10
- Routing Mark: (dropdown menu)
- Pref. Source: (dropdown menu)

On the right side of the 'New Route' window, there is a vertical stack of buttons: OK, Cancel, Apply, Disable, Comment, Copy, and Remove. A mouse cursor is pointing at the 'Apply' button.

- ▶ IP – Routes
- ▶ Per nje Route te caktuar japim +, dhe shtojme Dst. Address dhe Gateway
- ▶ Japim OK

## DNS

The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar with various configuration categories. The main window is divided into two panes. The left pane shows the 'DHCP Client' configuration for the 'ether1' interface, with 'Use Peer DNS' checked. The right pane shows the 'DNS Settings' dialog box.

**Sidebar:**

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- IPv6
- MPLS
- OpenFlow
- Routing
- System
- Queues
- Files
- Log

**DHCP Client Configuration:**

| Interface | Use Peer DNS |
|-----------|--------------|
| ether1    | yes          |

**DNS Settings:**

- Servers: (empty)
- Dynamic Servers: 8.8.8.8, 80.78.66.66
- ☐ Allow Remote Requests
- Max UDP Packet Size: 4096
- Query Server Timeout: 2.000 s
- Query Total Timeout: 10.000 s
- Max. Concurrent Queries: 100
- Max. Concurrent TCP Sessions: 20
- Cache Size: 2048 KiB
- Cache Max TTL: 7d 00:00:00
- Cache Used: 18 KiB

- ▶ IP – DNS
- ▶ Vendorsim IP e serverave
- ▶ Japim OK

The screenshot shows the 'New DNS Static Entry' dialog box. It contains fields for Name, Regexp, Address, and TTL, along with buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

**New DNS Static Entry:**

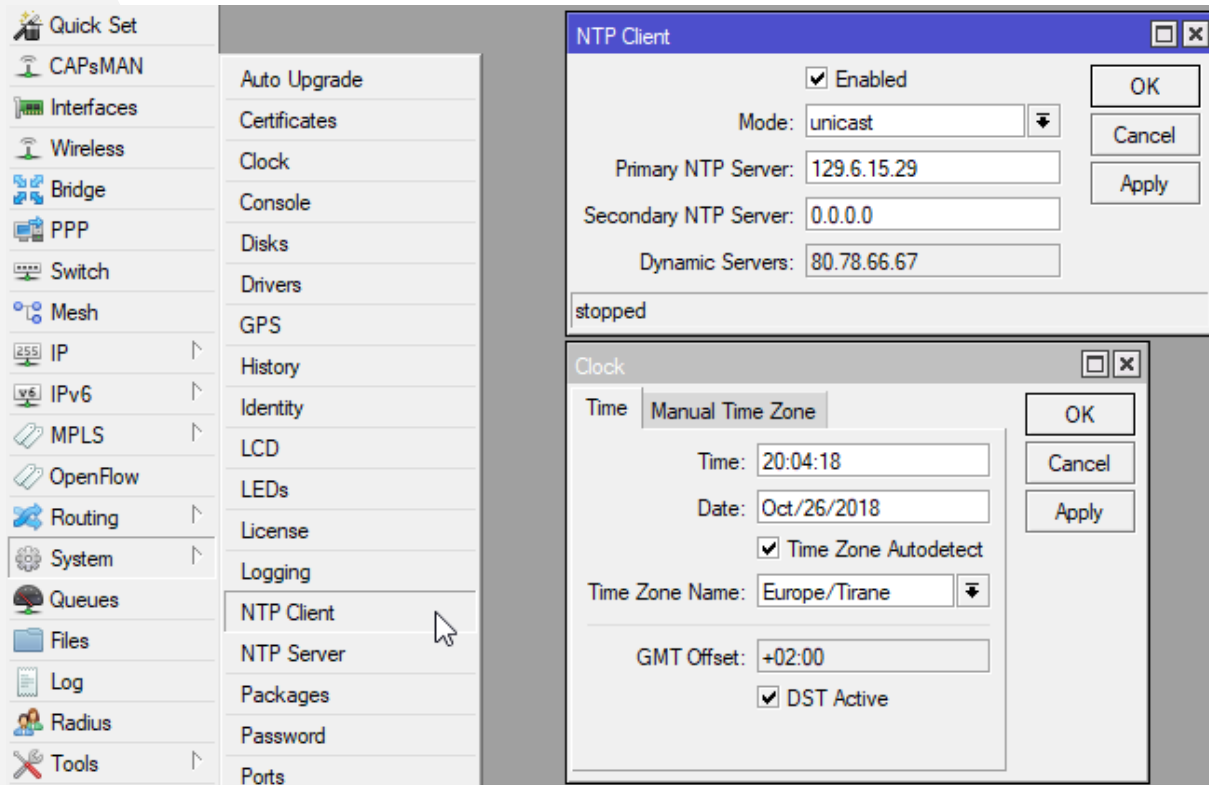
- Name: kiufiu.com
- Regexp: (empty)
- Address: 192.168.1.2
- TTL: 1d 00:00:00 s

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove.

0 items

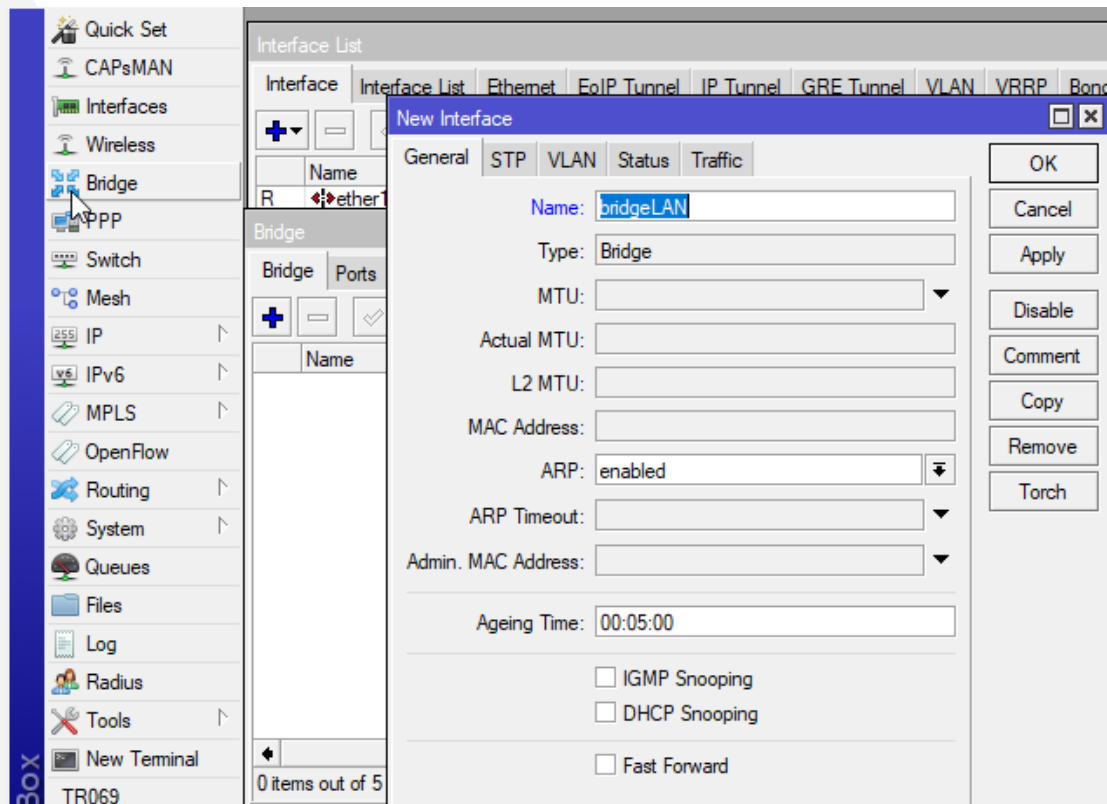
enabled

# NTP – Network Time Protocol

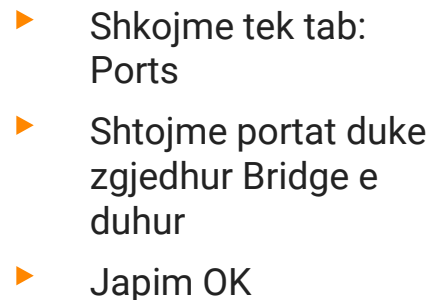


- ▶ System – NTP Client
  - ▶ Vendosim IP e serverave
  - ▶ Japim OK
- 
- ▶ System – Clock
  - ▶ Zgjedhim Time Zone
  - ▶ Japim OK

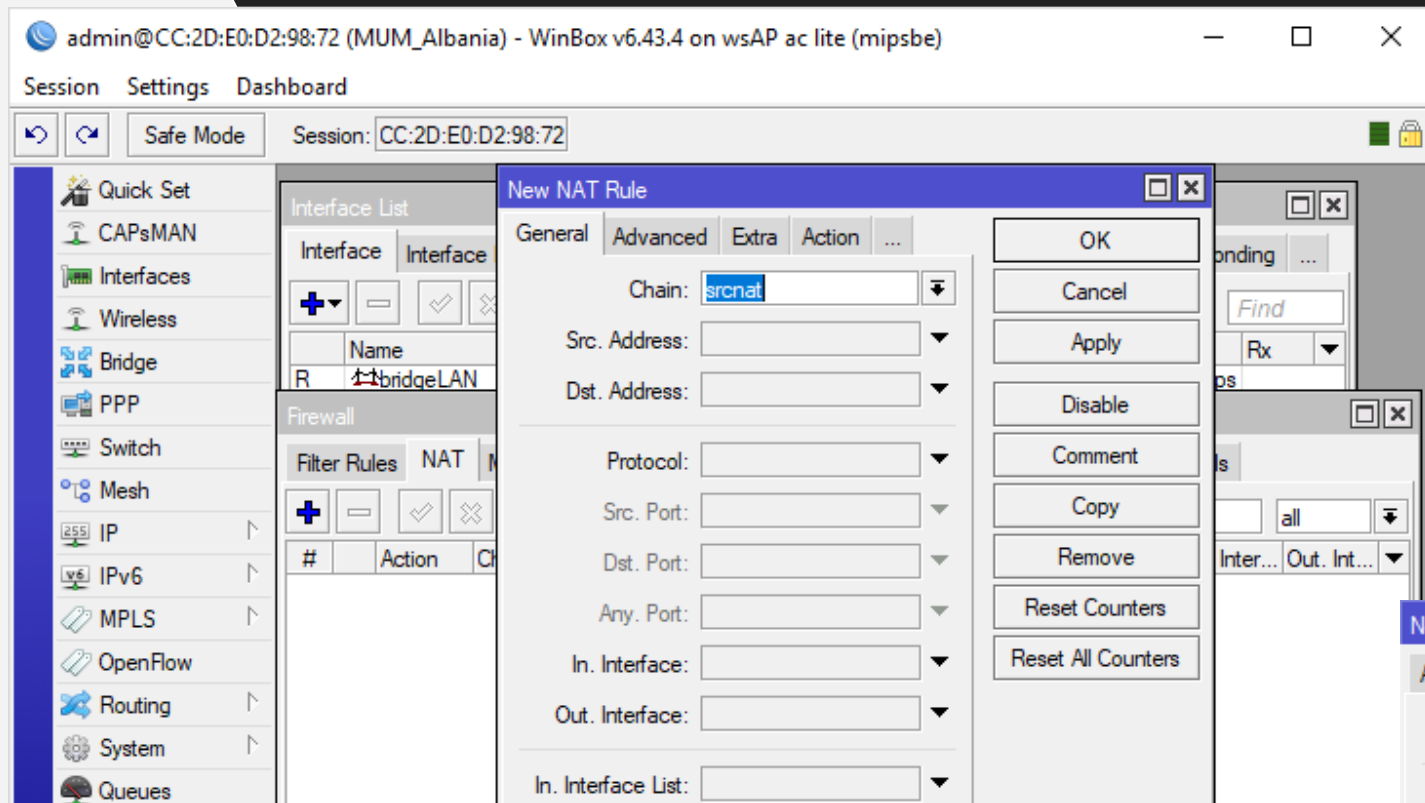
# Bridge



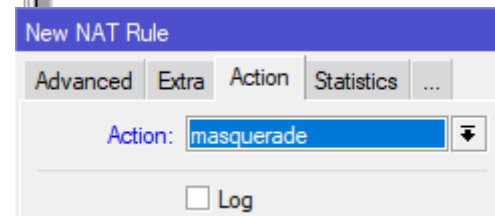
- ▶ Bridge
- ▶ Shtojme nje bridge
- ▶ I vendosim nje emer dallues
- ▶ Japim OK



# Masquerade



- ▶ Shkojme tek IP - Firewall
- ▶ Tab NAT
- ▶ Shtojme nje Rule te ri
- ▶ Chain=srcnat, action=masquerade





## Diagrama (Skema)

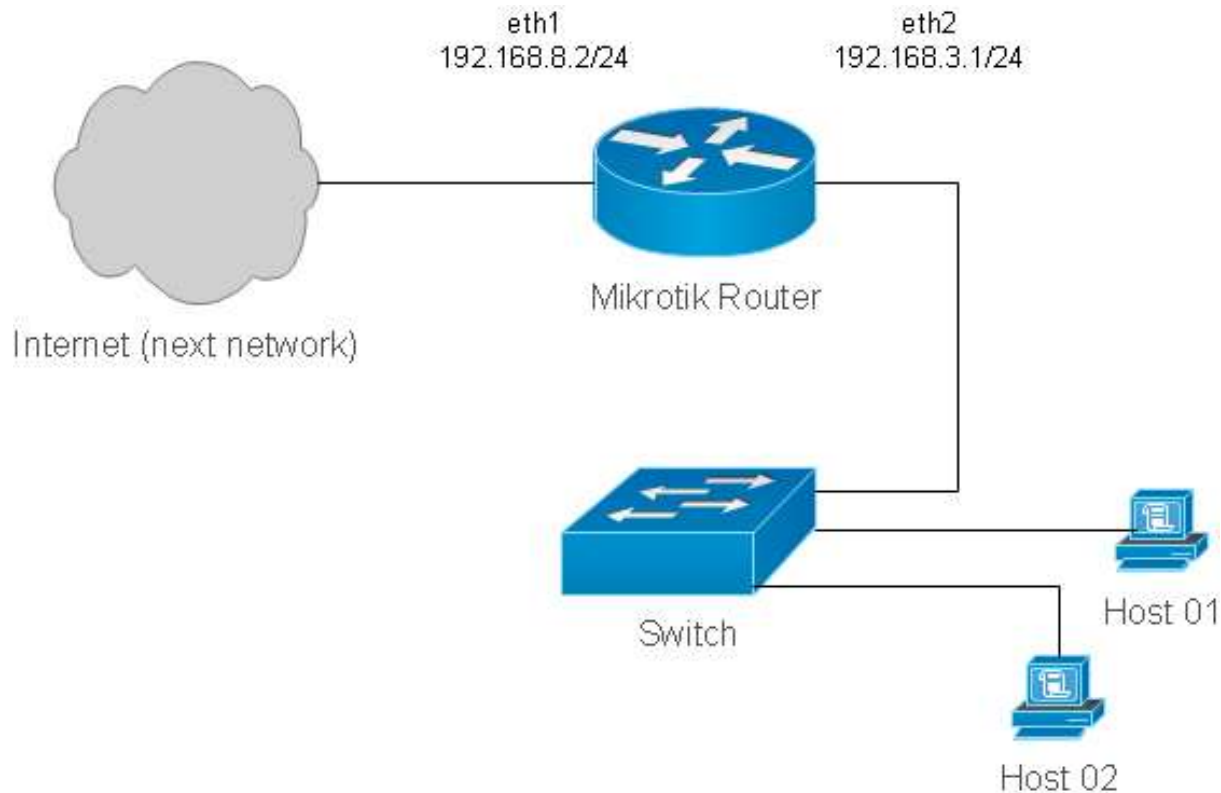
“Nuk duhet te nisim asnjehere nje konfigurim pa pasur te qarte pikat thelbesore te rrjetit ne fjale. Vizatimi i nje skeme te thjeshte ndihmon shume e na kthjellon idete”

# Ruteri me i thjeshte

**Shembull:** Konfigurojme nje ruter me

IP: 192.168.8.2/24 tek ether1

IP: 192.168.3.1/24 tek ether2



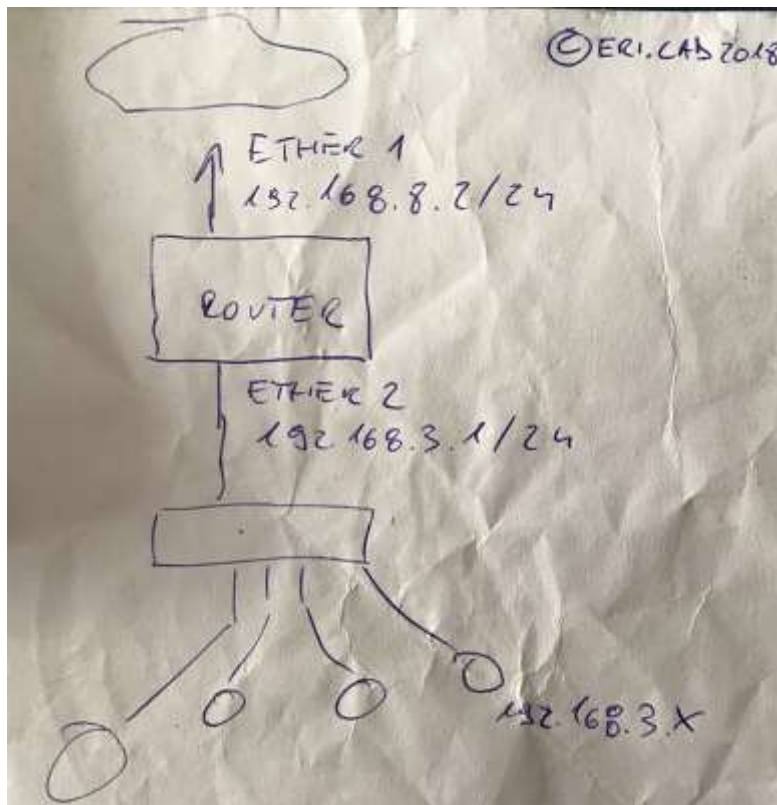
IP: 192.168.8.2/24 tek ether1

IP: 192.168.3.1/24 tek ether2

Interface List

|   | Name   | Type                      | Actual MTU | L2 MTU | Tx        |
|---|--------|---------------------------|------------|--------|-----------|
| R | ether1 | Ethernet                  | 1500       | 1598   | 69.4 kbps |
|   | ether2 | Ethernet                  | 1500       | 1598   | 0 bps     |
|   | ether3 | Ethernet                  | 1500       | 1598   | 0 bps     |
| X | wlan1  | Wireless (Atheros AR9130) | 1500       | 1600   | 0 bps     |
| X | wlan2  | Wireless (Atheros AR9130) | 1500       | 1600   | 0 bps     |

5 items



# 3. Wireless

# Wireless

The screenshot shows the WinBox WinBox interface. The top status bar displays: Safe Mode, Session: 192.168.2.2, Uptime: 03:19:13, Memory: 39.7 MiB, CPU: 4%, Date: Oct/28/2018, Time: 11:59:47. The left sidebar contains a tree view with categories like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, IPv6, MPLS, OpenFlow, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, TR069, and MetaROUTER. The main window is titled 'Interface <wlan1>' and has tabs for General, Wireless, HT, WDS, Nstreme, NV2, Status, and Traffic. The 'General' tab is active, showing configuration for the 'wlan1' interface. The 'Wireless Tables' section on the left lists 'wlan1' and 'wlan2'. The 'General' tab settings include: Mode: ap bridge, Band: 2GHz-B/G, Channel Width: 20MHz, Frequency: 2412 MHz, SSID: MikroTik, Scan List: default, Wireless Protocol: any, Security Profile: default, WPS Mode: push button, Bridge Mode: enabled, VLAN Mode: no tag, and VLAN ID: 1. At the bottom, there are checkboxes for 'Default Authenticate' (checked), 'Default Forward' (checked), and 'Hide SSID' (unchecked). On the right side of the 'General' tab, there are buttons for OK, Cancel, Apply, Enable, Comment, Advanced Mode, Torch, WPS Accept, WPS Client, Setup Repeater, Scan..., Freq. Usage..., Align..., Sniff..., Snooper..., and Reset Configuration.

▶ Ne winbox klikojme mbi Wireless

▶ Tek dritarja qe shfaqet zgjedhim interface me te cilen do te punojme

# Wireless

Session: 192.168.2.2 Uptime: 03:21:32 Memory: 39.7 MiB CPU: 5% Date: Oct/28/2018 Time: 12:02:06

Wireless Tables

| WiFi Interfaces |   |
|-----------------|---|
| W60G            |   |
| +               | - |
| ✓               | ✗ |
| Name            |   |
| X wlan1         |   |
| X wlan2         |   |

Interface <wlan1>

General Wireless HT WDS Nstreme NV2 Status Traffic

Mode: ap bridge

Band: 2GHz-B/G

Channel Width: 2GHz-B  
2GHz-only-G  
2GHz-B/G

Frequency: 2GHz-only-N  
2GHz-B/G/N  
2GHz-G/N

SSID:

OK  
Cancel  
Apply  
Enable

Routeri me te cilin po punojme ka dy karta wireless:

- ▶ wlan1 2.4Ghz
- ▶ wlan2 5Ghz

Session: 192.168.2.2 Uptime: 03:22:33 Memory: 39.7 MiB CPU: 4% Date: Oct/28/2018 Time: 12:03:07

Wireless Tables

| WiFi Interfaces |   |
|-----------------|---|
| W60G            |   |
| +               | - |
| ✓               | ✗ |
| Name            |   |
| X wlan1         |   |
| X wlan2         |   |

Interface <wlan2>

General Wireless HT WDS Nstreme NV2 Status Traffic

Mode: ap bridge

Band: 5GHz-A

Channel Width: 5GHz-A  
5GHz-only-N  
5GHz-A/N  
5GHz-A/N/AC  
5GHz-only-AC  
5GHz-N/AC

Frequency:

SSID:

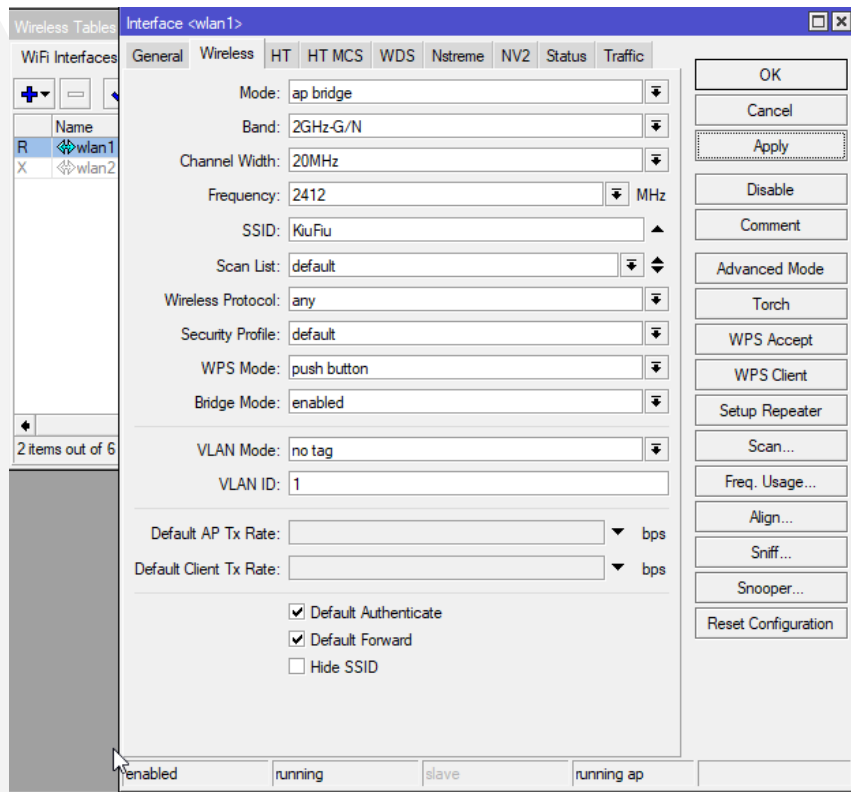
Scan List: default

Wireless Protocol: any

Security Profile: default

OK  
Cancel  
Apply  
Enable  
Comment  
Advanced Mode  
Torch  
WPS Accept

# Wireless



Per nje AP te thjeshte zgjedhim:

- ▶ Mode: ap bridge
- ▶ Band: 2GHZ-G/N
- ▶ Channel Width: 20MHz
- ▶ Frequency: 2412
- ▶ SSID: KiuFiu
- ▶ Security Profile: default

# Wireless – Security Profiles

admin@192.168.2.2 (MUM\_Albania) - WinBox v6.43.4 on wsAP ac lite (mipsbe)

Session Settings Dashboard

Inline Comments 2.2 Uptime: 03:30:55 Memory: 39.1 MiB CPU: 4% Date: Oct/28/2018

Hide Passwords

WiFi Interfaces W60G Station Nstream Dual Access List Registration Connect List Security Profiles

Name \* default

Security Profile <default>

General RADIUS EAP Static Keys

Name: default

Mode: dynamic keys

Authentication Types: ☒ WPA PSK ☒ WPA2 PSK  
☐ WPA EAP ☐ WPA2 EAP

Unicast Ciphers: ☒ aes ccm ☐ tkip

Group Ciphers: ☒ aes ccm ☐ tkip

WPA Pre-Shared Key: .....

WPA2 Pre-Shared Key: .....

OK Cancel Apply Comment Copy Remove

- ▶ Tek wireless interfaces shkojme tek “Security Profiles”
- ▶ Vendosim te dhenat



# 4. Monitorimi

# RESOURCES

## ► System – Resources

Resources

|                             |                      |     |
|-----------------------------|----------------------|-----|
| Uptime:                     | 00:45:43             | OK  |
| Free Memory:                | 40.8 MiB             | PCI |
| Total Memory:               | 64.0 MiB             | USB |
| CPU:                        | MIPS 24Kc V7.4       | CPU |
| CPU Count:                  | 1                    | IRQ |
| CPU Frequency:              | 650 MHz              |     |
| CPU Load:                   | 1 %                  |     |
| Free HDD Space:             | 3684 KiB             |     |
| Total HDD Size:             | 16.0 MiB             |     |
| Sector Writes Since Reboot: | 139                  |     |
| Total Sector Writes:        | 5 162                |     |
| Bad Blocks:                 | 0.0 %                |     |
| Architecture Name:          | mipsbe               |     |
| Board Name:                 | wsAP ac lite         |     |
| Version:                    | 6.43.4 (stable)      |     |
| Build Time:                 | Oct/17/2018 06:37:48 |     |
| Factory Software:           | 6.40.5               |     |

68.2.2 (MUM\_Albania) - WinBox v6.43.4 on wsAP ac lite (mipsbe)

### Dashboard

- Add Time
- Add Date
- Add CPU
- Add Memory
- Add Uptime

Uptime: 00:47:09 Memory: 40.8 MiB CPU: 0% Date: Oct/28/2018 Time: 09:27:42

# SNMP

SNMP Settings

☒ Enabled

OK

Contact Info: KiuFiu@ens-al.com

Cancel

Location: KullaQafaBarit

Apply

Engine ID: ▼

Communities

Trap Target: ▲▼

Trap Community: public ▼

Trap Version: 1 ▼

Trap Generators: temp-exception ▼▲

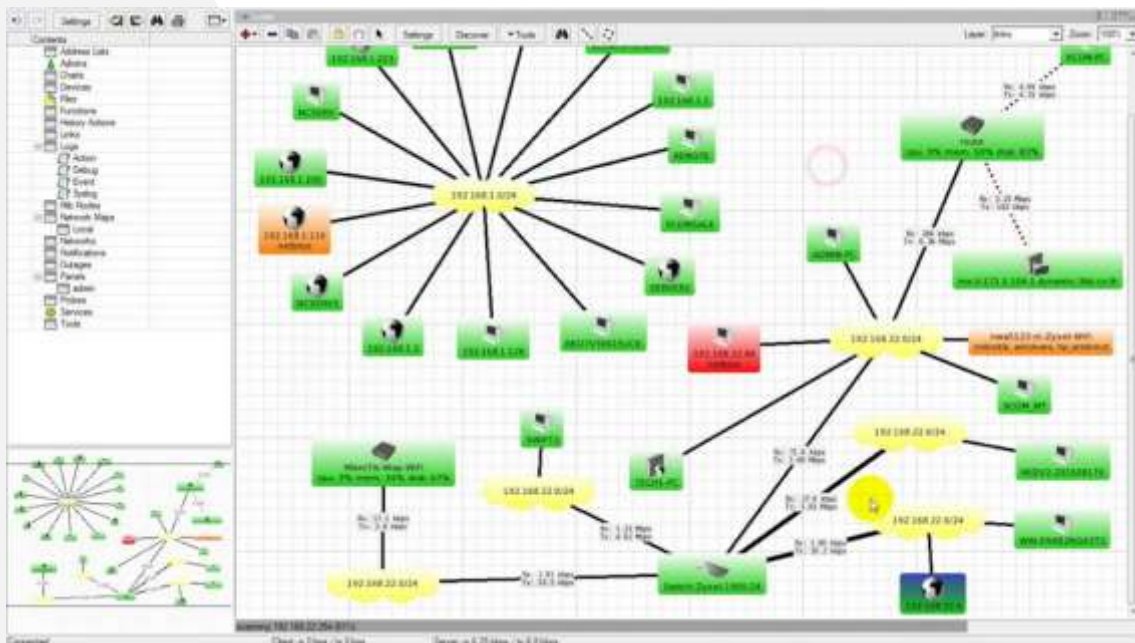
Trap Interfaces: ▲▼

Src. Address: ::

## SIMPLE NETWORK MONITORING PROTOCOL

- ▶ Krijuar 1989
- ▶ Funksionon ne baze: Manaxher – Agjent
- ▶ Nga MikroTik suportohen vers: v1-v3

# THE DUDE



Sistem monitorimi falas nga MikroTik

Mund te instalohet ne:

- ▶ CCR
- ▶ CHR
- ▶ X86
- ▶ RB3011/1100AHx4 Dude Edition

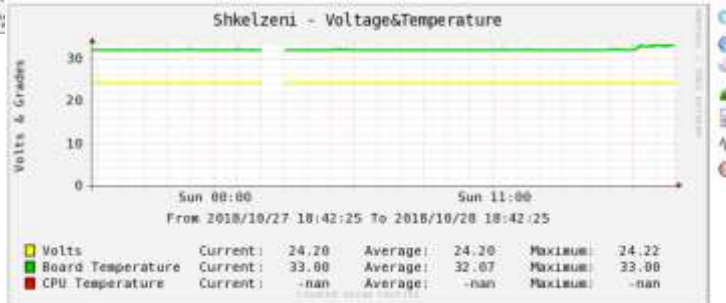
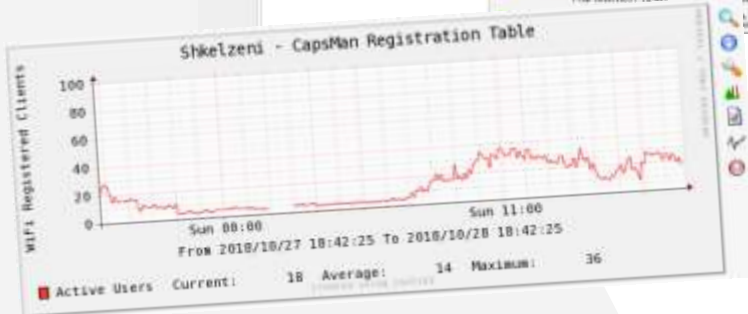


*Me shume info: Prezantim Pauls Jukonis, MikroTik ne MUM Vietnam 2017*

## CACTI



- ▶ Sistem i plote open-source per monitorim
- ▶ Mund te instalohet ne X86 ose X64
- ▶ Set i madh pluginesh, si pershembull: syslog



Me shume info: <https://www.youtube.com/watch?v=tH-smIBg1Gg>

Navigation: Home, Change Logs, Documentation, FAQ, HowTos, Contributing, Plugins, Templates/Packages, Scripts

Search:  Go Search

Toolbox: What links here, Upload file, Recent Changes, Special Pages, Printable Version, Permanent link, Cite this Article

cacti forums documentation Login

documentation and howtos

article discussion show pagesource old revisions

## MikroTik

**USERTEMPLATE:** mikrotik  
**AUTHOR:** guack20  
**DESCRIPTION:**  
 MikroTik host template. Work started from mojito, edited for the new Odis, added voltage+temperature and many other fixes. Work still in progress. Welcomed everyone to collaborate  
**Cacti:** 0.8.8a, 0.8.8f  
**HOMEPAGE:** <https://www.youtube.com/channel/UCLEzRukQK4Qo1TG1gsOdw>  
**DATE:** Started 06/February/2015, Last addition: 01/January/2017  
**EMAIL:** erion@gmail.com  
**INCLUDES:** yes  
**SCRIPT:** PHP Script Server  
**TEMPLATES:** MikroTik, Router, Wireless

### Download

| Version | File                                                           |
|---------|----------------------------------------------------------------|
| 0.8.8a  | <a href="#">cacti_host_template_mikrotik_0.8.8a_rev1.2.zip</a> |
| 0.8.8a  | <a href="#">cacti_host_template_mikrotik_0.8.8a_rev1.1.zip</a> |
| 0.8.8f  | <a href="#">cacti_host_template_mikrotik_rev1.0.zip.zip</a>    |

### Installation

Table of Contents: MikroTik, Download, Installation, Screenshots



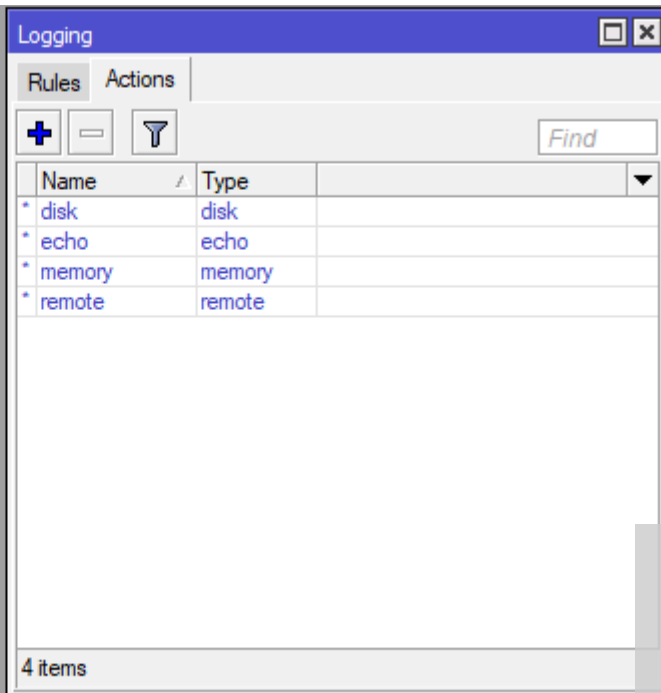
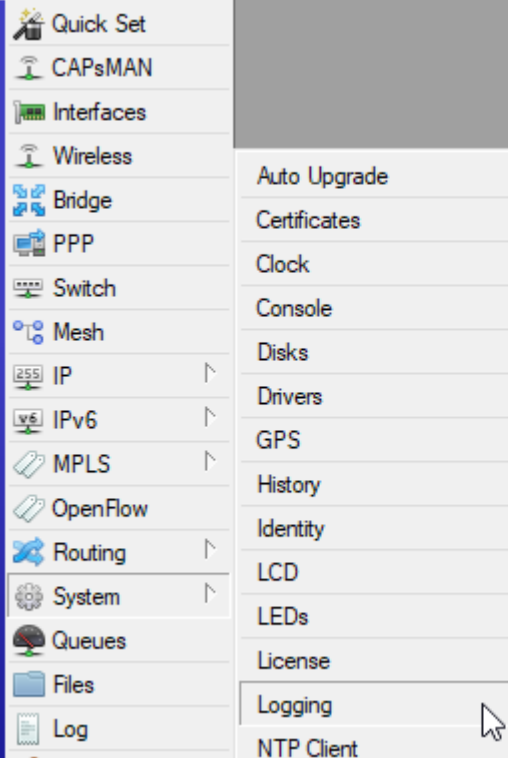
# ZABBIX

## ZABBIX

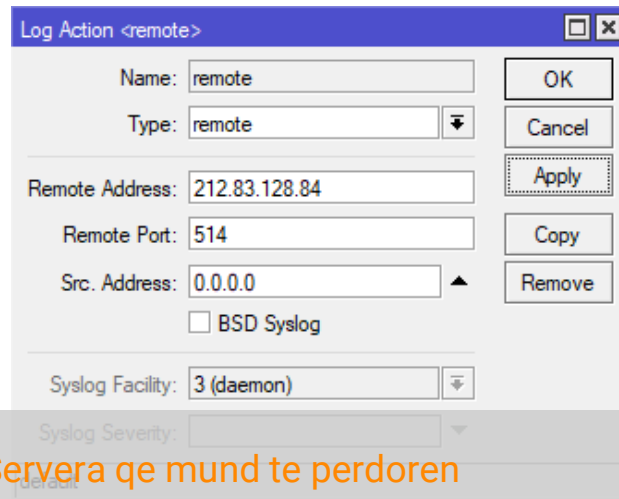
- ▶ Sistem i plote open-source per monitorim
- ▶ Mund te instalohet ne X86 ose X64
- ▶ Agjente te gatshem per MikroTik RouterOS



# Logging



- ▶ System – Logging
- ▶ Action – Remote

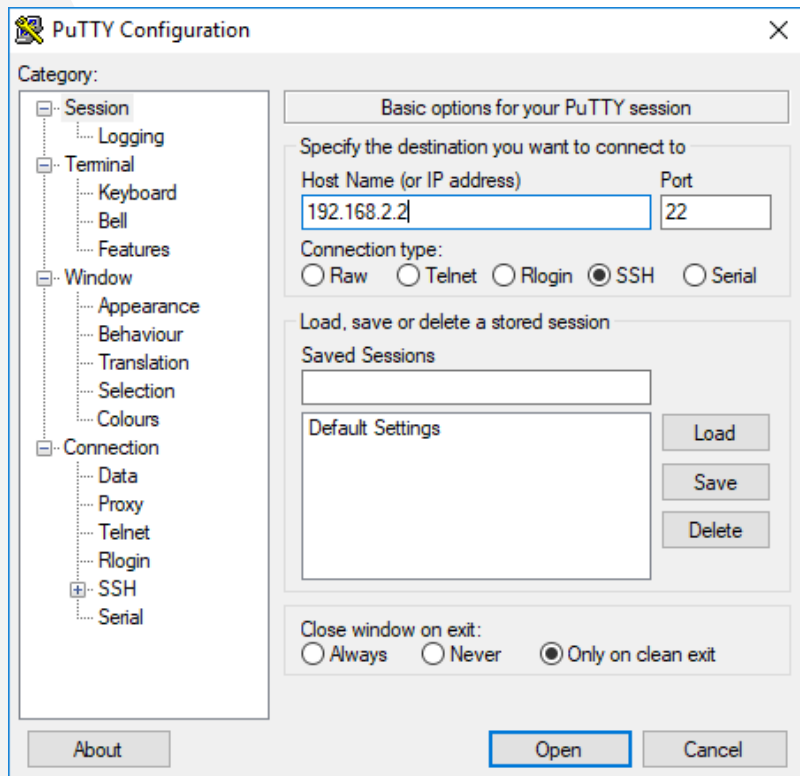


Servera qe mund te perdoren

- ▶ Dude, Nagios, Syslog-Ng (lin)
- ▶ Kiwi-syslog, Paessler PRTG (win)

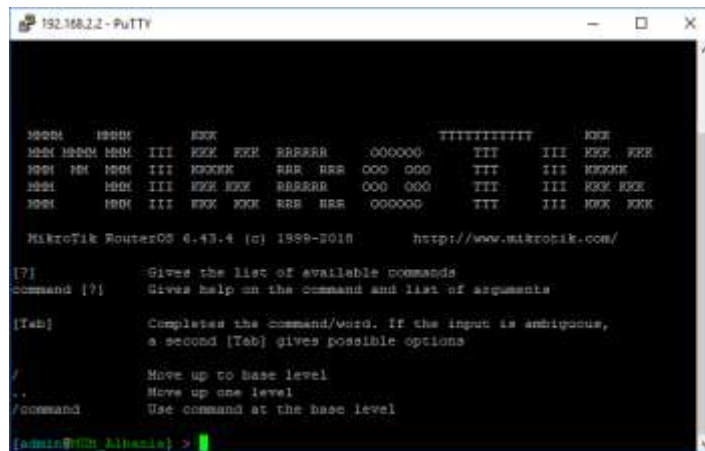


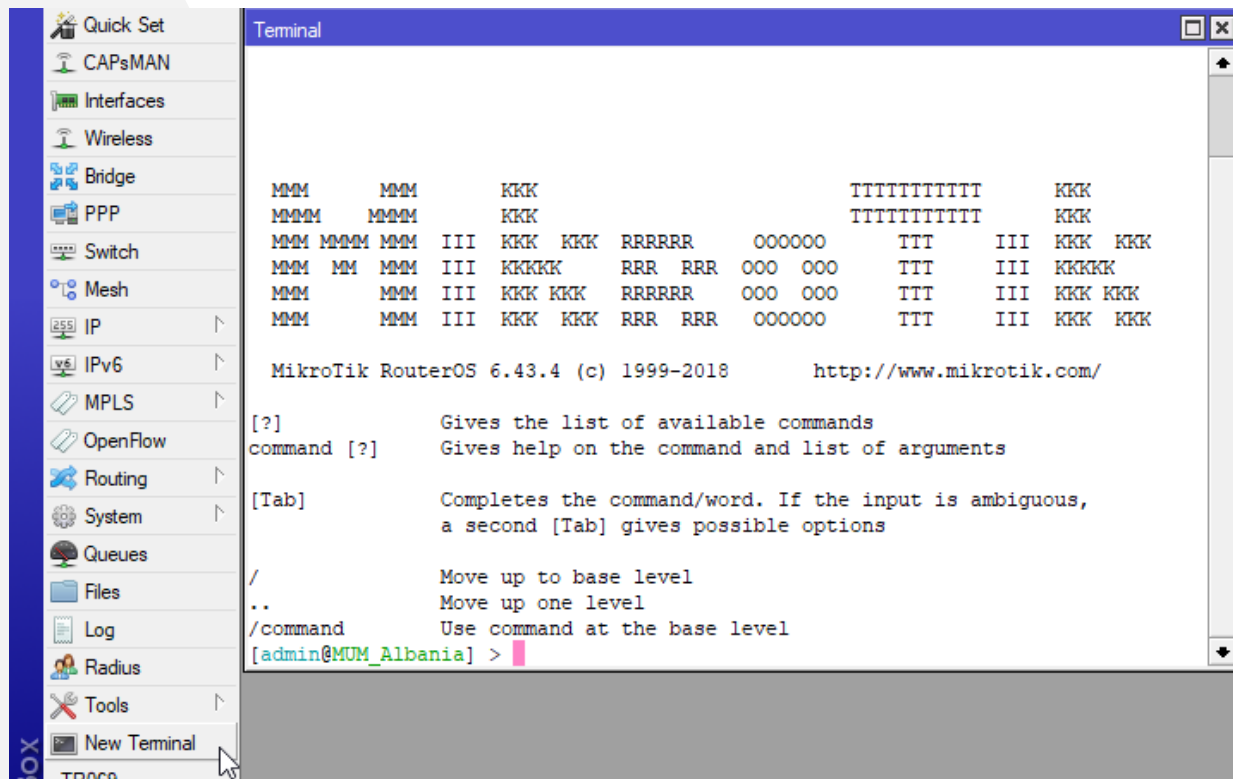
# 5. CLI



## COMMAND LINE INTERFACE

- ▶ Telnet
- ▶ SSH
- ▶ Serial
- ▶ Keyboard
- ▶ Winbox – New Terminal





► Winbox – New Terminal

Quick Set  
CAPsMAN  
Interfaces  
Wireless  
Bridge  
PPP  
Switch  
Mesh  
IP  
IPv6  
MPLS  
OpenFlow  
Routing  
System  
Queues  
Files  
Log

Neighbor List

Discovery Settings

| Interface | IP Address    | MAC Address       | Identity  | Platform  | Version       | Board Na... | Il |
|-----------|---------------|-------------------|-----------|-----------|---------------|-------------|----|
| ether1    |               | CC:2D:E0:28:5C:6E | HotiNew   | Mikro Tik | 6.39.2 (st... | RB952Ui...  | n  |
| ether1    | 192.168.2.3   | 64:D1:54:88:9B:F8 | HoTi      | Mikro Tik | 6.39.2 (st... | RB952Ui...  | n  |
| ether1    | 192.168.2.42  | CC:2D:E0:28:58:4B | MUM_CA... | Mikro Tik | 6.43.2 (st... | RB952Ui...  | n  |
| ether1    | 192.168.2.203 | D4:CA:6D:E8:71:4C | Ar...     | Mikro Tik | 6.40.5 (st... | RB952Ui...  | y  |
| ether1    | 192.168.2.39  | 00:0C:42:E3:C1:38 | Le...     |           |               |             | y  |
| ether1    | 192.168.2.200 | 00:0C:42:32:D2:D7 | xN        |           |               |             | y  |
| ether1    | 192.168.2.1   | 00:0C:42:F8:71:9A | Sh        |           |               |             | y  |
| ether1    | 192.168.2.48  | 00:00:00:00:00:00 |           |           |               |             | n  |

8 items (1 selected)

- Show Categories
- Detail Mode
- Show Columns >
- Find Ctrl+F
- Find Next Ctrl+G
- Ping
- MAC Ping
- Telnet
- MAC Telnet
- Torch

- ▶ Telnet
- ▶ MAC Telnet

6.

# IMPLEMENTIMI I SIGURISE

# CIA VAULT 7



- ▶ E marte, 7 Mars 2017 - WikiLeaks fillon publikimin e serise se ashtuquajtur VAULT7 te dokumentave te CIA.
- ▶ Permban dobesi te:
  - **iPhone, Android, smart TVs**
  - Routera, switch (CISCO, JUNIPER, MikroTik, Huawei, Asus, Ubiquiti, D-link

## CIA VAULT 7



- ▶ E marte, 7 Mars 2017 - WikiLeaks fillon publikimin e serise se ashtuquajtur VAULT7 te dokumentave te CIA.
- ▶ Chimay Red – modul specifikisht per MikroTik permбан:
  - http server vulnerability
  - Winbox unauthenticated file read

- ▶ MikroTik OFFICIAL standing is that the “Winbox unauthenticated file read” vulnerability, is not described in Chimay Red.

*“We have asked many times to Wikileaks to send us where in the Vault7 documents, this vulnerability is described, BUT they said that they were going to send them, but DIDN'T. We are sure that this vulnerability was not described there.”*



## Chimay Red – http server vulnerability



- ▶ Kjo dobesei konsiston ne dhenien e mundesise per te ekzekutuar komanda ne linux e ruterit
- ▶ MikroTik leshon versionin 6.38.5  
What's new in 6.38.5 (2017-Mar-09 11:32)  
!) www - fixed http server vulnerability;

## Chimay Red – http server vulnerability



- ▶ Ne dokumentat e Vault7 permbahet vetem menyra si te shfrytezohet kjo dobese, dhe jo nje kod aktual per t'u ekzekutuar
- ▶ Keqberesit neper bote e kane shfrytezuar Chimay Red per:
  - Tynyshell, Hive (data warehouse infrastructure Hadoop)
  - Injektimi i DLL

# Winbox unauthenticated file read

- ▶ Mundeson leximin e fileve te sistemit, nepermjet nje sesioni winbox te pa-autentifikuar
- ▶ **Leximi i fileve mundeson leximin e user database**
- ▶ Mundesohet akses i plote ne router
- ▶ Ne cdo pergjigje te ruterit injektohet nje js per cryptocurrency mining, specifikisht Monero



The screenshot shows a web browser displaying a news article from Trend Micro. The article title is "Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign", dated August 03, 2018. The text describes a security campaign where attackers hijack systems to conduct cryptocurrency mining, specifically mentioning a malicious version of Coinhive injected into MikroTik routers. A photograph of yellow Ethernet cables plugged into a network switch is shown. A sidebar on the right lists related posts about critical infrastructure, fraud, and cybersecurity awareness.

Trend Micro Inc. (US) <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats>

Products & Solutions IoT Security Intelligence Support Partners About Contact

## Over 200,000 MikroTik Routers Compromised in Cryptojacking Campaign

August 03, 2018

Security researchers **uncovered** a cryptojacking campaign — where attackers hijack systems to conduct **cryptocurrency mining** — that injects a **malicious version of Coinhive**, a web-based cryptocurrency miner, by exploiting a vulnerability in MikroTik routers. Here's what you need to know about this threat:



### What happened?

The initial phase of the cryptojacking campaign **reportedly** hacked 72,000 MikroTik routers in Brazil. As of this writing, over 200,000 MikroTik routers have already been compromised. While the majority of the routers were in Brazil, researchers also noted that the attacks are now also **spreading** outside the country.

This indicates that users or organizations using a vulnerable MikroTik router are susceptible to cryptojacking. In fact, researchers saw cases where non-MikroTik routers were also affected,

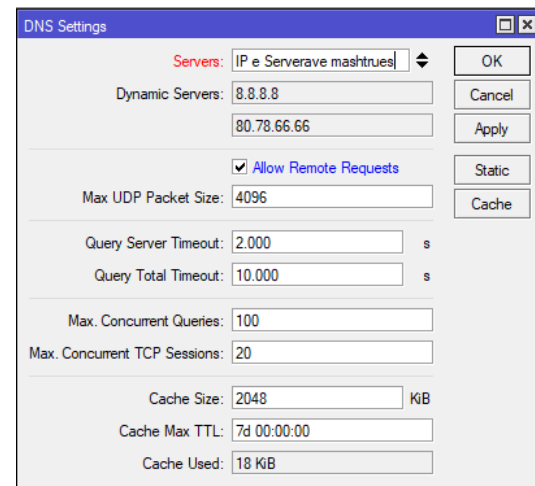
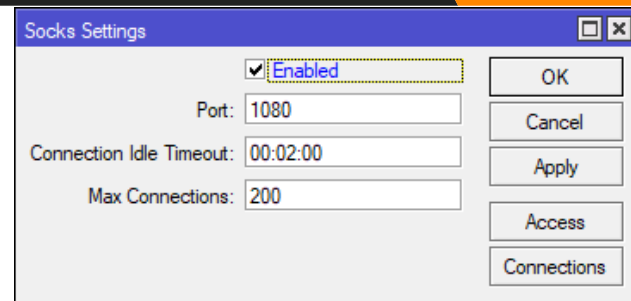
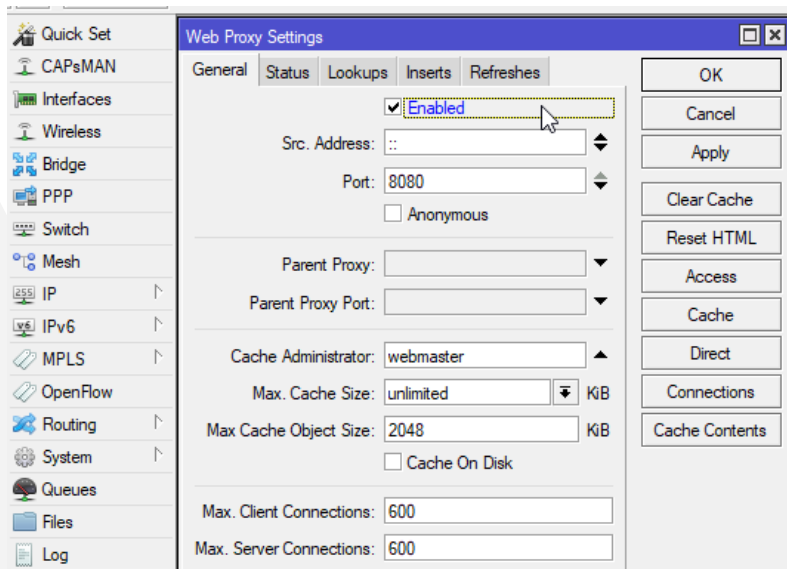
#### Related Posts

- Critical Infrastructures Exposed and at Risk: Energy and Water Industries
- Toil Fraud, International Revenue Share Fraud and More: How Criminals Monetize Hacked Cellphones and IoT Devices for Telecom Fraud
- National Cyber Security Awareness Month: The Enterprise's Safety Online is Everyone's Business
- Report Finds Increased Credential Stuffing Attacks on Financial Sector
- New Multi-Platform Xbash Packs: Obfuscation, Ransomware, Coommer, Worm and Botnet

# Winbox unauthenticated file read

## Shfrytezohet per:

- ▶ Cryptocurrency mining
- ▶ Socks proxy
- ▶ DNS Server
- ▶ etc..



# Vulnerabilities

## Simptomat:

- Usera te tjere te krijuar
- Socks proxy aktive
- Web proxy aktive
- DNS Server
- Scripte te panjohur
- Pamundesi logimi ne ruter

Script List

| Name      | Owner | Last Time Started    | Run Count |
|-----------|-------|----------------------|-----------|
| k4m45utr4 | admin | Oct/30/2018 20:15:45 | 1         |

1 item

2:98:72 (MUM\_Albania) - WinBox v6.43.4 on wsAP ac lite (mipsbe)

hboard

Session: CC:2D:E0:D2:98:72

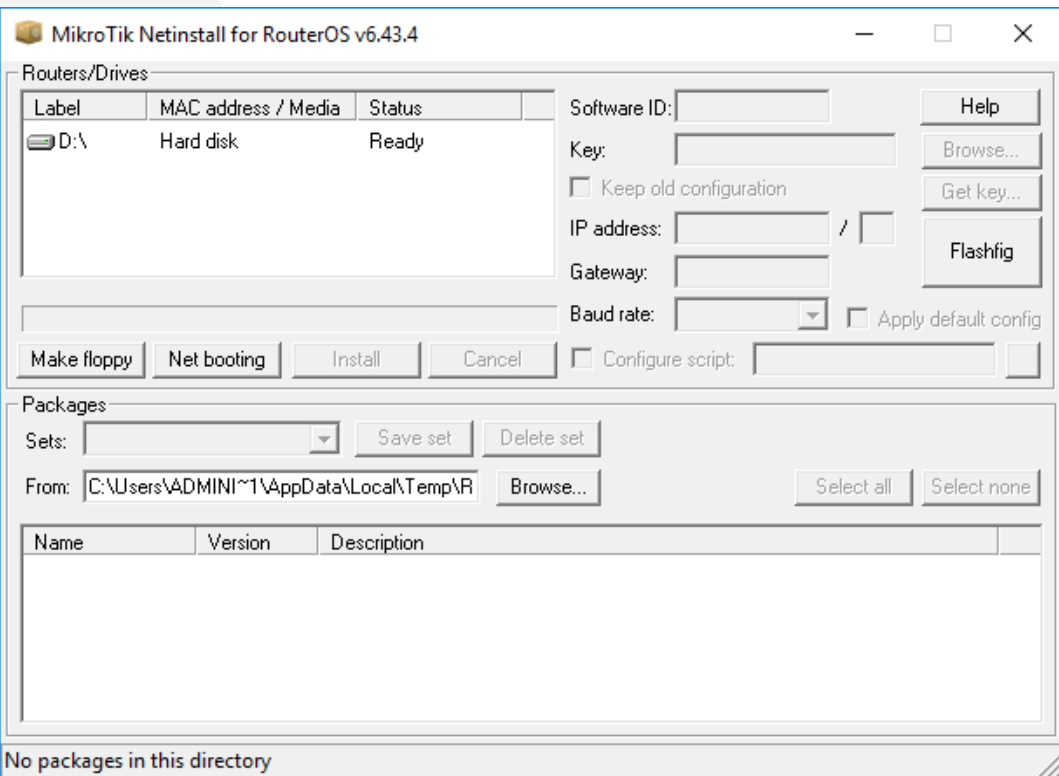
User List

| Name                | Group | Allowed Address | Last Logged In |
|---------------------|-------|-----------------|----------------|
| system default user |       |                 |                |
| admin               | read  |                 | Oct/30/2018    |
| router              | full  |                 |                |

File List

| File Name                | Type      | Size     | Creation    |
|--------------------------|-----------|----------|-------------|
| auto-before-reset.backup | backup    | 20.4 KiB | Oct/30/2018 |
| dnstest                  | file      | 66.2 KiB | Oct/30/2018 |
| flash                    | disk      |          | Jan/01/2019 |
| mikrotik.php             | .php file | 0 B      | Oct/30/2018 |
| save.sh                  | .sh file  | 674 B    | Oct/30/2018 |

5 items 12.4 MiB of 16.0 MiB used 22% free

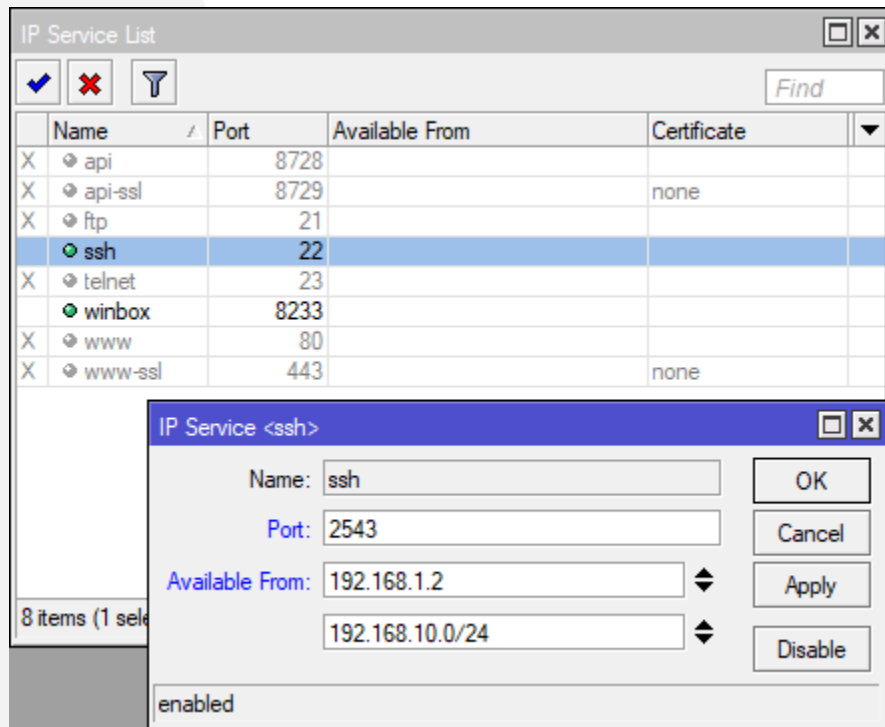


What's new in **6.42.1 (2018-Apr-23 10:46)**:

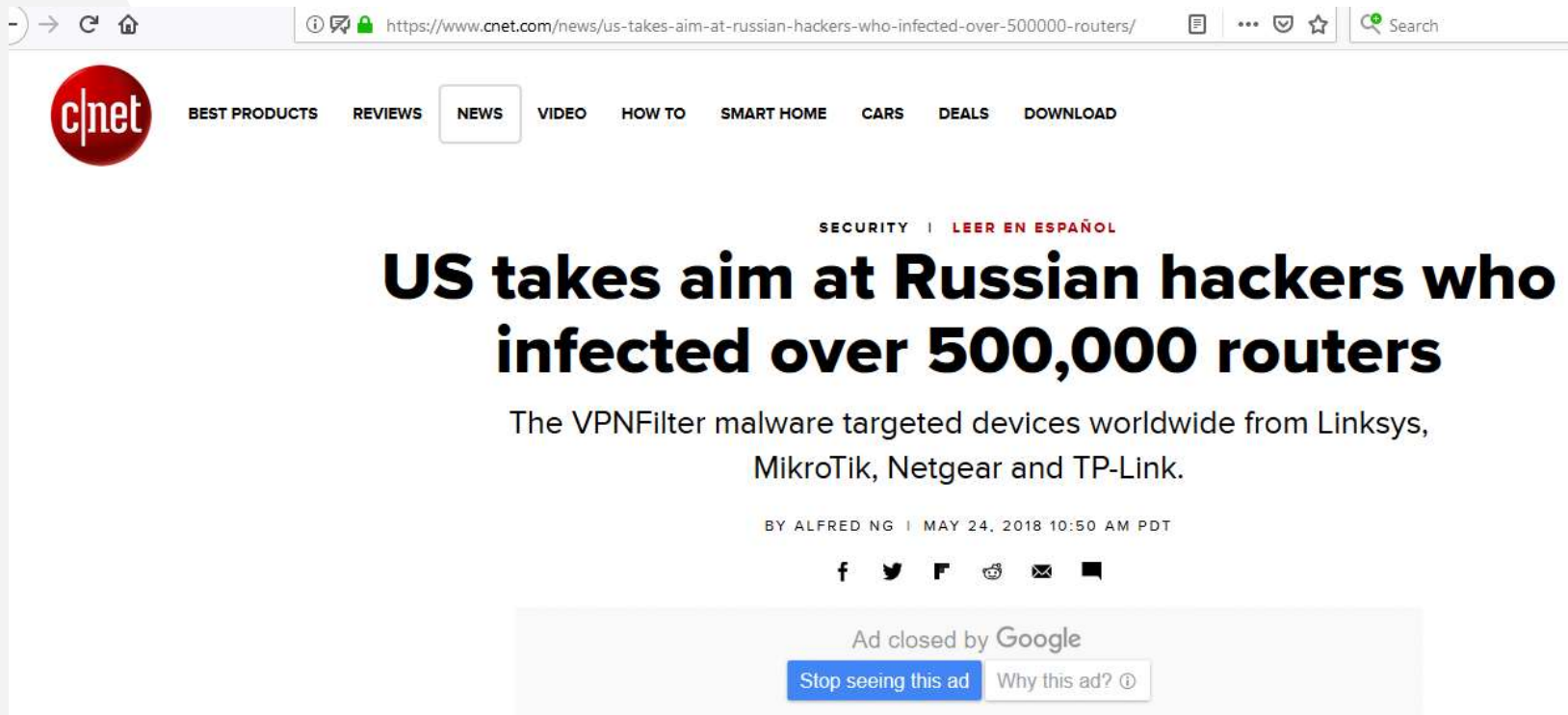
!) winbox - fixed vulnerability that allowed to gain access to an unsecured router;

► **Netinstall**

## Mbrojtja per te ardhmen



- ▶ Ndrysho userin admin
- ▶ Ndrysho passin ne varesi te klientit/ruterit
- ▶ Mos ler te hapur sherbime qe nuk i shfrytezon
- ▶ Ndrysho portat default
- ▶ Lejo aksesin ne winbox vetem nga subnet te njohur
- ▶ Mer pjese ne ENS (Easy Network Solutions) mailing list.



The screenshot shows a web browser displaying a CNET news article. The browser's address bar shows the URL: <https://www.cnet.com/news/us-takes-aim-at-russian-hackers-who-infected-over-500000-routers/>. The CNET logo is in the top left, and a navigation menu includes links for BEST PRODUCTS, REVIEWS, NEWS (which is highlighted), VIDEO, HOW TO, SMART HOME, CARS, DEALS, and DOWNLOAD. The article title is "US takes aim at Russian hackers who infected over 500,000 routers", with a sub-header "SECURITY | LEER EN ESPAÑOL". The lead text states: "The VPNFilter malware targeted devices worldwide from Linksys, MikroTik, Netgear and TP-Link." The byline reads "BY ALFRED NG | MAY 24, 2018 10:50 AM PDT". Below the text are social media sharing icons for Facebook, Twitter, Facebook, Reddit, Email, and Print. At the bottom, there is a Google ad notice: "Ad closed by Google" with buttons for "Stop seeing this ad" and "Why this ad? ⓘ".

https://www.cnet.com/news/us-takes-aim-at-russian-hackers-who-infected-over-500000-routers/

**c|net** BEST PRODUCTS REVIEWS **NEWS** VIDEO HOW TO SMART HOME CARS DEALS DOWNLOAD

SECURITY | LEER EN ESPAÑOL

# US takes aim at Russian hackers who infected over 500,000 routers

The VPNFilter malware targeted devices worldwide from Linksys, MikroTik, Netgear and TP-Link.

BY ALFRED NG | MAY 24, 2018 10:50 AM PDT

f t f r e m

Ad closed by Google

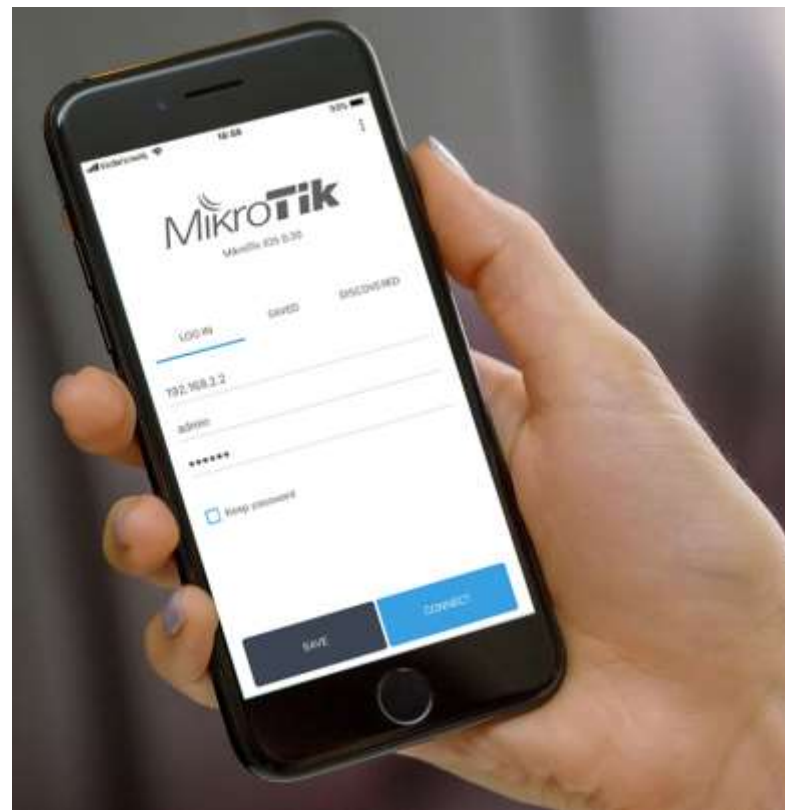
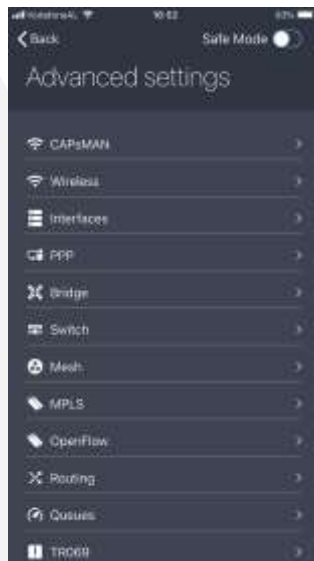
Stop seeing this ad Why this ad? ⓘ



# WINBOX në IPHONE



Me ne fund per perdoruesit e Iphone, version Beta i MikroTik iOS 0.20



# FALEMINDERIT PER VEMENDJEN!

**Pyetje?**

[erioni@gmail.com](mailto:erioni@gmail.com)

