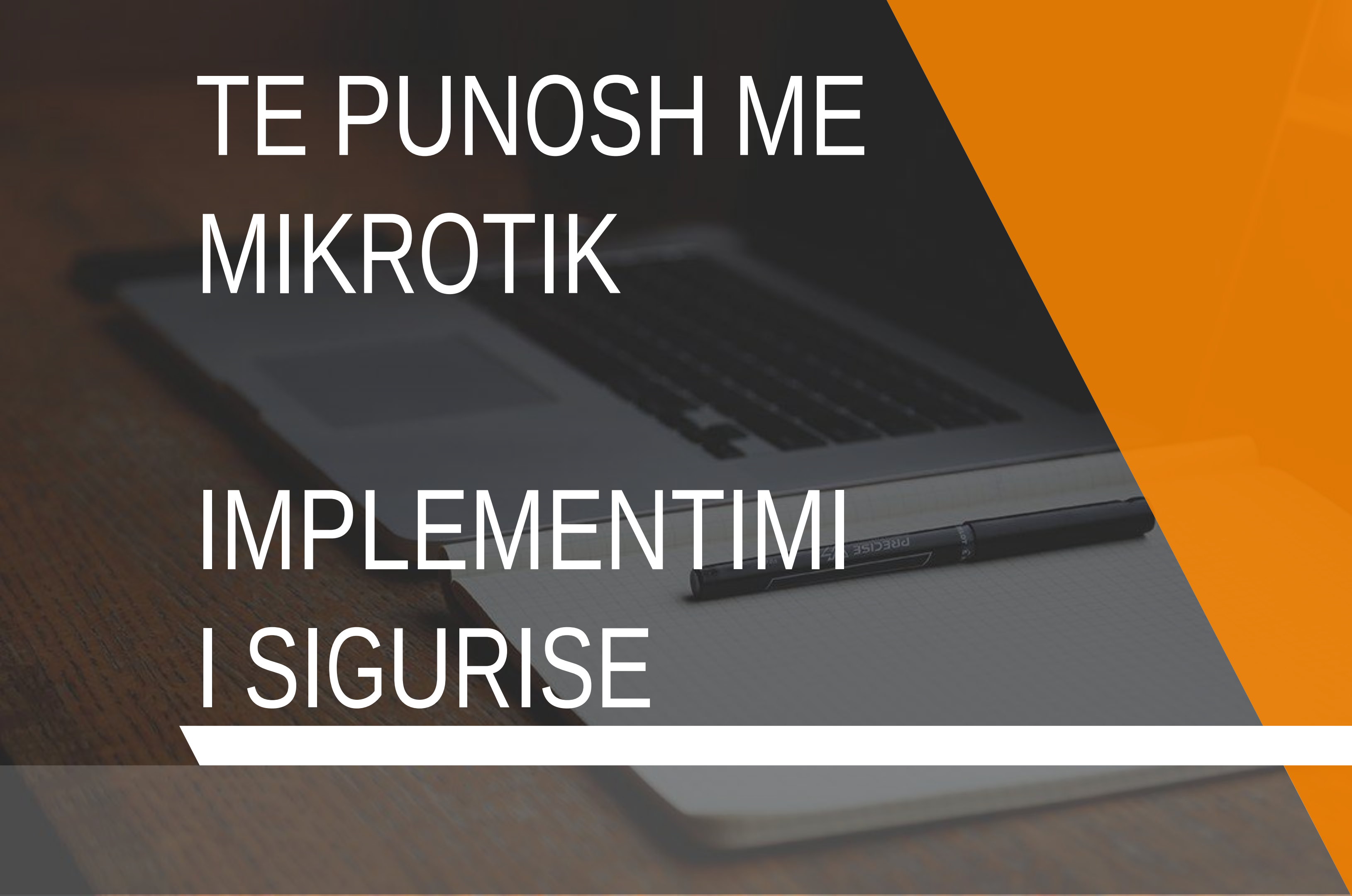


MUM
TIRANA
01. Nov. 2018

# TE PUNOSH ME MIKROTIK

# IMPLEMENTIMI I SIGURISE

ens
EASY NETWORK SOLUTIONS

# 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 rutera

Implementimi I sigurise eshte nje nga proceset kyce te ndertimit te nje rrjeti kompjuterik. Meqenese nje ruter eshte porta hyrese per nje rrjet, atehere 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

# BIO

- 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

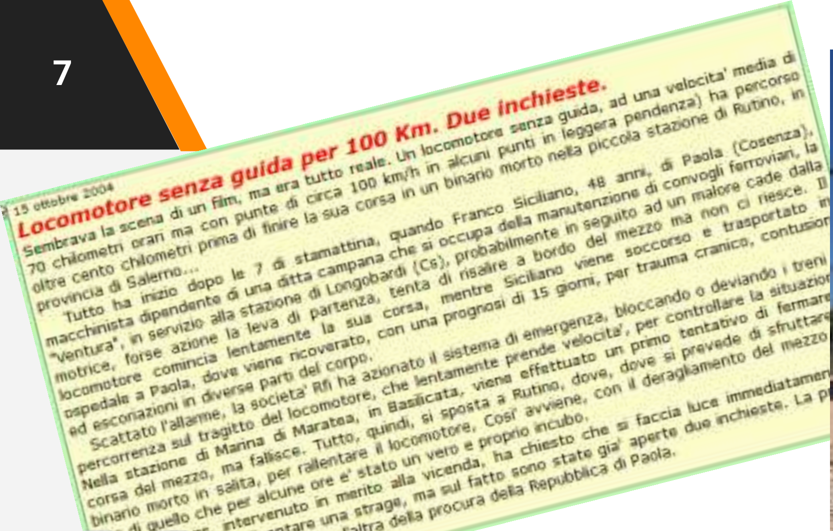
# ENS – EASY NETWORK SOLUTIONS

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

# WIFI

PROJEKTE

# MOBILE VPN



15 ottobre 2004

**Locomotore senza guida per 100 Km. Due inchieste.**

Sembrava la scena di un film, ma era tutto reale. Un locomotore senza guida, ad una velocita' media di 70 chilometri orari ma con punte di circa 100 km/h in alcuni punti in leggera pendenza) ha percorso oltre cento chilometri prima di finire la sua corsa in un binario morto nella piccola stazione di Rutino, in provincia di Salerno...

Tutto ha inizio dopo le 7 di stamattina, quando Franco Siciliano, 48 anni, di Paola (Cosenza), macchinista dipendente di una ditta campana che si occupa della manutenzione di convogli ferroviari, la "Ventura", in servizio alla stazione di Longobardi (Cs), probabilmente in seguito ad un malore cade dalla motrice, forse azione la leva di partenza, tenta di risalire a bordo del mezzo ma non ci riesce. Il locomotore comincia lentamente la sua corsa, mentre Siciliano viene soccorso e trasportato in ospedale a Paola, dove viene ricoverato, con una prognosi di 15 giorni, per trauma cranico, contusion ed escoriazioni in diverse parti del corpo.

Scattato l'allarme, la societa' Rfi ha azionato il sistema di emergenza, bloccando o deviando i treni in percorrenza sul tragitto del locomotore, che lentamente prende velocita', per controllare la situazio Nella stazione di Marina di Maratea, in Basilicata, viene effettuato un primo tentativo di fermar corsa del mezzo, ma fallisce. Tutto, quindi, si sposta a Rutino, dove si prevede di sfruttar binario morto in salita, per rallentare il locomotore. Cosi' avviene, con il deragliamento del mezzo e di quello che per alcune ore e' stato un vero e proprio incubo.

Il C ns, intervenuto in merito alla vicenda, ha chiesto che si faccia luce immediatamen ella oteva diventare una strage, ma sul fatto sono state gia' aperte due inchieste. La p cata della societa' Rfi e l'altra della procura della Repubblica di Paola.

Fonte line)

OmniTIK5

3G TIM Usb Key

SIEMENS PLC

# 1.

# MikroTik - RouterOS

Pse MikroTik?

“

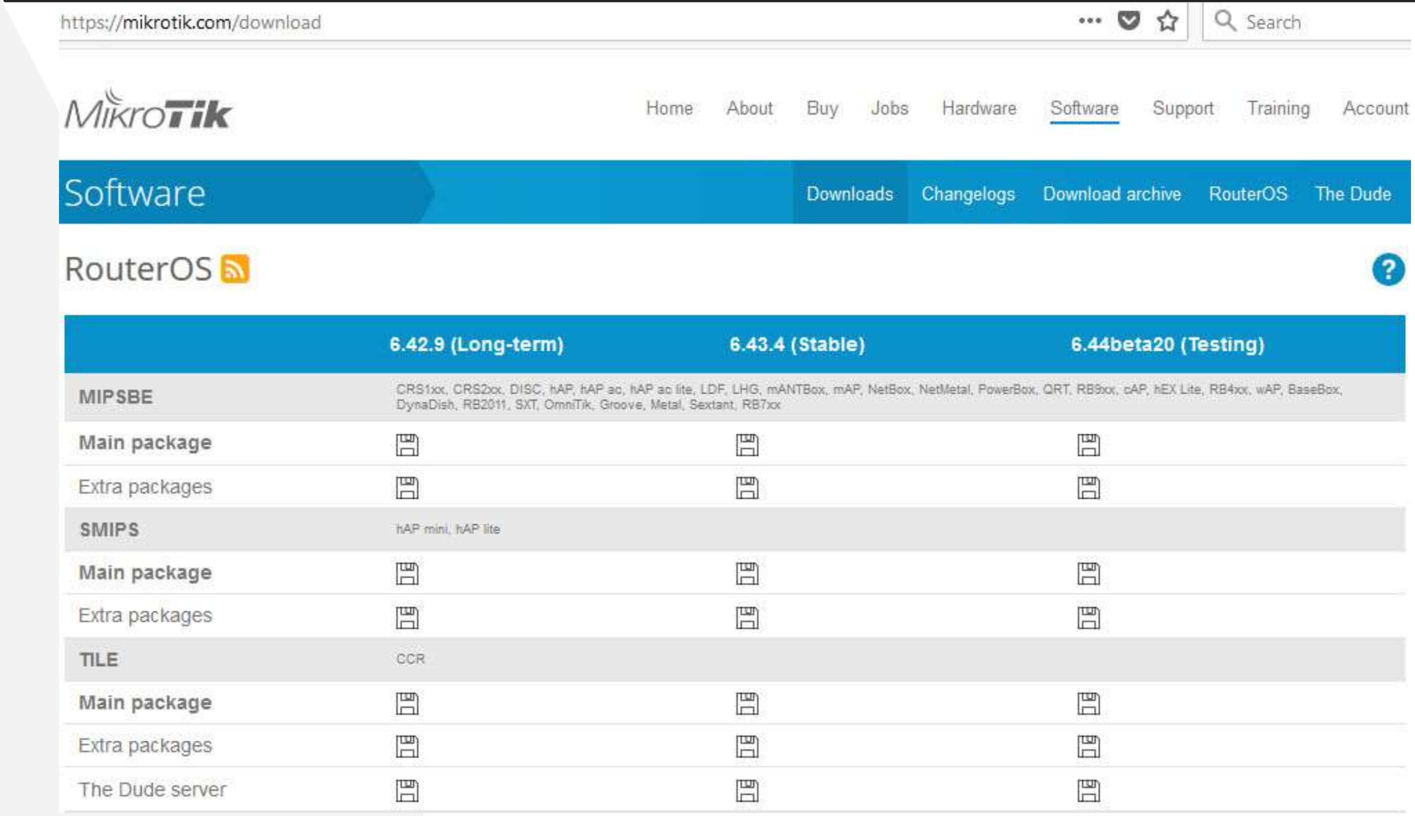
*MikroTik RouterOS eshte nje sistem operativ i dizenjuar per rutera, i bazuar ne Linux, me nje game te gjere funksionesh, qe i japin nje inxhinieri rrjetesh, mundesi per konfigurime nga me te ndryshmet.*

”

# 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



## RouterOS

| | 6.42.9 (Long-term) | 6.43.4 (Stable) | 6.44beta20 (Testing) |
|---|---|---|---|
| **MIPSBE** | 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 | 💾 | 💾 | 💾 |
| **SMIPS** | hAP mini, hAP lite | | |
| **Main package** | 💾 | 💾 | 💾 |
| Extra packages | 💾 | 💾 | 💾 |
| **TILE** | CCR | | |
| **Main package** | 💾 | 💾 | 💾 |
| Extra packages | 💾 | 💾 | 💾 |
| The Dude server | 💾 | 💾 | 💾 |

# Arkitekturat

- 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 ac², LDF ac, LHG ac, SXTsq (ac series), Wireless Wire, CRS3xx, RB3011, RB1100AHx4, RB450Gx4
- X86

# Arkitekturat

- X86 Pentium III Router

# Cloud Hosted Router

## CHR

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

# 2.
# Hapat e pare

# Kutia e cudirave

**hAP Mini – RB931-2nd**

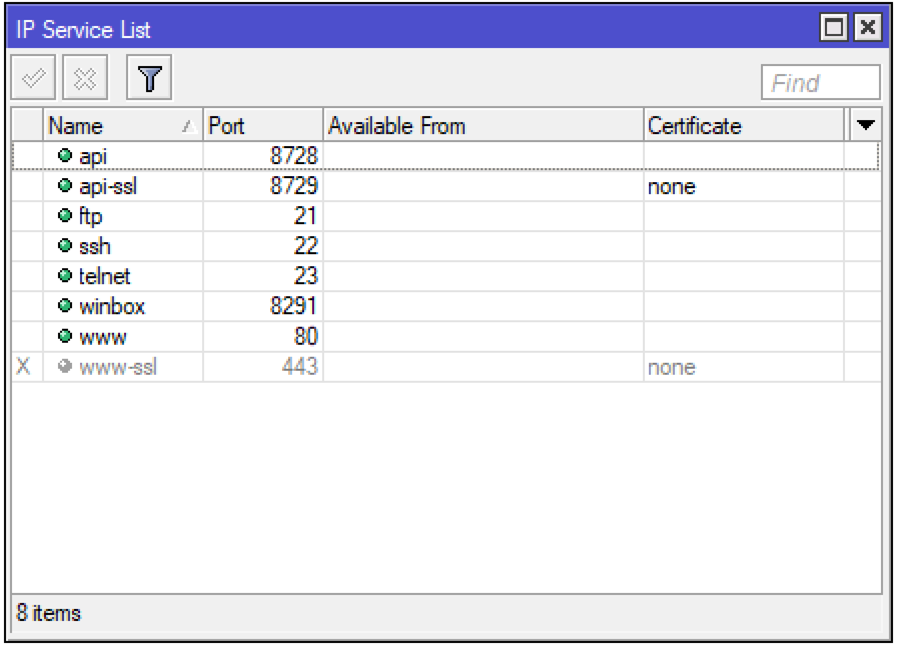
SMIPS, 650 MHz, 3 Ethernet, 32 MB Ram, 16 MB Flash, Dual Chain 802.11b/g/n.

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

# RouterBoard

## Menyrat e lidhjes

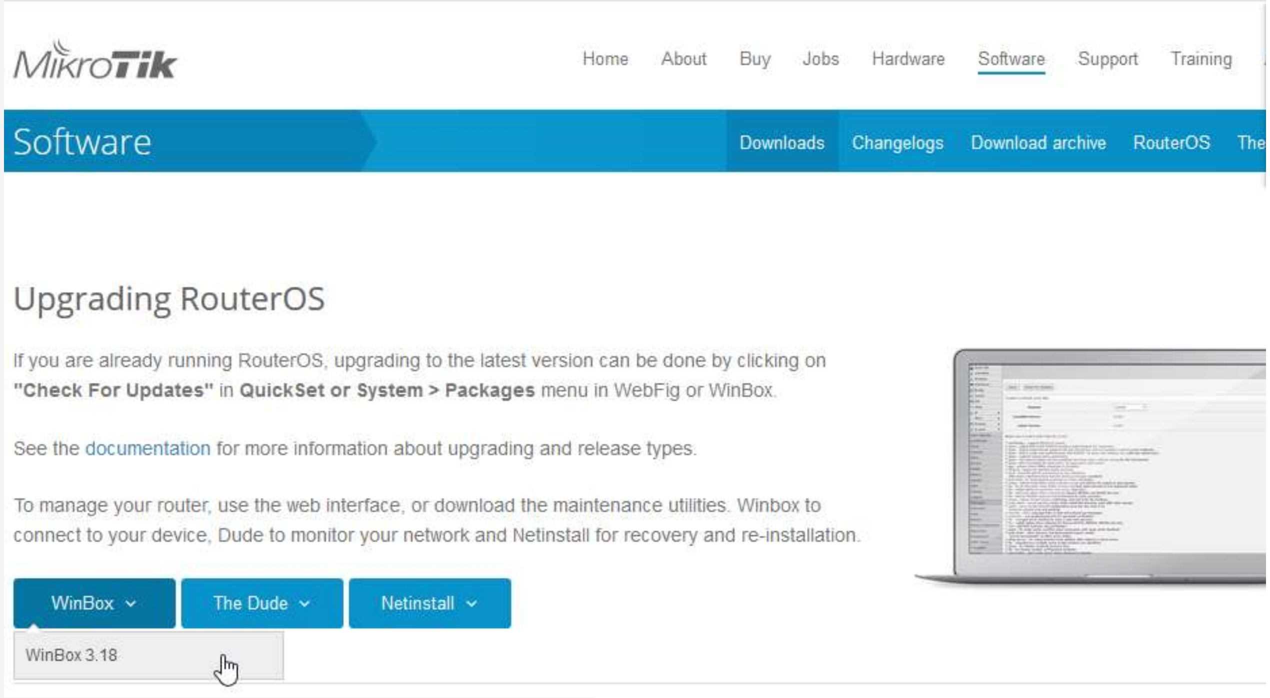
- Winbox
- SSH
- Telnet
- Serial
- API
- FTP
- WWW



|  | 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

# Winbox



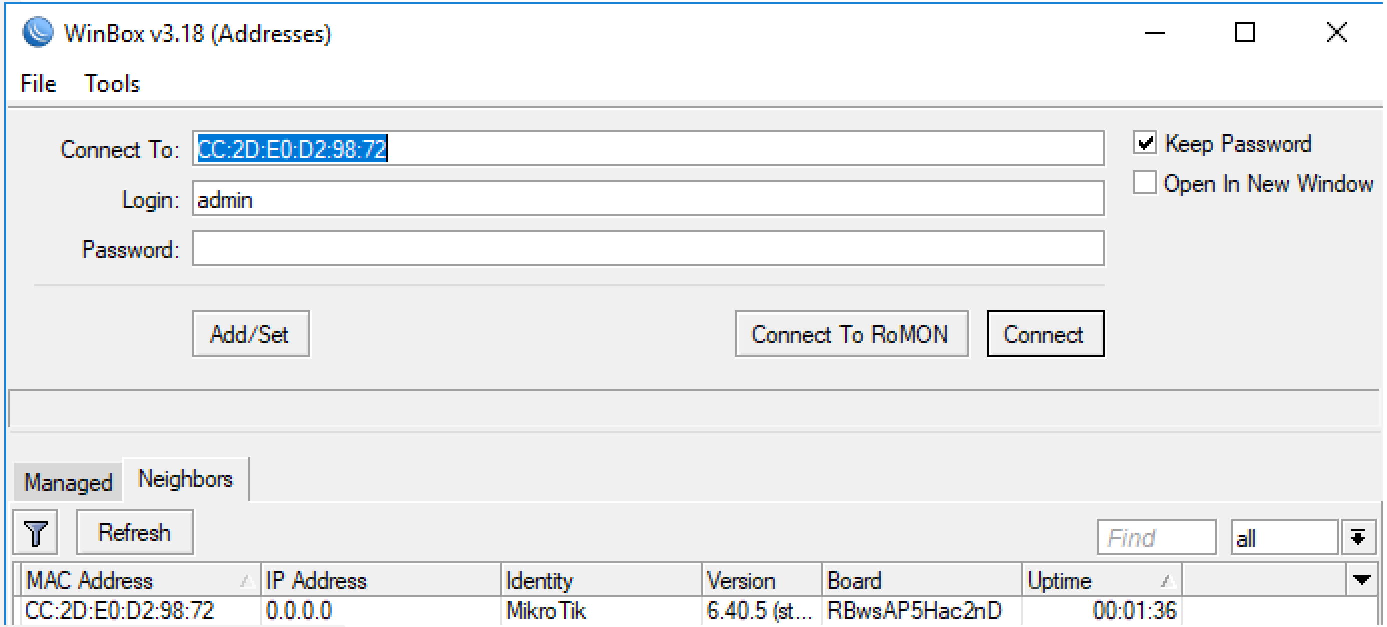
## Upgrading RouterOS

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



Connect To: CC:2D:E0:D2:98:72

Login: admin

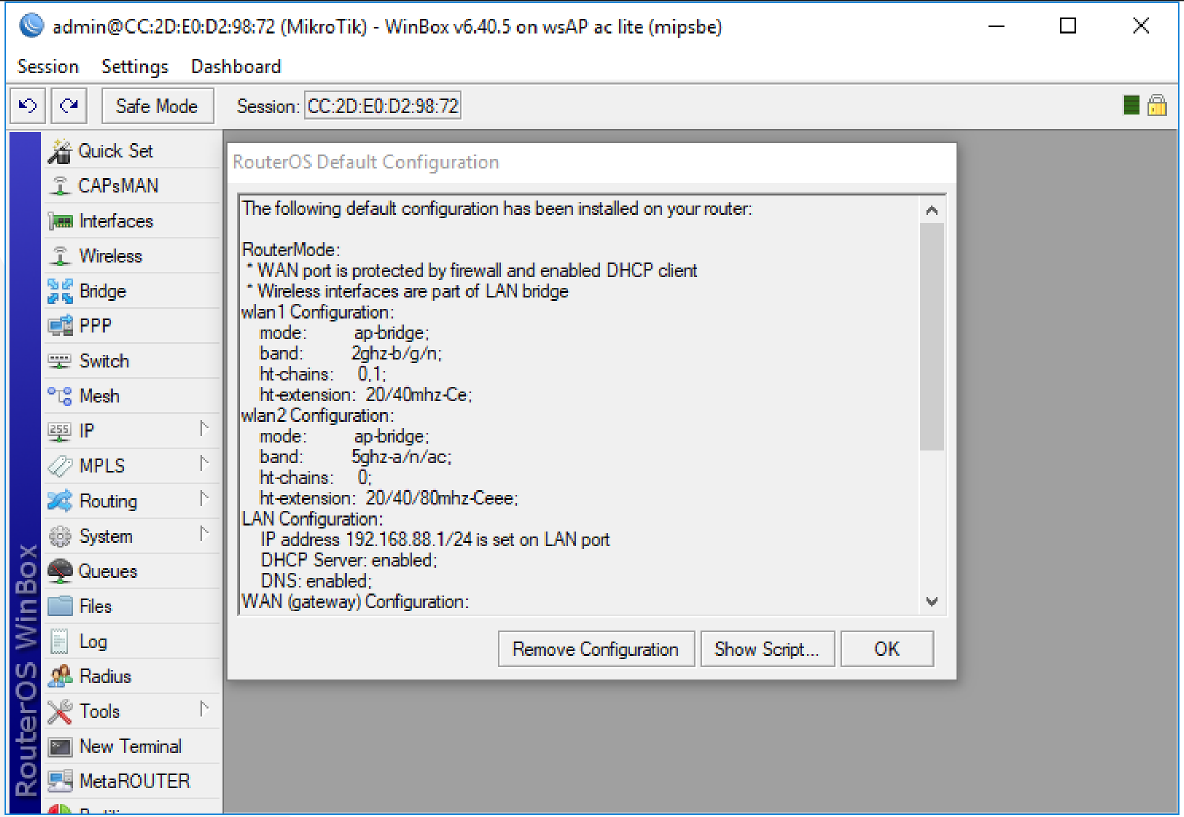
Password:

☑ Keep Password

□ Open In New Window

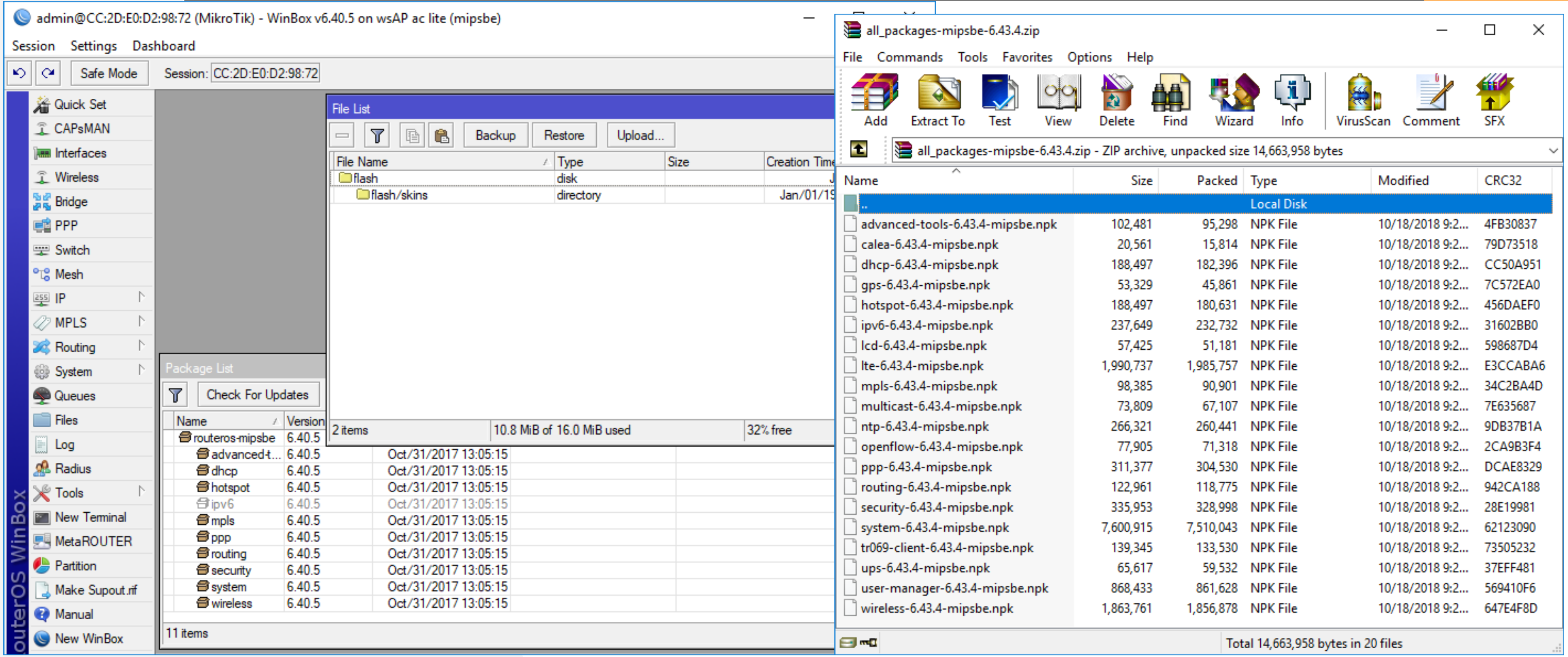
| MAC Address | IP Address | Identity | Version | Board | Uptime |
|---|---|---|---|---|---|
| CC:2D:E0:D2:98:72 | 0.0.0.0 | MikroTik | 6.40.5 (st... | RBwsAP5Hac2nD | 00:01:36 |

# Winbox



```
The following default configuration has been installed on your router:

RouterMode:
 * WAN port is protected by firewall and enabled DHCP client
 * Wireless interfaces are part of LAN bridge
wlan1 Configuration:
    mode:          ap-bridge;
    band:          2ghz-b/g/n;
    ht-chains:     0,1;
    ht-extension:  20/40mhz-Ce;
wlan2 Configuration:
    mode:          ap-bridge;
    band:          5ghz-a/n/ac;
    ht-chains:     0;
    ht-extension:  20/40/80mhz-Ceee;
LAN Configuration:
    IP address 192.168.88.1/24 is set on LAN port
    DHCP Server: enabled;
    DNS: enabled;
WAN (gateway) Configuration:
```

# Upgrade



File List

| File Name | Type | Size | Creation Time |
|---|---|---|---|
| flash | disk | | J |
| flash/skins | directory | | Jan/01/19 |

2 items | 10.8 MiB of 16.0 MiB used | 32% free

Package List

| Name | Version | |
|---|---|---|
| routeros-mipsbe | 6.40.5 | |
| advanced-t... | 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 |

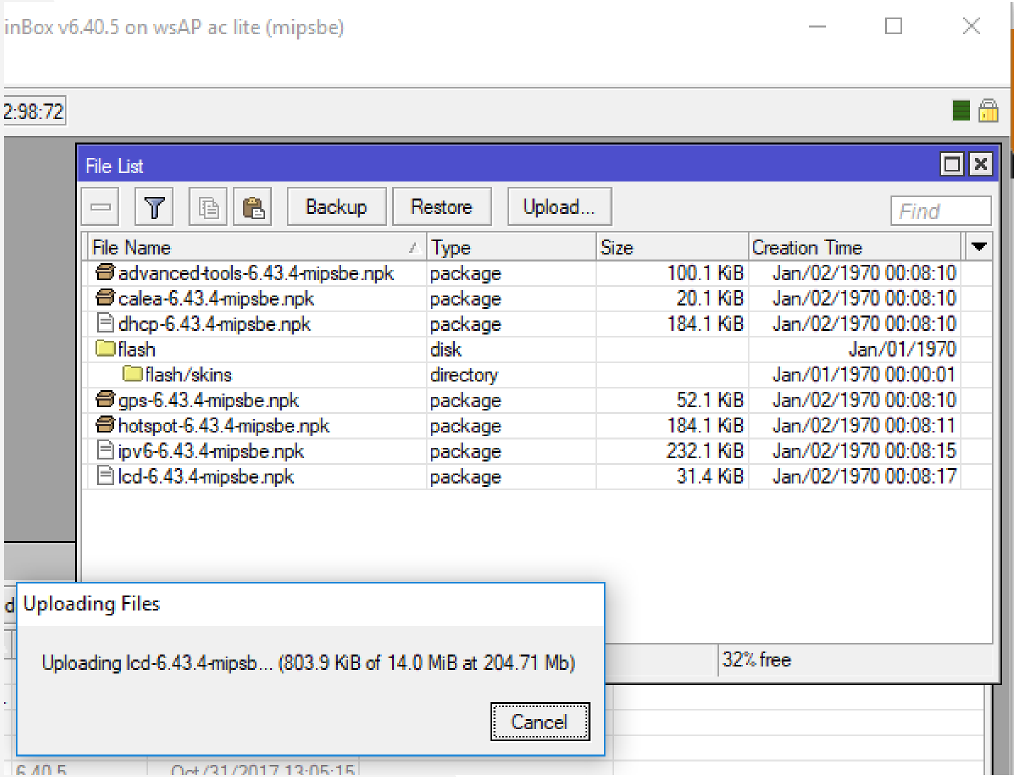
11 items

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



| File Name | Type | Size | Creation Time |
|---|---|---|---|
| advanced-tools-6.43.4-mipsbe.npk | package | 100.1 KiB | Jan/02/1970 00:08:10 |
| calea-6.43.4-mipsbe.npk | package | 20.1 KiB | Jan/02/1970 00:08:10 |
| dhcp-6.43.4-mipsbe.npk | package | 184.1 KiB | Jan/02/1970 00:08:10 |
| flash | disk | | Jan/01/1970 |
| flash/skins | directory | | Jan/01/1970 00:00:01 |
| gps-6.43.4-mipsbe.npk | package | 52.1 KiB | Jan/02/1970 00:08:10 |
| hotspot-6.43.4-mipsbe.npk | package | 184.1 KiB | Jan/02/1970 00:08:11 |
| ipv6-6.43.4-mipsbe.npk | package | 232.1 KiB | Jan/02/1970 00:08:15 |
| lcd-6.43.4-mipsbe.npk | package | 31.4 KiB | Jan/02/1970 00:08:17 |

32% free

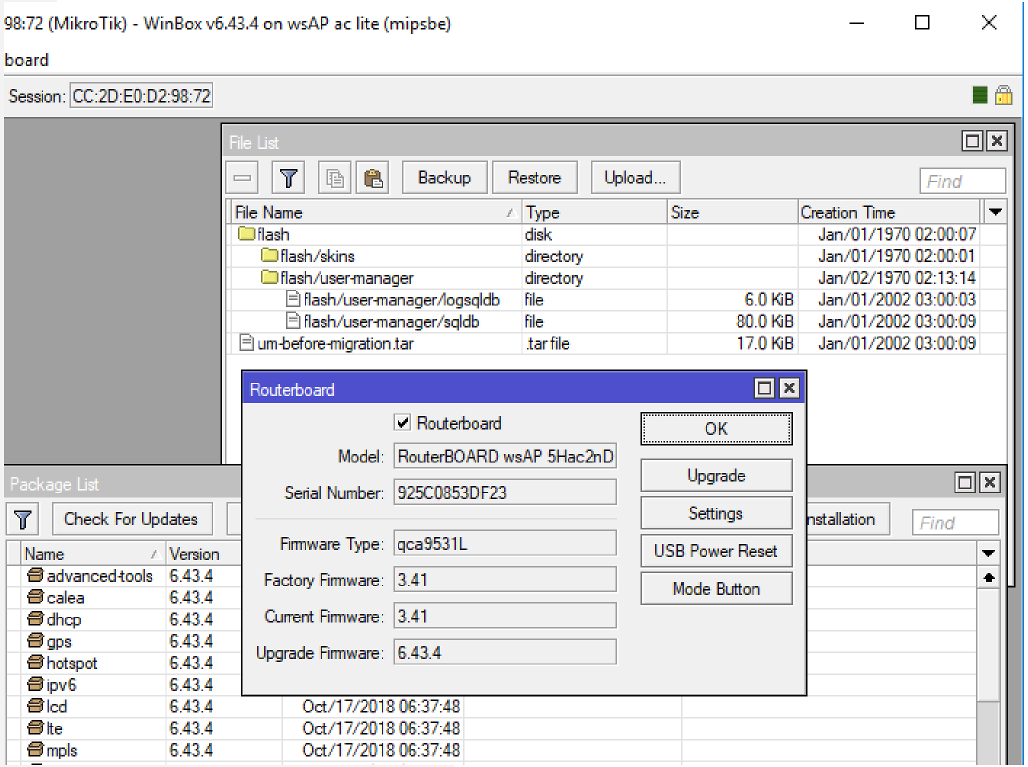
Uploading Files

Uploading lcd-6.43.4-mipsb... (803.9 KiB of 14.0 MiB at 204.71 Mb)

## 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/sqldb | 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

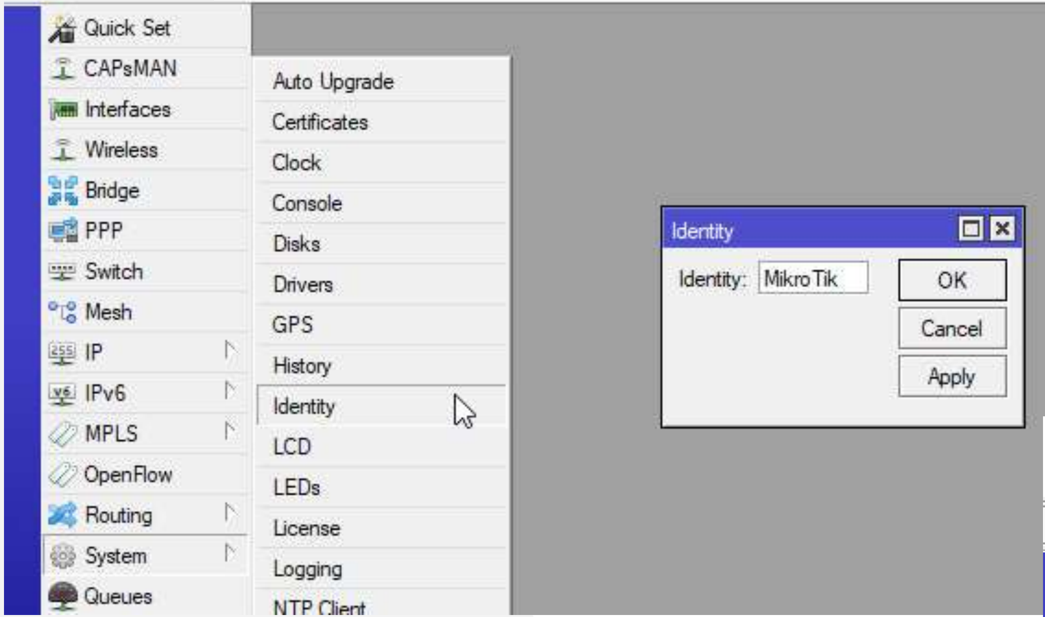
Package List

| 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 | Oct/17/2018 06:37:48 |
| lte | 6.43.4 | Oct/17/2018 06:37:48 |
| mpls | 6.43.4 | Oct/17/2018 06:37:48 |

## Upgrade firmware

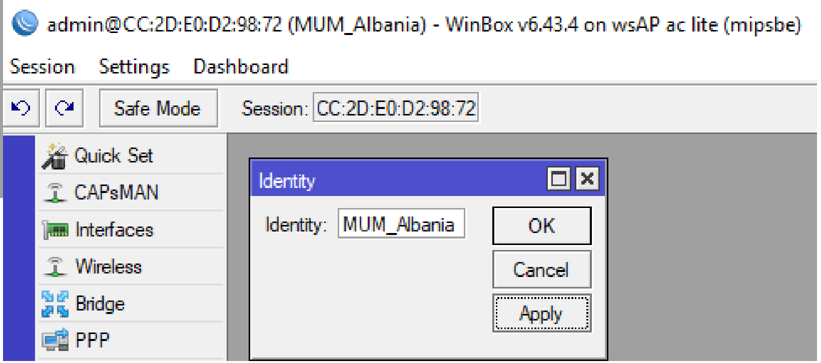
- Shkojme tek System – Routerboard
- Japim “Upgrade”

# Identiteti



Identity

Identity: MikroTik



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

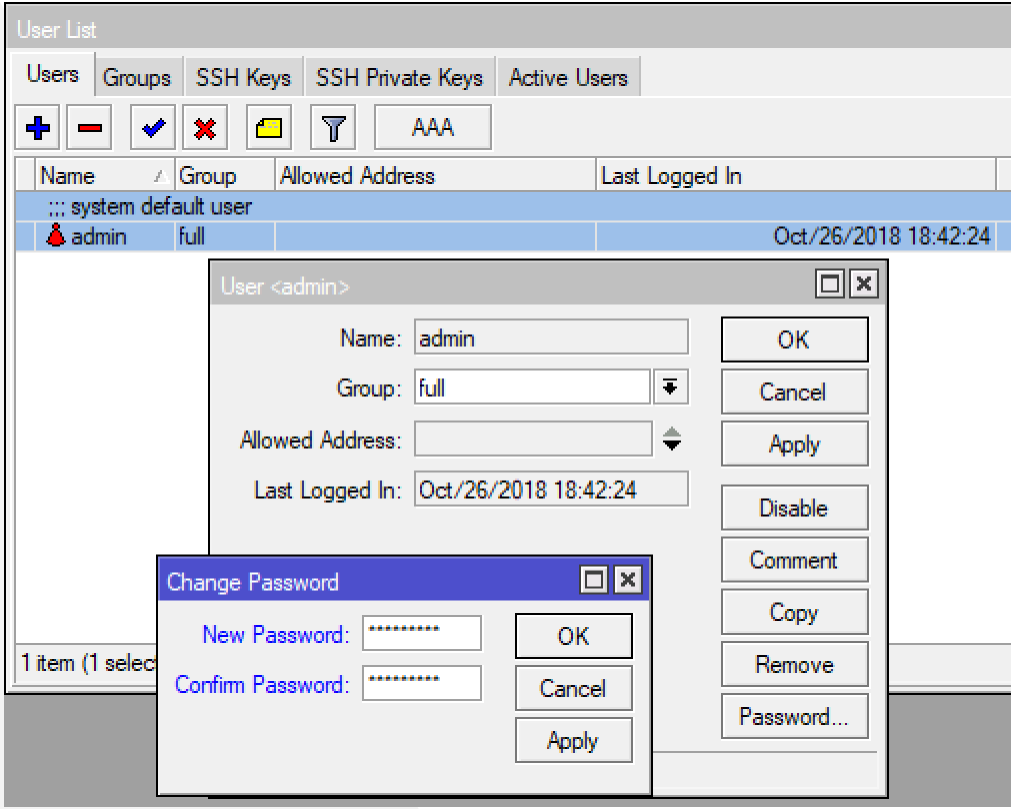
Session: CC:2D:E0:D2:98:72

Identity

Identity: MUM_Albania

- Shkojme tek System - Identity
- Vendosim identitetin

# Perdoruesit e sistemit - Users



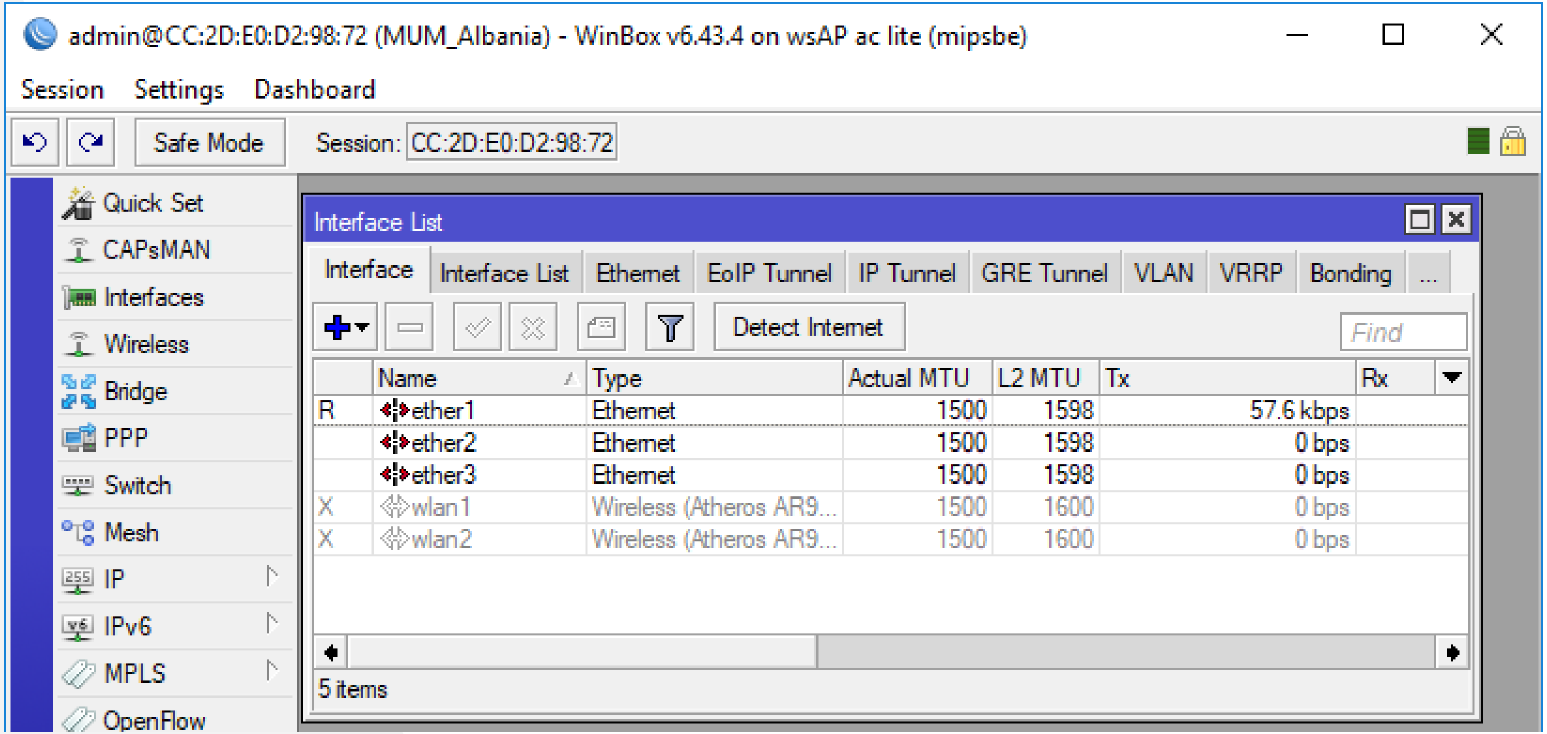
| Name | Group | Allowed Address | Last Logged In |
|---|---|---|---|
| ;;; system default user | | | |
| admin | full | | Oct/26/2018 18:42:24 |

Name: admin
Group: full
Allowed Address:
Last Logged In: Oct/26/2018 18:42:24

New Password: **********
Confirm Password: **********

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

# Interfaces



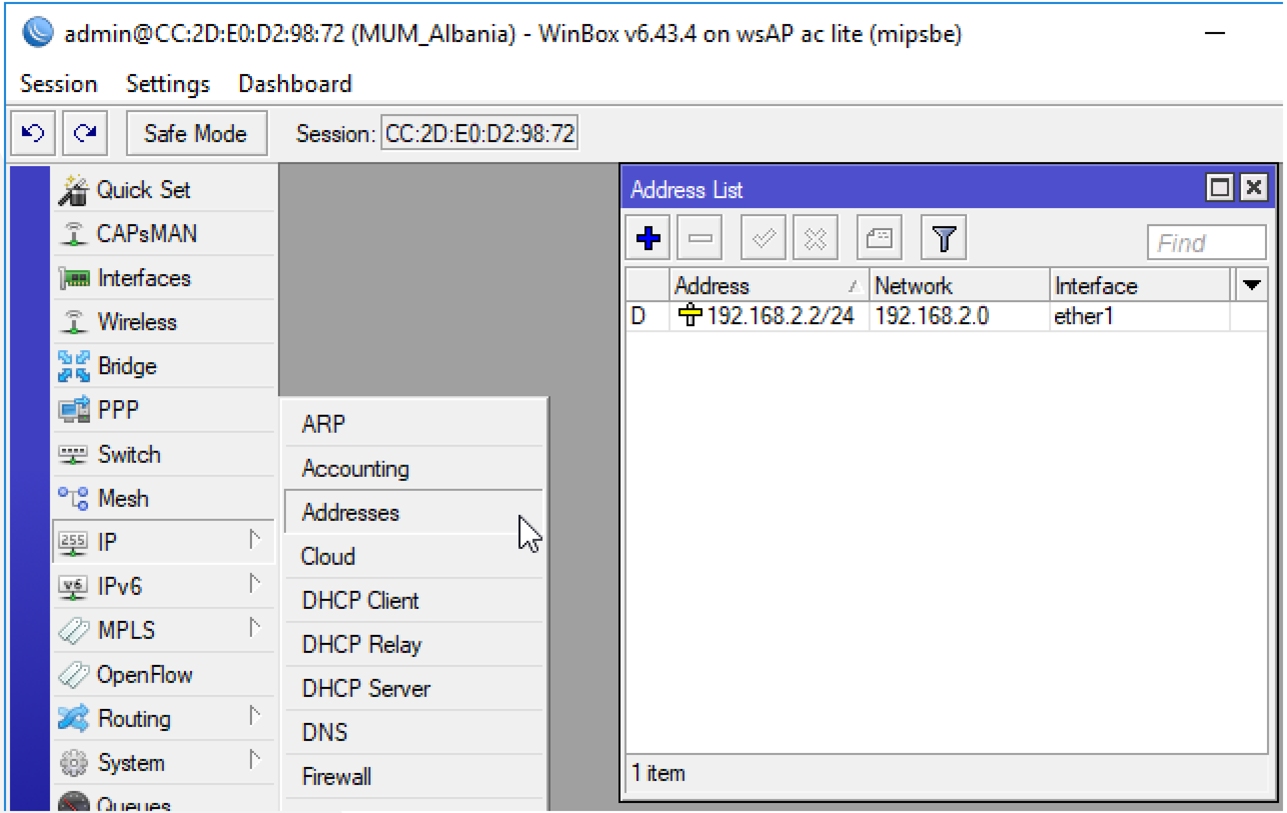
admin@CC:2D:E0:D2:98:72 (MUM_Albania) - WinBox v6.43.4 on wsAP ac lite (mipsbe)

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

|  | 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

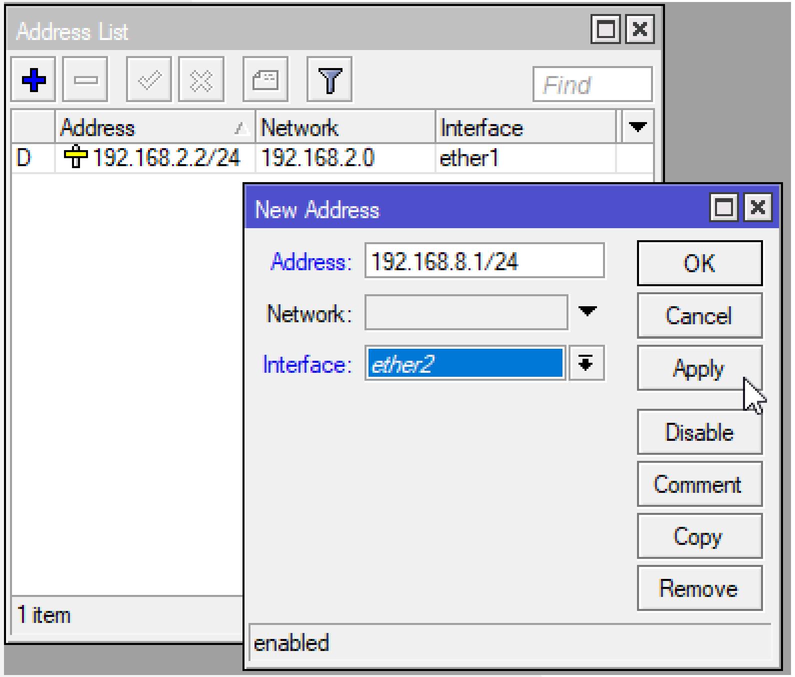
# Adresat IP



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

1 item

# Adresat IP - Statike



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

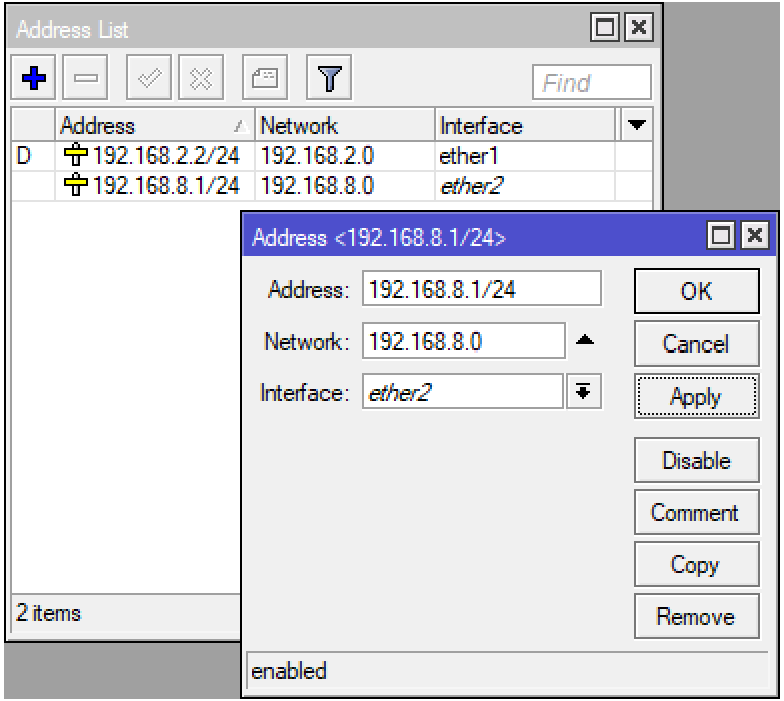
1 item

Address: 192.168.8.1/24

Network:

Interface: ether2

enabled



|  | Address | Network | Interface |
|---|---|---|---|
| D | 192.168.2.2/24 | 192.168.2.0 | ether1 |
|  | 192.168.8.1/24 | 192.168.8.0 | ether2 |

2 items

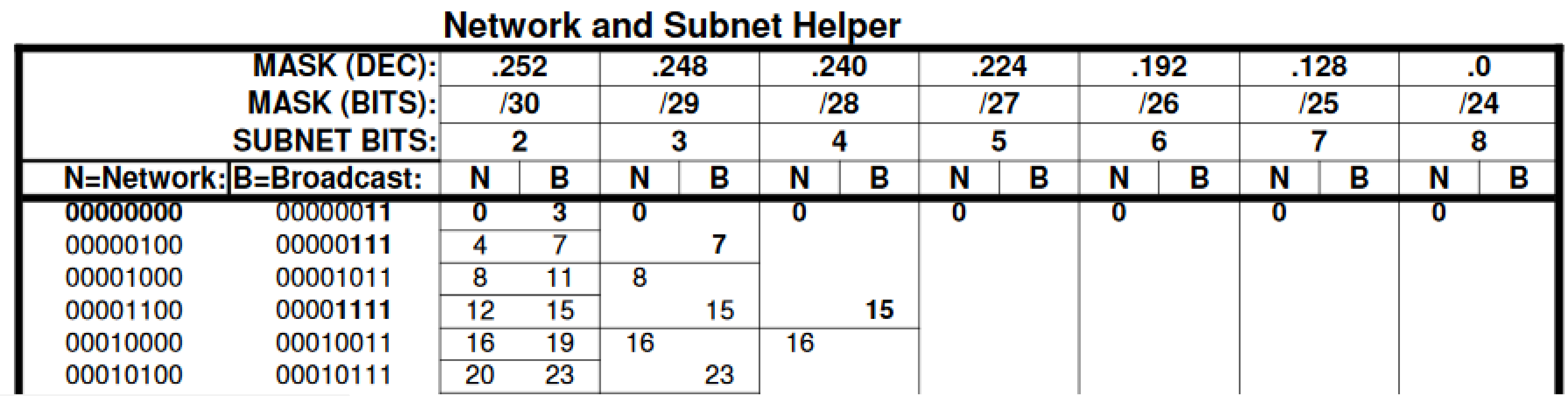
Address: 192.168.8.1/24

Network: 192.168.8.0

Interface: ether2

enabled

# Adresat IP - Statike



Network and Subnet Helper

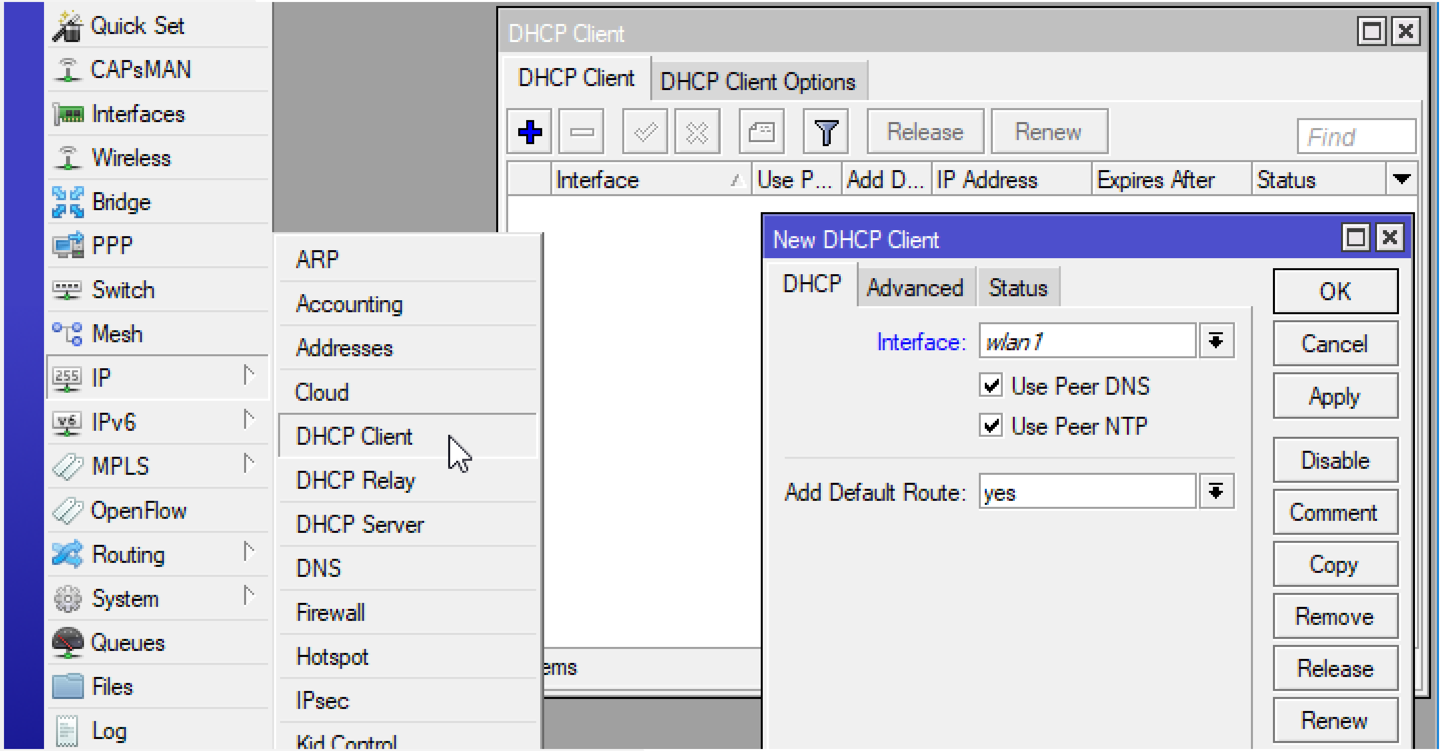
| MASK (DEC): | | .252 | | .248 | | .240 | | .224 | | .192 | | .128 | | .0 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| MASK (BITS): | | /30 | | /29 | | /28 | | /27 | | /26 | | /25 | | /24 | |
| SUBNET BITS: | | 2 | | 3 | | 4 | | 5 | | 6 | | 7 | | 8 | |
| N=Network: | B=Broadcast: | 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……

**https://mikrotik.com/img/netaddresses2.pdf**

# Adresat IP - Dinamike



Interface: wlan1

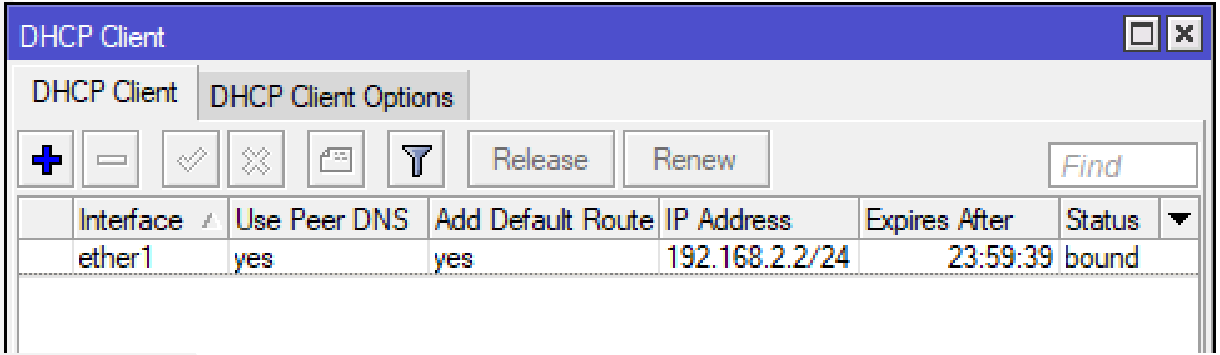
☑ Use Peer DNS

☑ Use Peer NTP

Add Default Route: yes

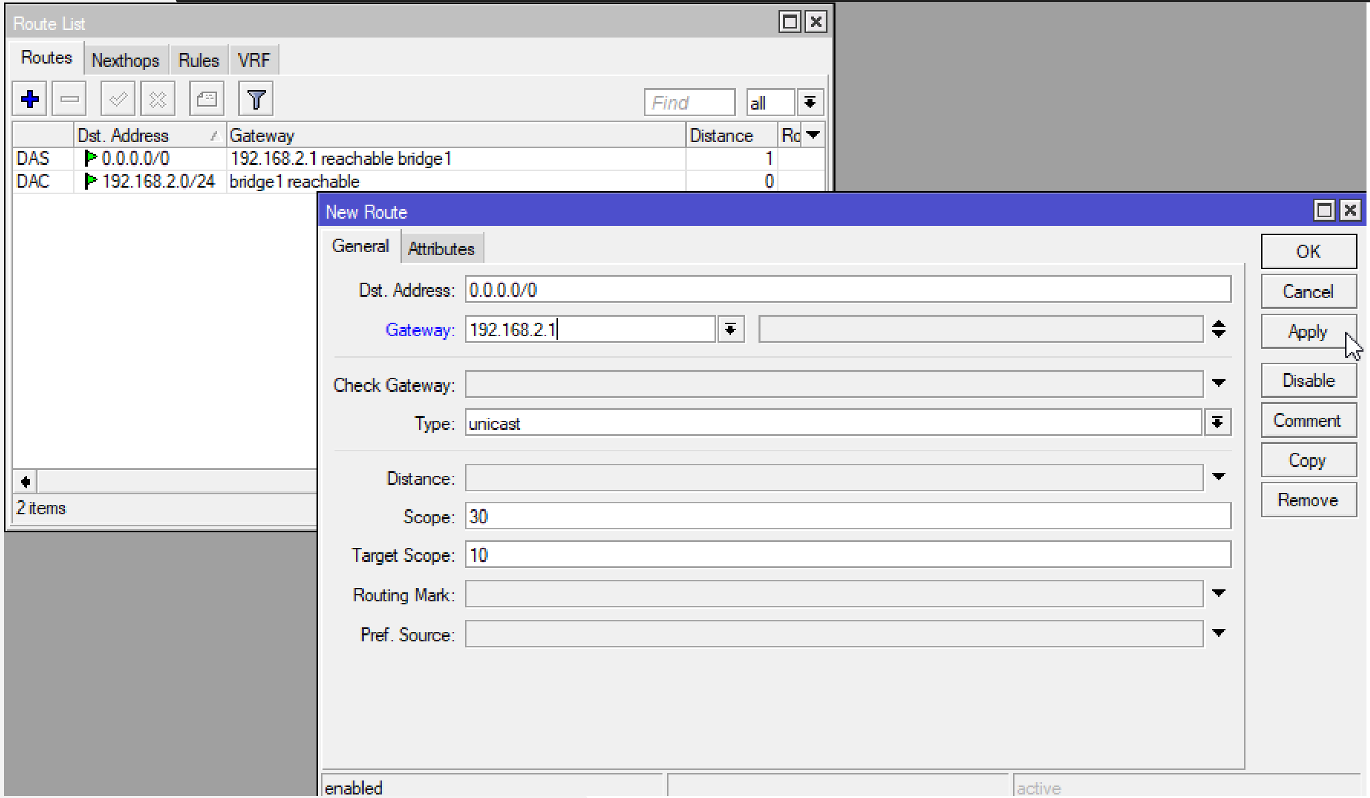
- IP – DHCP Client
- Japim +
- Zgjedhim Nderfaqjen
- Japim OK

# Adresat IP - Dinamike



| | Interface | Use Peer DNS | Add Default Route | IP Address | Expires After | Status |
|---|---|---|---|---|---|---|
| | ether1 | yes | yes | 192.168.2.2/24 | 23:59:39 | bound |

# Routes



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

2 items

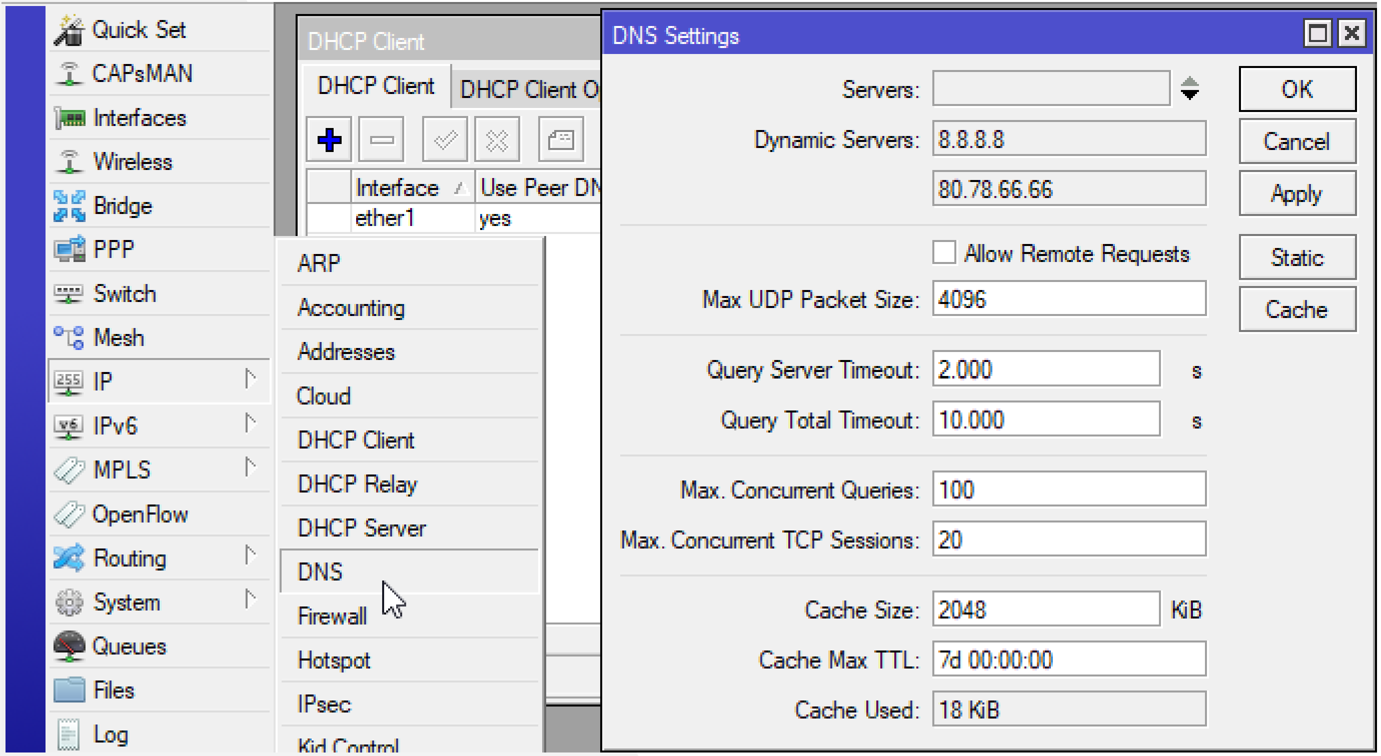
|  |  |
|---|---|
| Dst. Address: | 0.0.0.0/0 |
| Gateway: | 192.168.2.1 |
| Check Gateway: |  |
| Type: | unicast |
| Distance: |  |
| Scope: | 30 |
| Target Scope: | 10 |
| Routing Mark: |  |
| Pref. Source: |  |

enabled

active

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

# DNS



Servers:

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

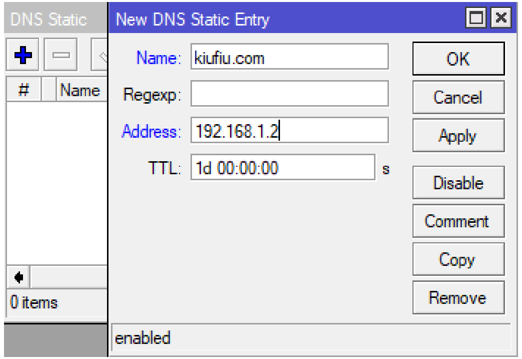
Max. Concurrent TCP Sessions: 20

Cache Size: 2048 KiB

Cache Max TTL: 7d 00:00:00

Cache Used: 18 KiB

- IP – DNS
- Vendosim IP e serverave
- Japim OK



Name: kiufiu.com

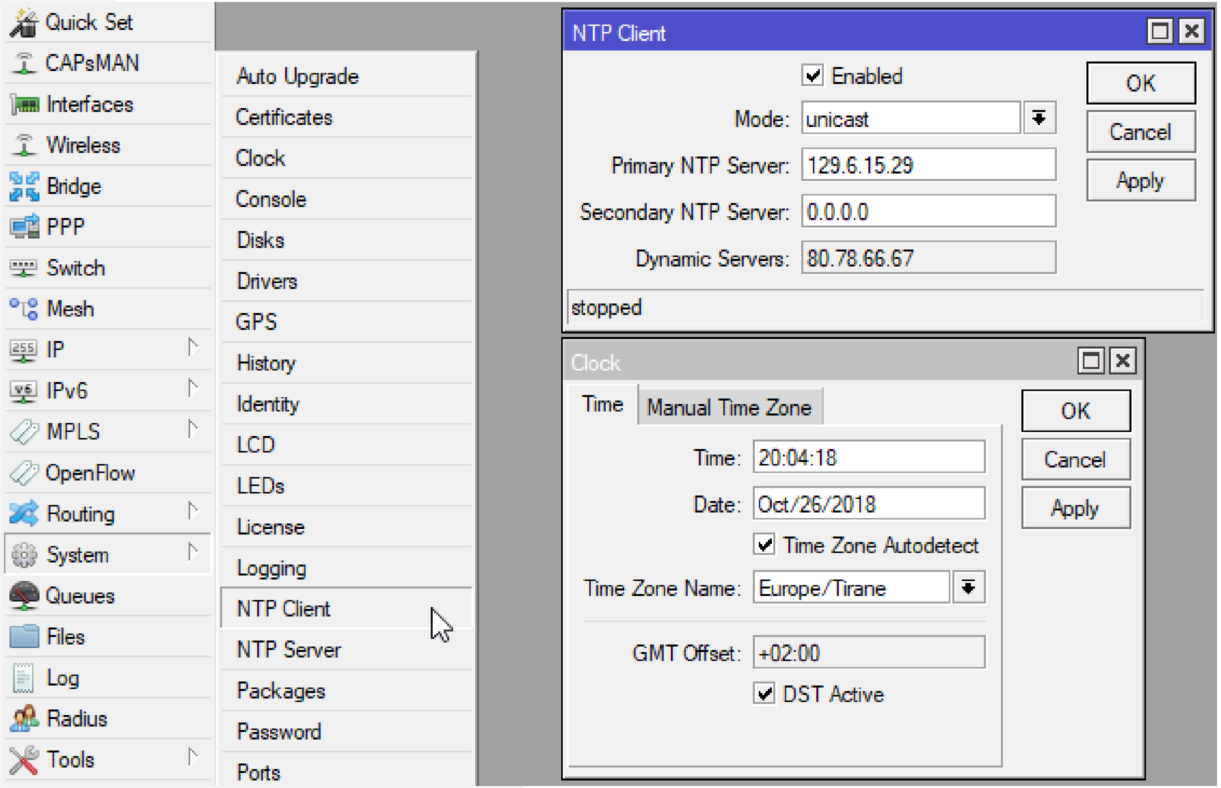
Regexp:

Address: 192.168.1.2

TTL: 1d 00:00:00 s

enabled

# NTP – Network Time Protocol



NTP Client

☑ Enabled

Mode: unicast

Primary NTP Server: 129.6.15.29

Secondary NTP Server: 0.0.0.0

Dynamic Servers: 80.78.66.67

stopped

Clock

Time: 20:04:18

Date: Oct/26/2018

☑ Time Zone Autodetect

Time Zone Name: Europe/Tirane

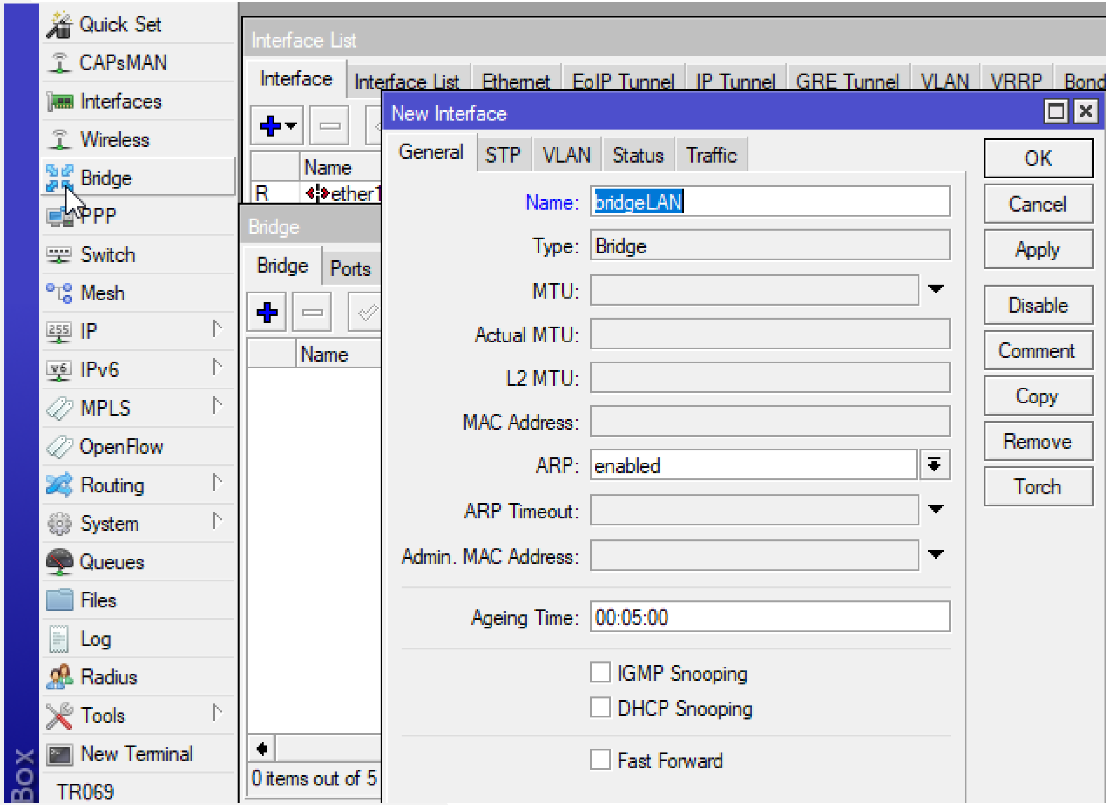
GMT Offset: +02:00

☑ DST Active

- System – NTP Client
- Vendosim IP e serverave
- Japim OK

- System – Clock
- Zgjedhim Time Zone
- Japim OK

# Bridge



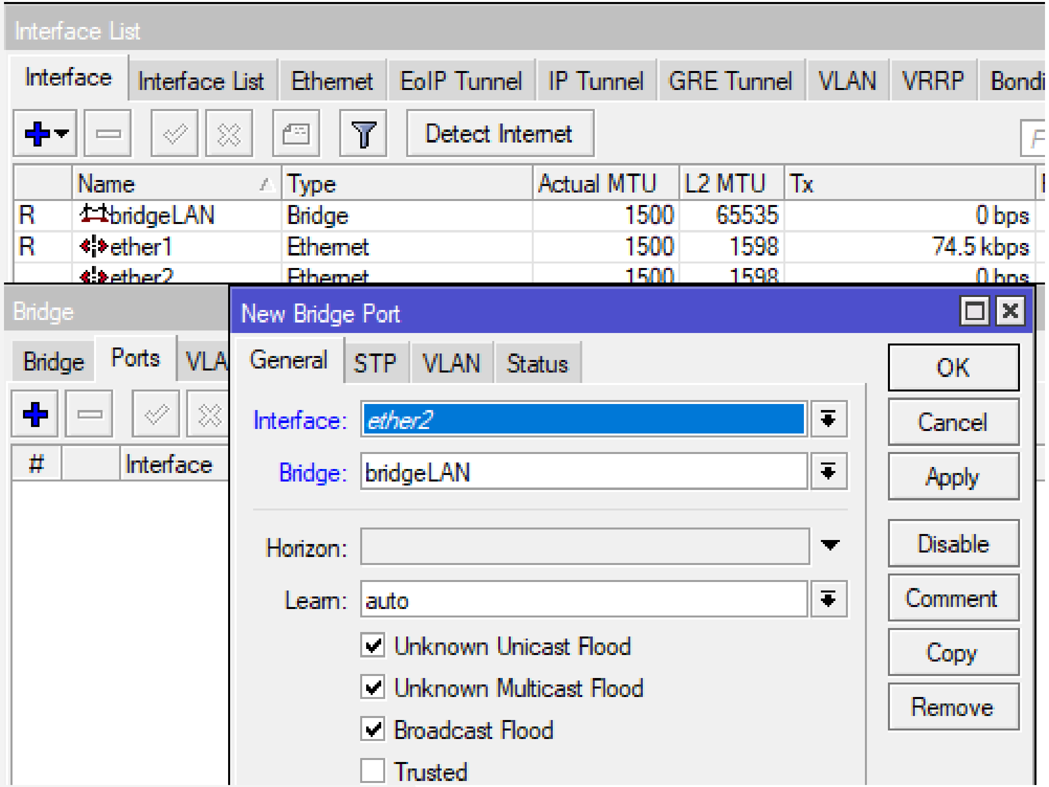
Name: bridgeLAN
Type: Bridge
MTU:
Actual MTU:
L2 MTU:
MAC Address:
ARP: enabled
ARP Timeout:
Admin. MAC Address:
Ageing Time: 00:05:00

□ IGMP Snooping
□ DHCP Snooping

□ Fast Forward

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

# Bridge - Ports



| | Name | Type | Actual MTU | L2 MTU | Tx |
|---|---|---|---|---|---|
| R | bridgeLAN | Bridge | 1500 | 65535 | 0 bps |
| R | ether1 | Ethernet | 1500 | 1598 | 74.5 kbps |
| | ether2 | Ethernet | 1500 | 1598 | 0 bps |

Interface: ether2

Bridge: bridgeLAN

Horizon:

Learn: auto

☑ Unknown Unicast Flood

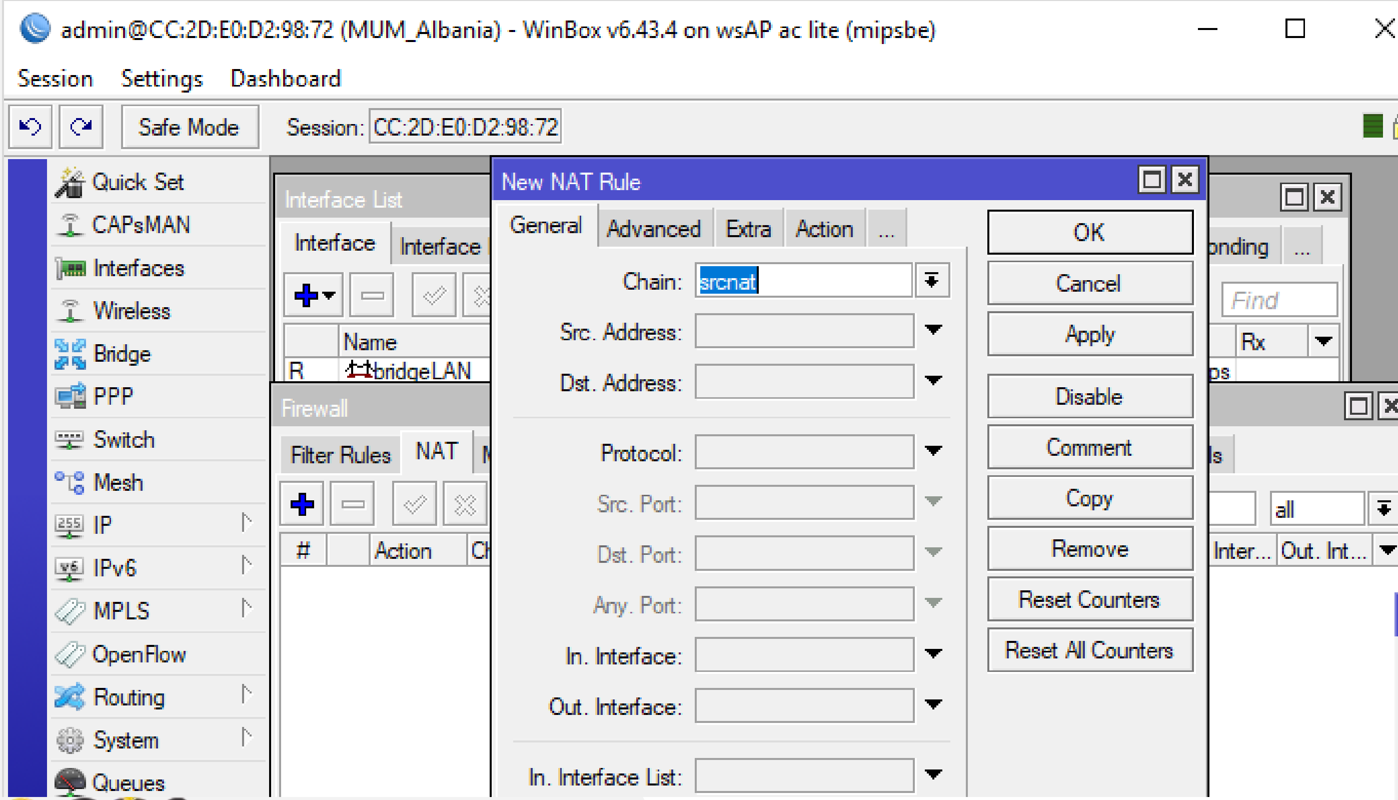
☑ Unknown Multicast Flood

☑ Broadcast Flood

□ Trusted

- Shkojme tek tab: Ports
- Shtojme portat duke zgjedhur Bridge e duhur
- Japim OK

# Masquerade



Chain: srcnat

Src. Address:

Dst. Address:

Protocol:

Src. Port:

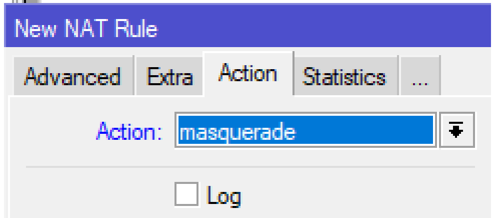
Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:



Action: masquerade

□ Log

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

# Diagrama (Skema)

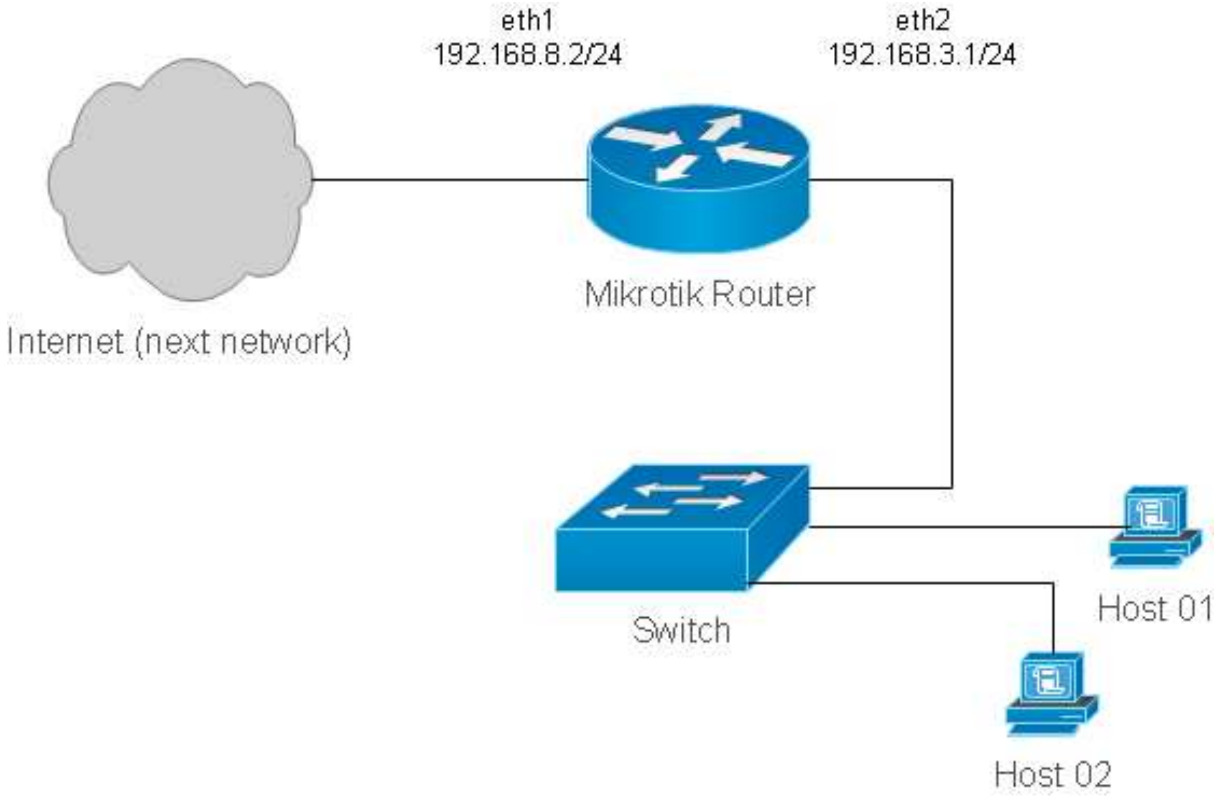
“Nuk duhet te nisim asnjehere nje konfigurim pa pasur te qarte pikat thelbesore te rrjetit ne fjale. Vizatimi i nje skeme te thjeshte ndihmon shume e na kthjellon idete”

# 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

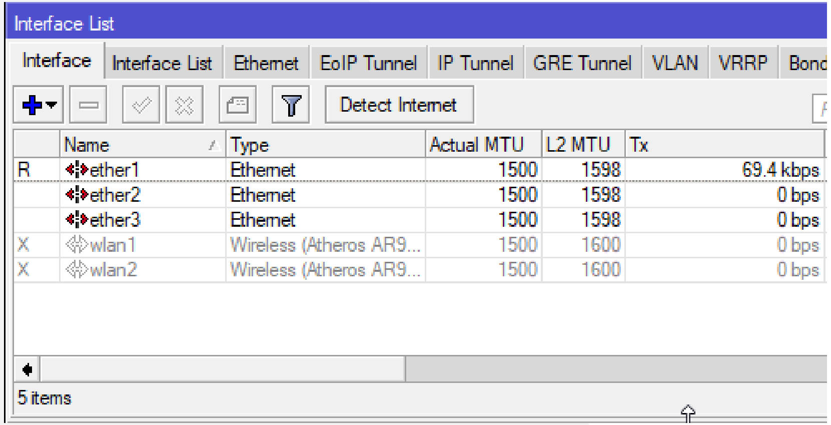


# Ruteri me i thjeshte

**Shembull:** Konfigurojme nje ruter me

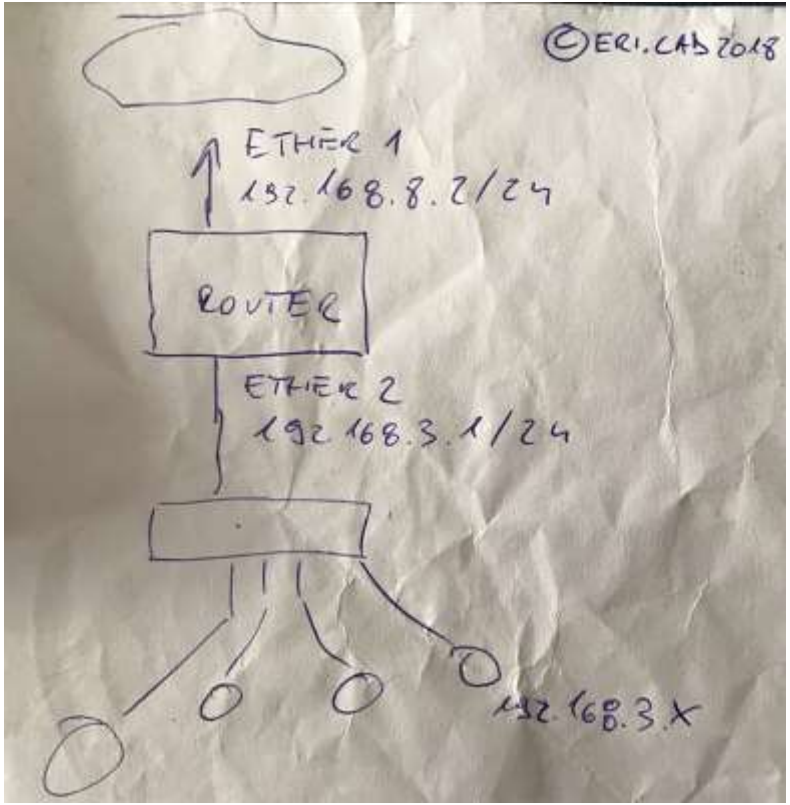
IP: 192.168.8.2/24 tek ether1

IP: 192.168.3.1/24 tek ether2



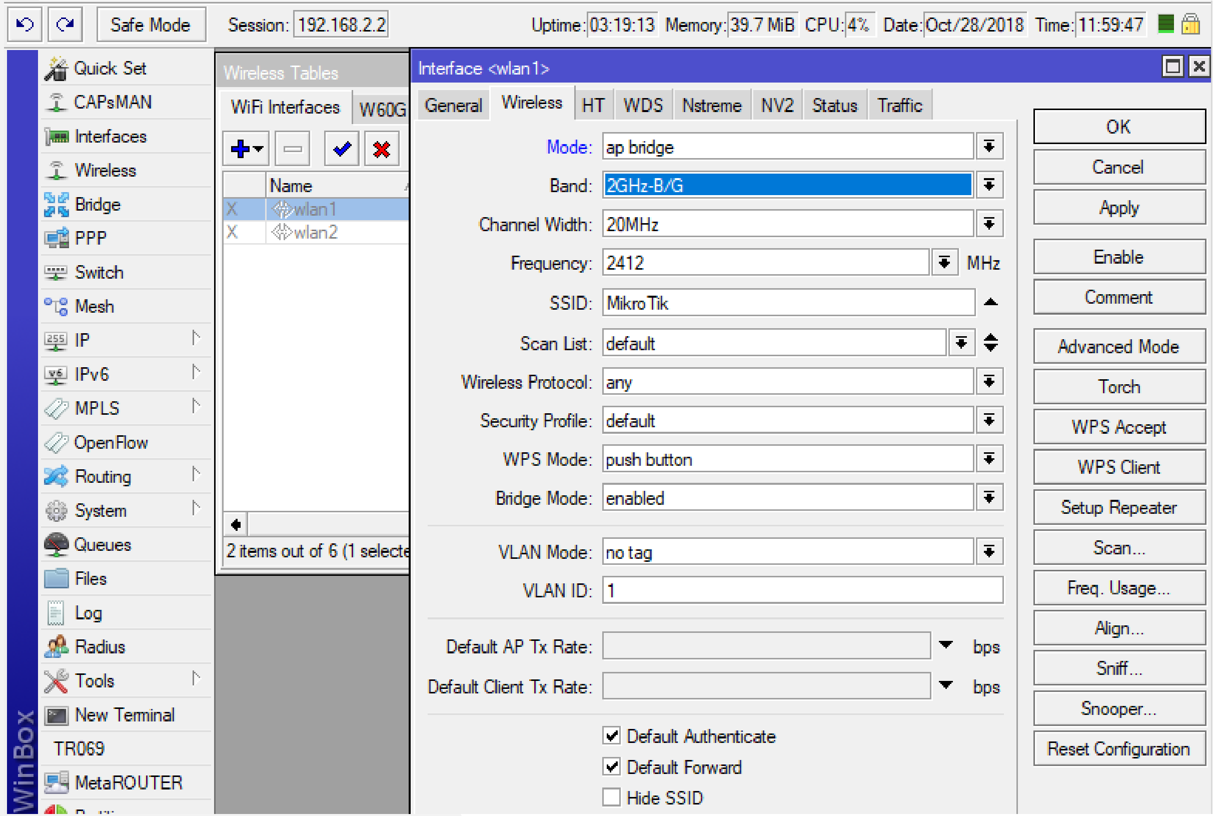
| | Name | Type | Actual MTU | L2 MTU | Tx |
|---|---|---|---|---|---|
| R | ether1 | Ethernet | 1500 | 1598 | 69.4 kbps |
| | ether2 | Ethernet | 1500 | 1598 | 0 bps |
| | ether3 | Ethernet | 1500 | 1598 | 0 bps |
| X | wlan1 | Wireless (Atheros AR9... | 1500 | 1600 | 0 bps |
| X | wlan2 | Wireless (Atheros AR9... | 1500 | 1600 | 0 bps |

5 items



# 3.
# Wireless

# Wireless



Session: 192.168.2.2 Uptime: 03:19:13 Memory: 39.7 MiB CPU: 4% Date: Oct/28/2018 Time: 11:59:47

| Name |
|---|
| X wlan1 |
| X wlan2 |

2 items out of 6 (1 selecte

Interface <wlan1>

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

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

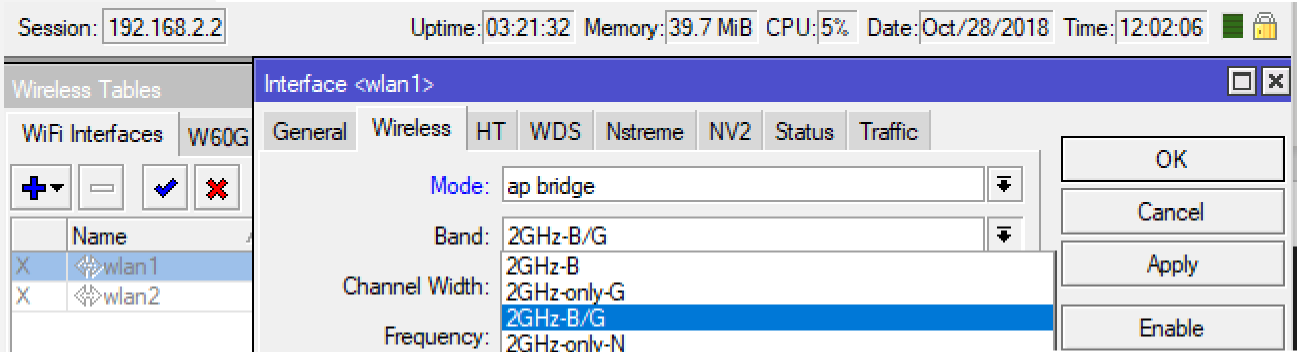
☑ Default Authenticate

☑ Default Forward

□ Hide SSID

- 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

Interface <wlan1>

Mode: ap bridge

Band: 2GHz-B/G

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

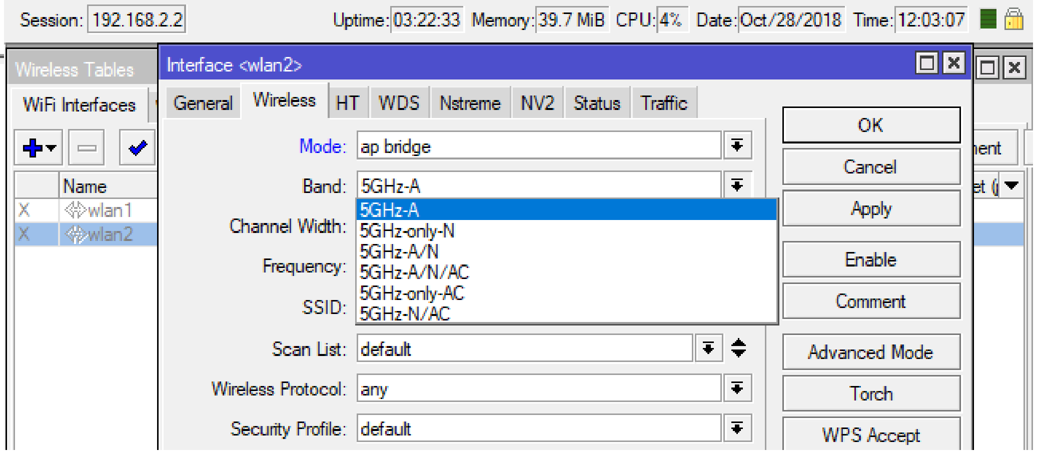
Channel Width:

Frequency:

SSID:

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

Interface <wlan2>

Mode: ap bridge

Band: 5GHz-A

- 5GHz-A
- 5GHz-only-N
- 5GHz-A/N
- 5GHz-A/N/AC
- 5GHz-only-AC
- 5GHz-N/AC

Channel Width:

Frequency:

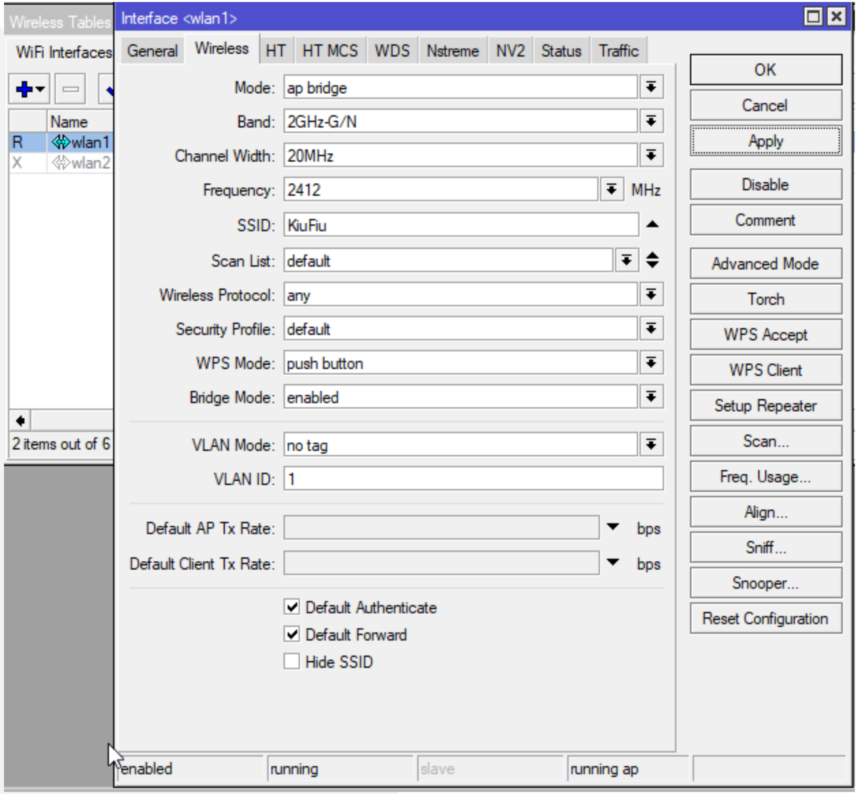
SSID:

Scan List: default

Wireless Protocol: any

Security Profile: default

# Wireless



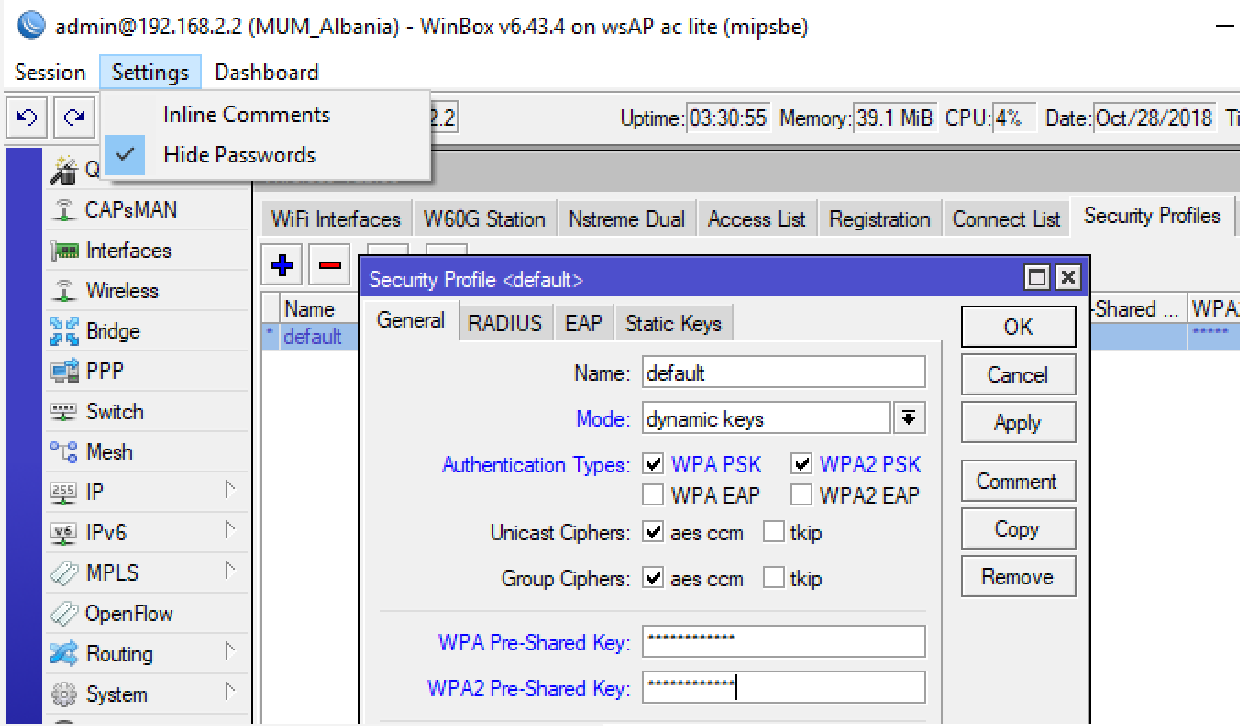
Mode: ap bridge
Band: 2GHz-G/N
Channel Width: 20MHz
Frequency: 2412 MHz
SSID: KiuFiu
Scan List: default
Wireless Protocol: any
Security Profile: default
WPS Mode: push button
Bridge Mode: enabled
VLAN Mode: no tag
VLAN ID: 1
Default AP Tx Rate: bps
Default Client Tx Rate: bps
☑ Default Authenticate
☑ Default Forward
□ Hide SSID

enabled | running | slave | running ap

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



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

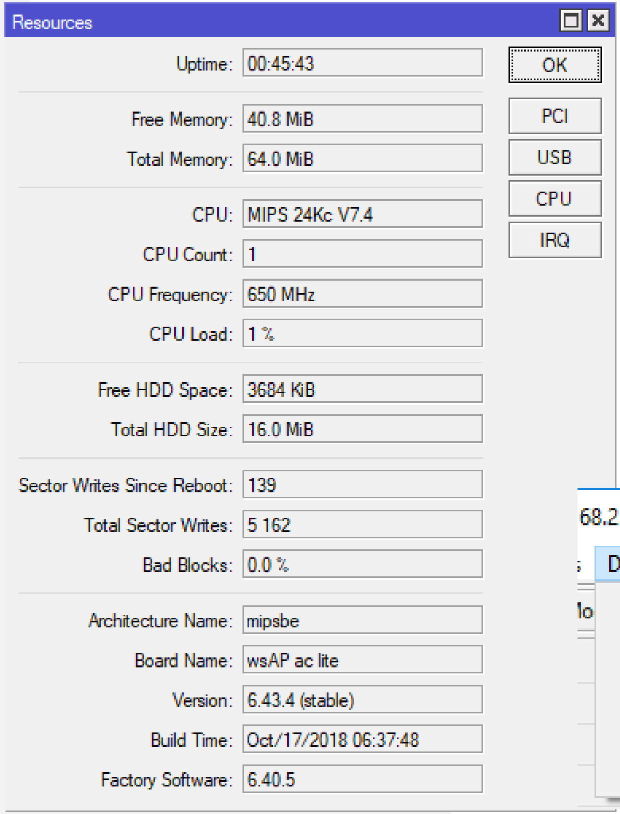
WPA Pre-Shared Key: *************

WPA2 Pre-Shared Key: *************

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

# 4.
# Monitorimi

# RESOURCES



Resources

Uptime: 00:45:43

Free Memory: 40.8 MiB

Total Memory: 64.0 MiB

CPU: MIPS 24Kc V7.4

CPU Count: 1

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

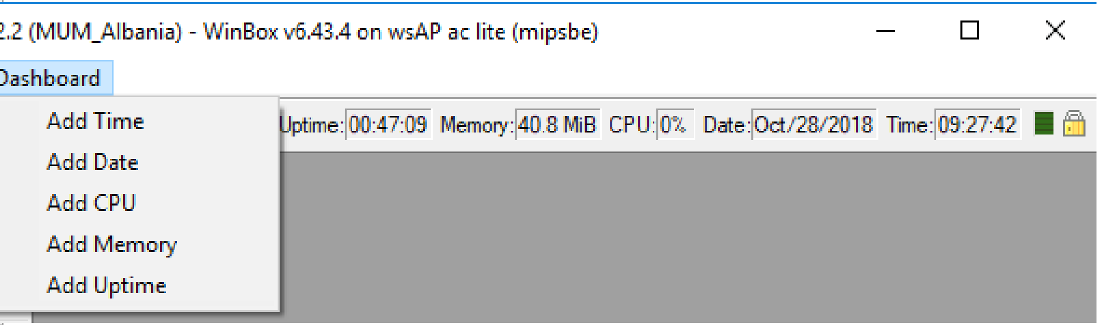
Board Name: wsAP ac lite

Version: 6.43.4 (stable)

Build Time: Oct/17/2018 06:37:48

Factory Software: 6.40.5

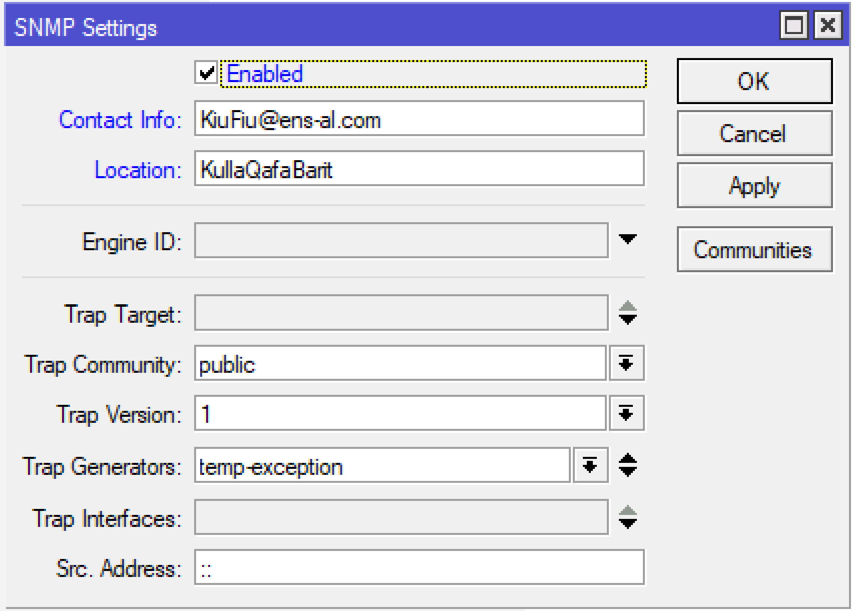
- System – Resources



68.2.2 (MUM_Albania) - WinBox v6.43.4 on wsAP ac lite (mipsbe)

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

# SNMP



SNMP Settings

☑ Enabled

Contact Info: KiuFiu@ens-al.com

Location: KullaQafaBarit

Engine ID:

Trap Target:

Trap Community: public

Trap Version: 1

Trap Generators: temp-exception

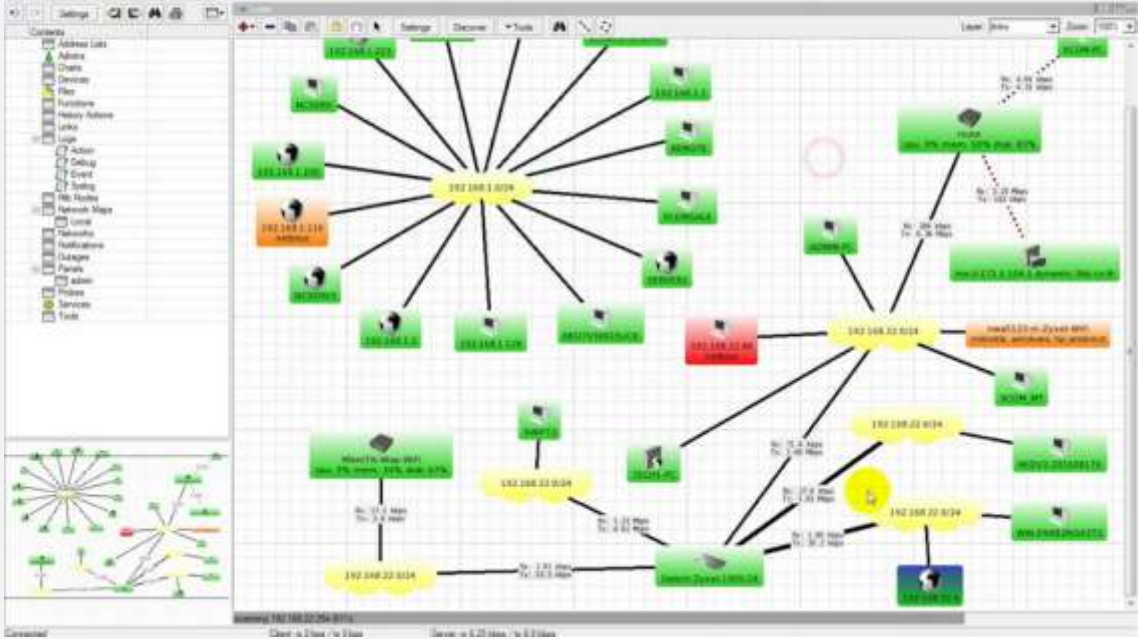
Trap Interfaces:

Src. Address: ::

## SIMPLE NETWORK MONITORING PROTOCOL

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

# THE DUDE



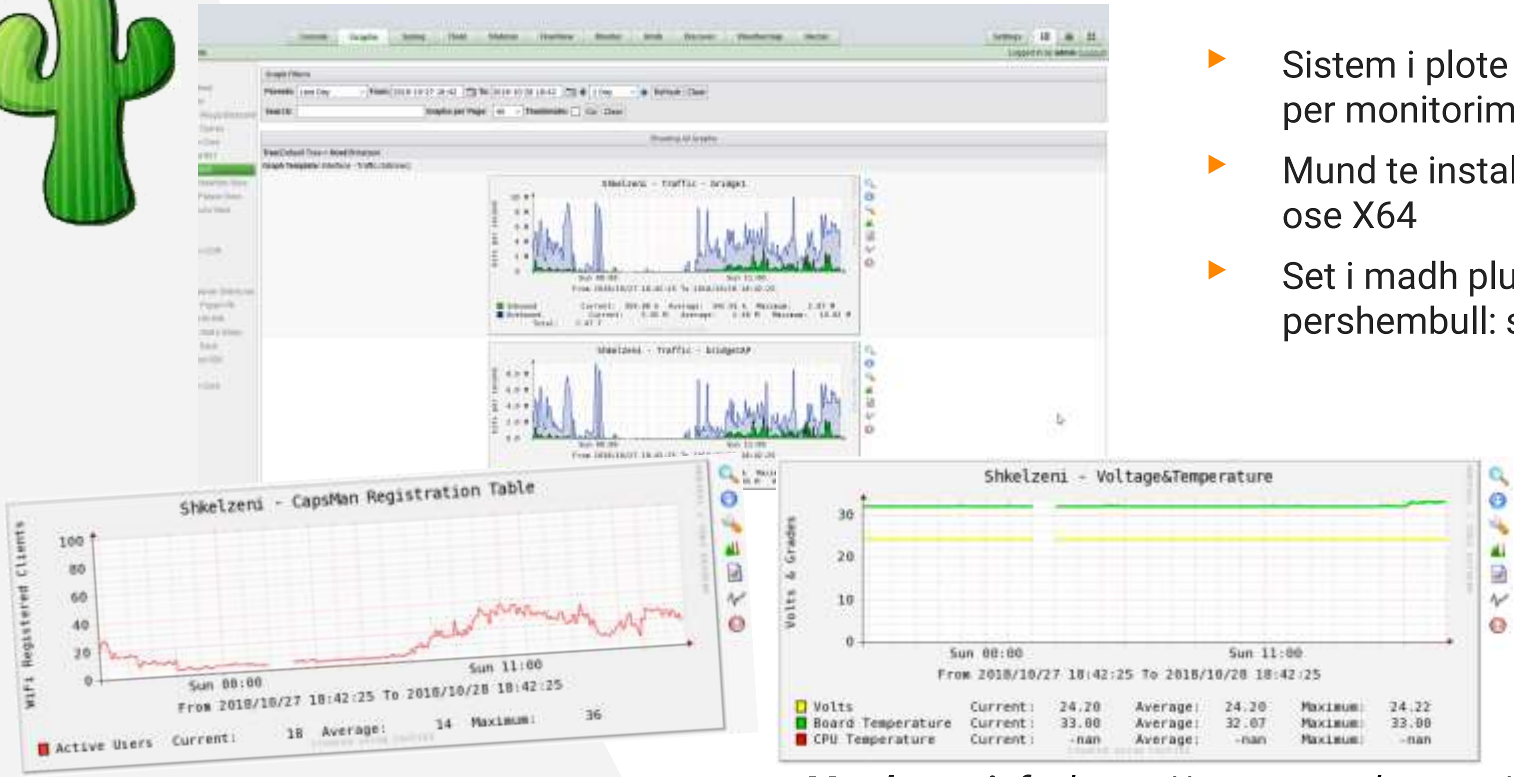
Sistem monitorimi falas nga MikroTik

Mund te instalohet ne:

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

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

# CACTI


Shkelzeni - Traffic - bridge1
Shkelzeni - Traffic - bridgeAP
Shkelzeni - CapsMan Registration Table
WiFi Registered Clients
100
80
60
40
20
0
Sun 00:00
Sun 11:00
Shkelzeni - Voltage&Temperature
Volts & Grades
30
20
10
0
Sun 00:00
Sun 11:00

From 2018/10/27 18:42:25 To 2018/10/28 18:42:25

🟥 Active Users Current: 18 Average: 14 Maximum: 36

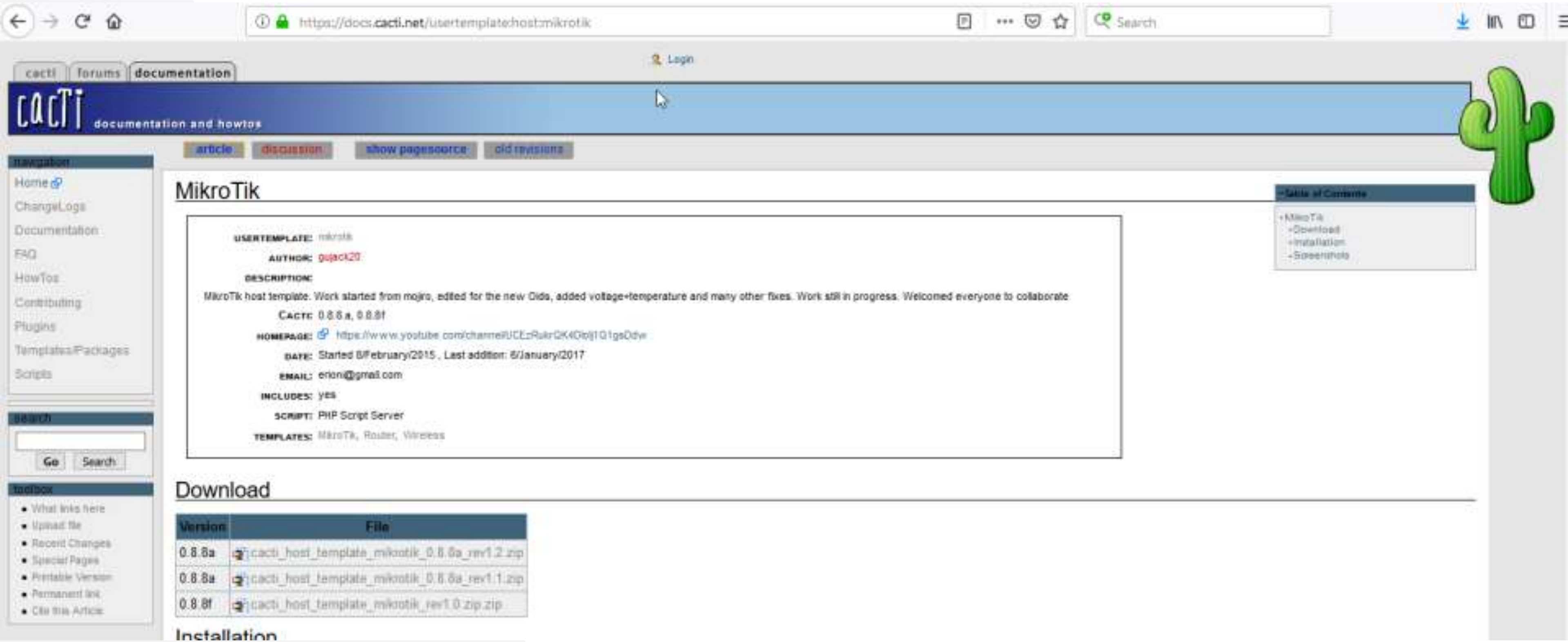
From 2018/10/27 18:42:25 To 2018/10/28 18:42:25

```
🟨 Volts              Current:  24.20   Average:  24.20   Maximum:  24.22
🟩 Board Temperature  Current:  33.00   Average:  32.07   Maximum:  33.00
🟥 CPU Temperature    Current:   -nan   Average:   -nan   Maximum:   -nan
```

- 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*

# CACTI



## MikroTik

USERTEMPLATE: mikrotik

AUTHOR: gujack20

DESCRIPTION:

MikroTik host template. Work started from mojro, edited for the new Oids, added voltage+temperature and many other fixes. Work still in progress. Welcomed everyone to collaborate

CACTI: 0.8.8.a, 0.8.8f

HOMEPAGE: https://www.youtube.com/channel/UCEzRukrQK4Oblj1Q1gsDdw

DATE: Started 8/February/2015 , Last addition: 6/January/2017

EMAIL: erioni@gmail.com

INCLUDES: yes

SCRIPT: PHP Script Server

TEMPLATES: MikroTik, Router, Wireless

## Download

| Version | File |
|---|---|
| 0.8.8a | cacti_host_template_mikrotik_0.8.8a_rev1.2.zip |
| 0.8.8a | cacti_host_template_mikrotik_0.8.8a_rev1.1.zip |
| 0.8.8f | cacti_host_template_mikrotik_rev1.0.zip.zip |

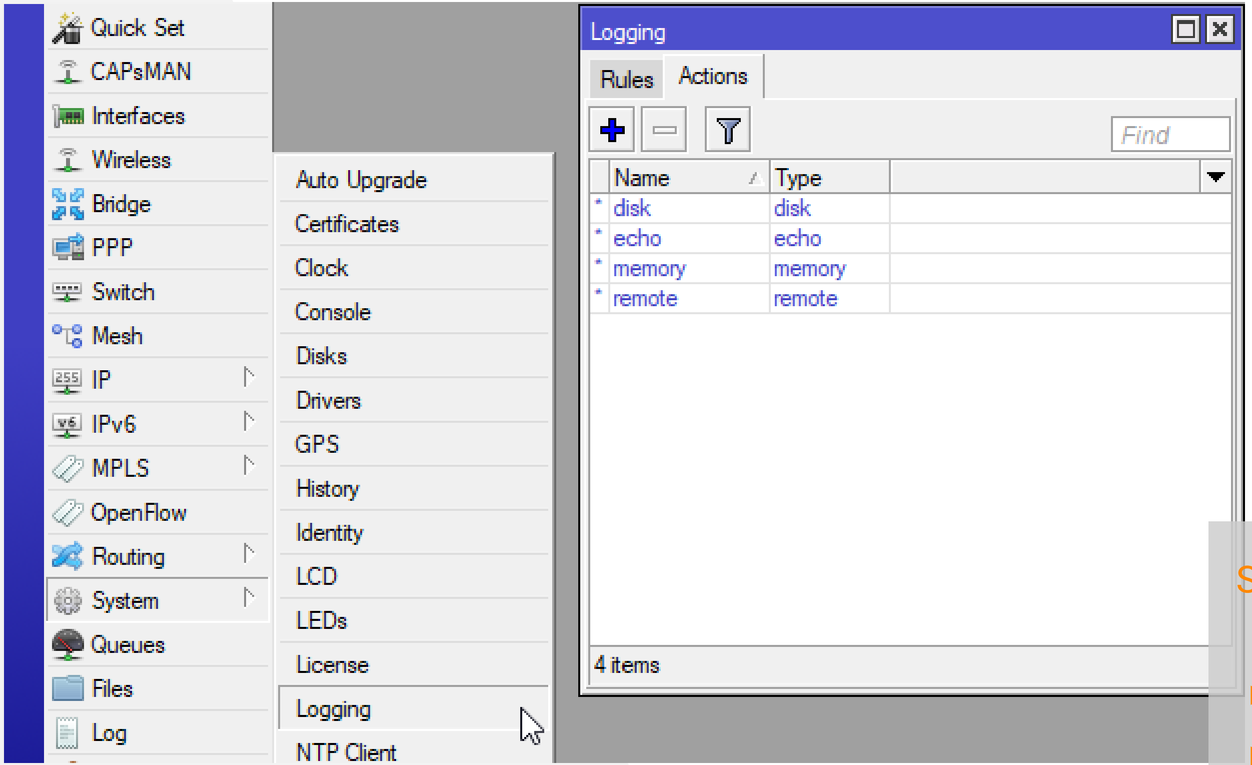
## Installation

# ZABBIX

ZABBIX

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

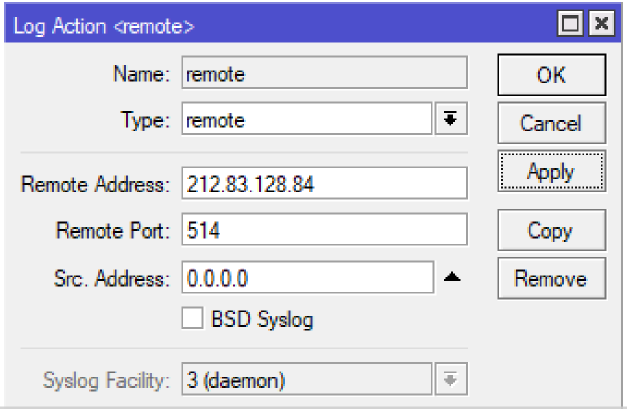
# Logging



| Name | Type |
|---|---|
| * disk | disk |
| * echo | echo |
| * memory | memory |
| * remote | remote |

4 items

- System – Logging
- Action – Remote



Name: remote

Type: remote

Remote Address: 212.83.128.84

Remote Port: 514

Src. Address: 0.0.0.0

□ BSD Syslog

Syslog Facility: 3 (daemon)

Syslog Severity:

default

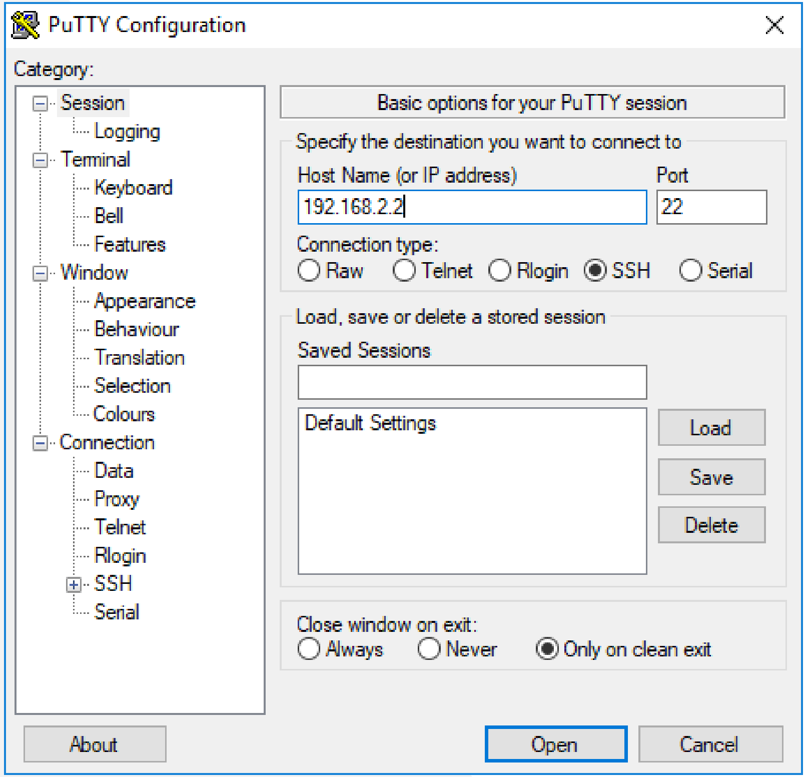
Servera qe mund te perdoren

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

# 5. CLI

# CLI

putty.exe



Specify the destination you want to connect to

Host Name (or IP address): 192.168.2.2

Port: 22

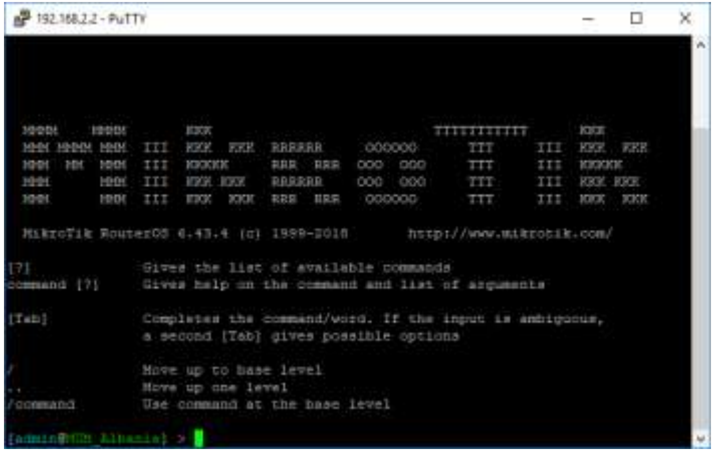
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

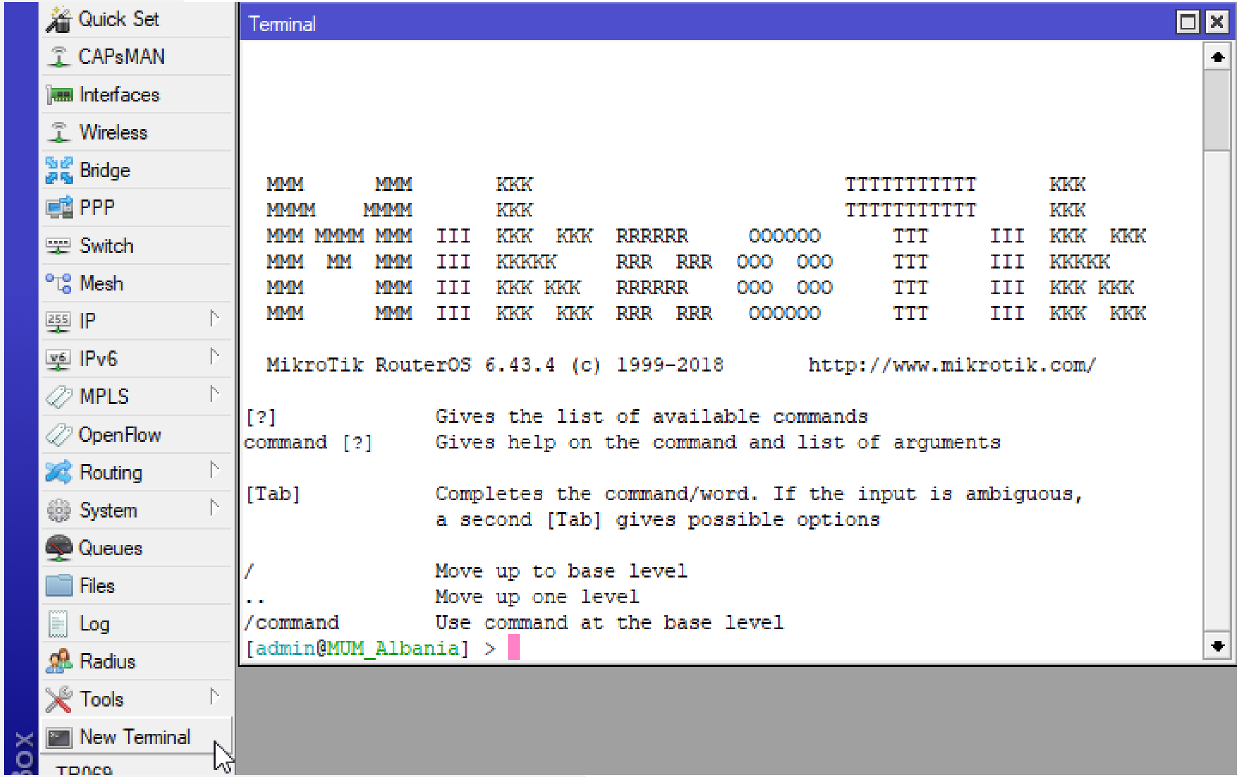
## COMMAND LINE INTERFACE

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



```
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.43.4 (c) 1999-2018       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level

[admin@MUM Albania] >
```

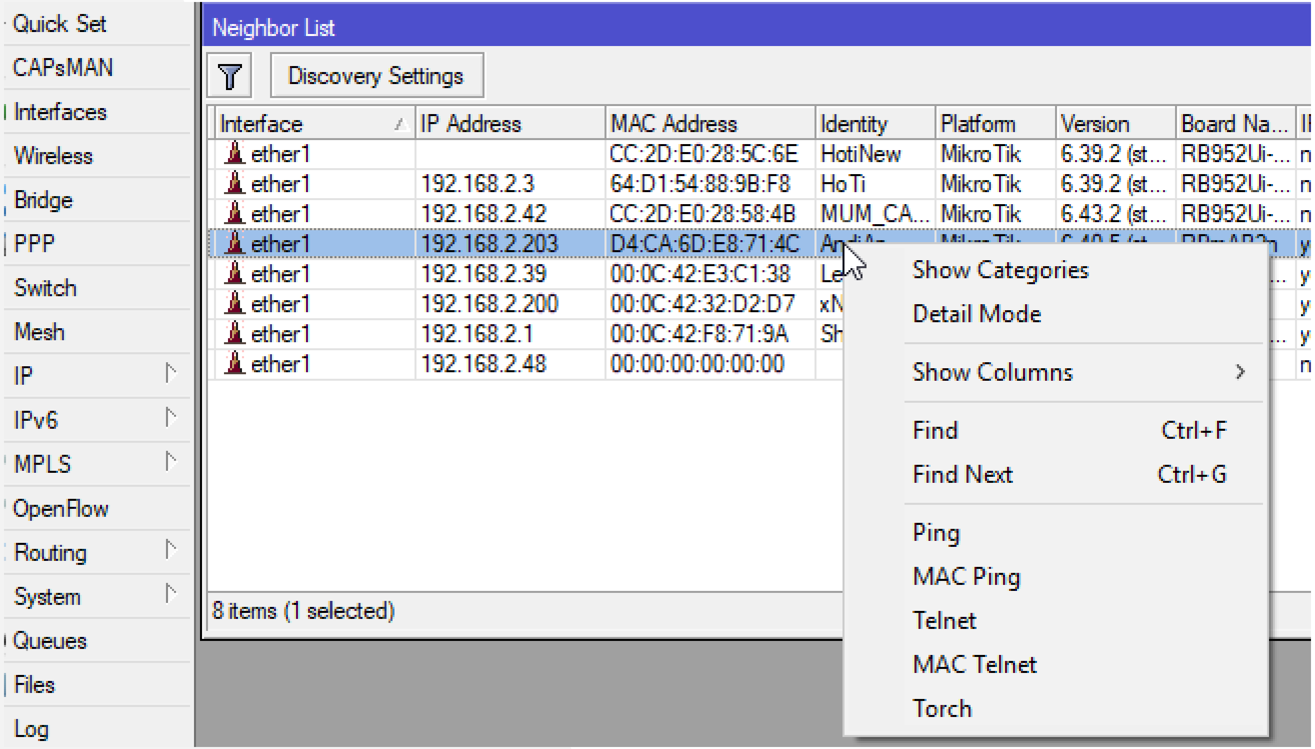
# CLI



```
  MMM      MMM       KKK                          TTTTTTTTTTT      KKK
  MMMM    MMMM       KKK                          TTTTTTTTTTT      KKK
  MMM MMMM MMM  III  KKK  KKK  RRRRRR     OOOOOO      TTT     III  KKK  KKK
  MMM  MM  MMM  III  KKKKK     RRR  RRR  OOO  OOO     TTT     III  KKKKK
  MMM      MMM  III  KKK KKK   RRRRRR    OOO  OOO     TTT     III  KKK KKK
  MMM      MMM  III  KKK  KKK  RRR  RRR   OOOOOO      TTT     III  KKK  KKK

  MikroTik RouterOS 6.43.4 (c) 1999-2018       http://www.mikrotik.com/

[?]             Gives the list of available commands
command [?]     Gives help on the command and list of arguments

[Tab]           Completes the command/word. If the input is ambiguous,
                a second [Tab] gives possible options

/               Move up to base level
..              Move up one level
/command        Use command at the base level
[admin@MUM_Albania] >
```

- Winbox – New Terminal

# CLI



| Interface | IP Address | MAC Address | Identity | Platform | Version | Board Na... | I |
|---|---|---|---|---|---|---|---|
| ether1 | | CC:2D:E0:28:5C:6E | HotiNew | MikroTik | 6.39.2 (st... | RB952Ui-... | n |
| ether1 | 192.168.2.3 | 64:D1:54:88:9B:F8 | HoTi | MikroTik | 6.39.2 (st... | RB952Ui-... | n |
| ether1 | 192.168.2.42 | CC:2D:E0:28:58:4B | MUM_CA... | MikroTik | 6.43.2 (st... | RB952Ui-... | n |
| ether1 | 192.168.2.203 | D4:CA:6D:E8:71:4C | [illegible] | [illegible] | [illegible] | [illegible] | 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)

- 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 permban:
  - http server vulneravility
  - Winbox unauthenticated file read

# CIA VAULT 7

- 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 dobesi 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;

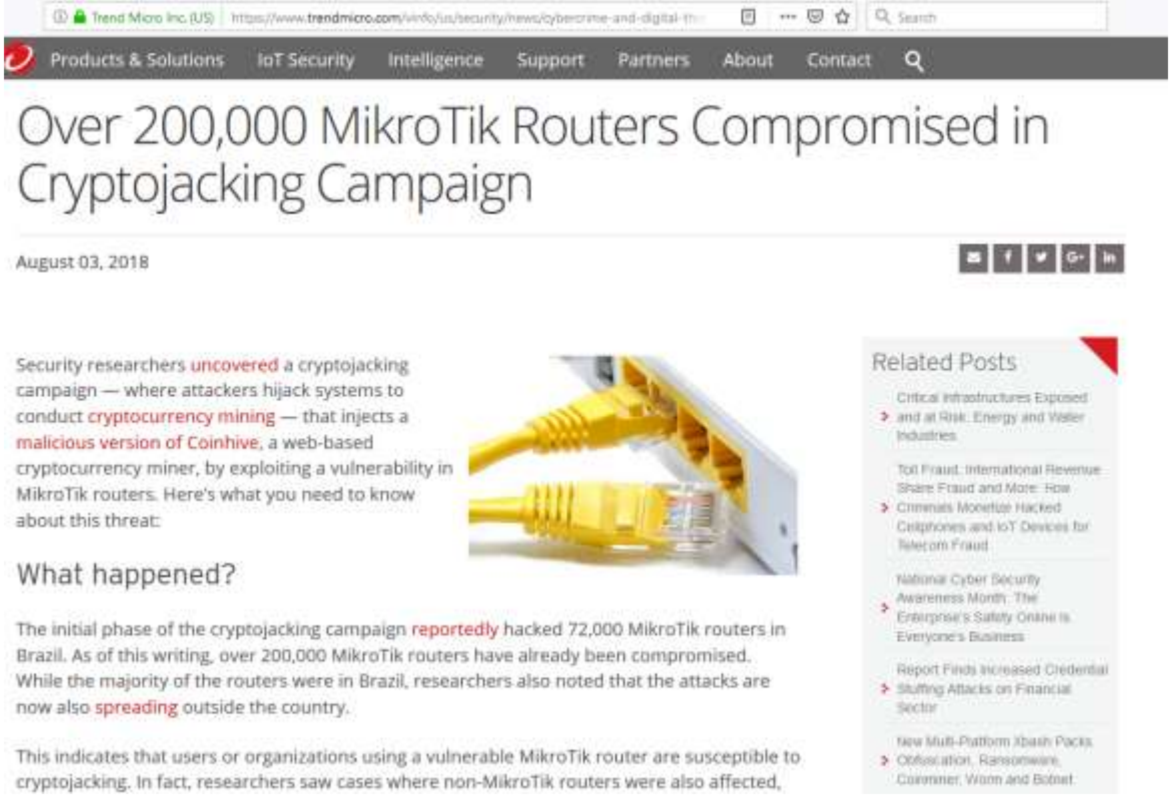
# Chimay Red – http server vulnerability

- Ne dokumentat e Vault7 permbahet vetem menyra si te shfrytezohet kjo dobesi, dhe jo nje kod aktual per t’u ekzekutuar

- Keqberesit neper bote e kane shfrytezuar Chimay Red per:
  - Tinyshell, 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



## 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.

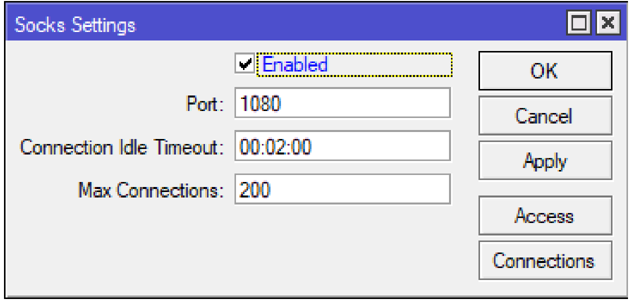
This indicates that users or organizations using a vulnerable MikroTik router are susceptible to cryptojacking. In fact, researchers saw cases where non-MikroTik routers were also affected,

Related Posts

- Critical Infrastructures Exposed and at Risk: Energy and Water Industries
- Toll 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, Coinminer, Worm and Botnet

# Winbox unauthenticated file read

- Shfrytezohet per:
  - Cryptocurrency mining
  - Socks proxy
  - DNS Server
  - etc..

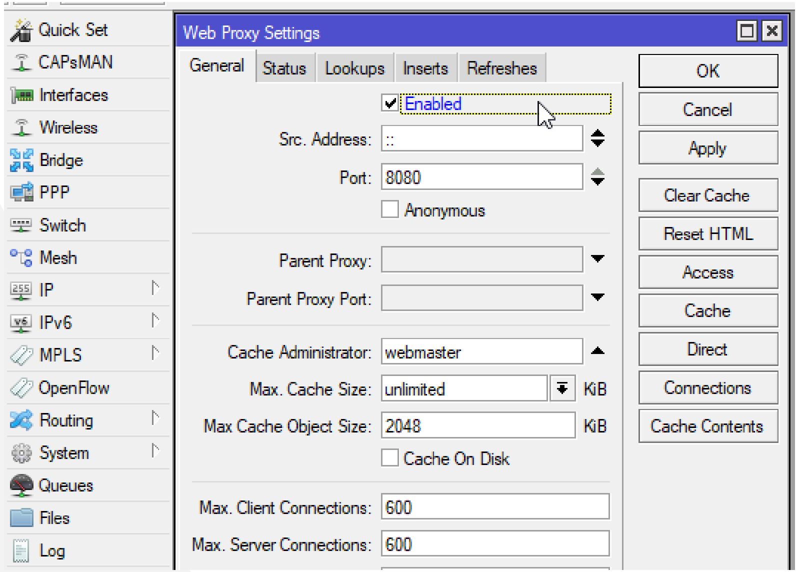

Socks Settings

☑ Enabled

Port: 1080

Connection Idle Timeout: 00:02:00

Max Connections: 200



Web Proxy Settings

☑ Enabled

Src. Address: ::

Port: 8080

☐ Anonymous

Parent Proxy:

Parent Proxy Port:

Cache Administrator: webmaster

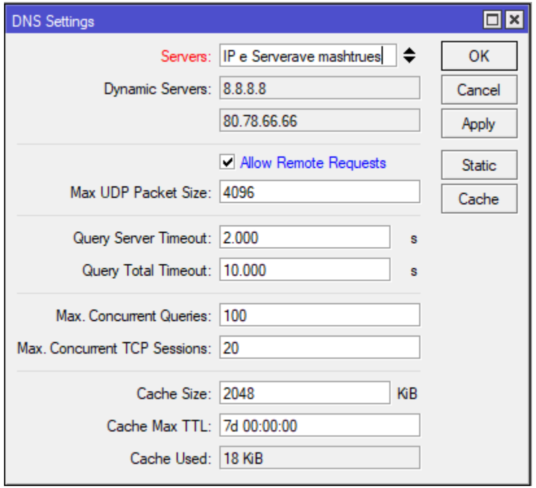
Max. Cache Size: unlimited KiB

Max Cache Object Size: 2048 KiB

☐ Cache On Disk

Max. Client Connections: 600

Max. Server Connections: 600


DNS Settings

Servers: IP e Serverave mashtrues

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

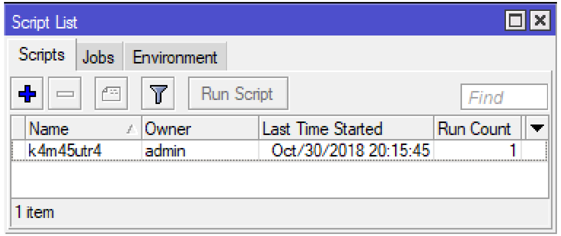
Cache Size: 2048 KiB

Cache Max TTL: 7d 00:00:00

Cache Used: 18 KiB

# Vulnerabilities

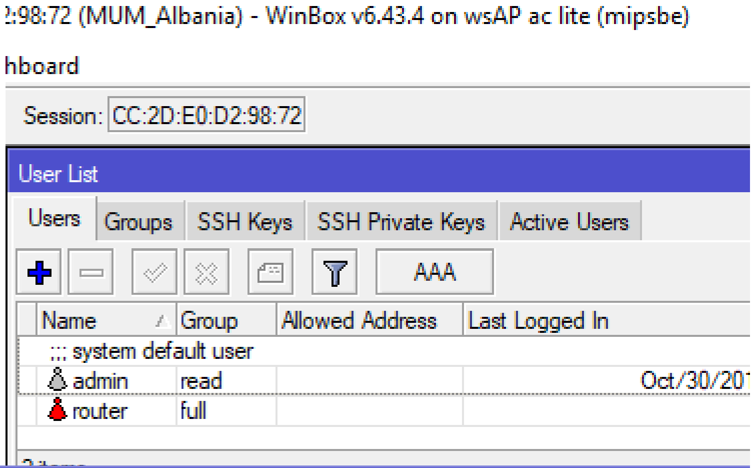
- Simptomat:
  - Usera te tjere te krijuar
  - Socks proxy aktive
  - Web proxy active
  - DNS Server
  - Scripte te panjohur
  - Pamundesi logimi ne ruter



Script List

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

1 item



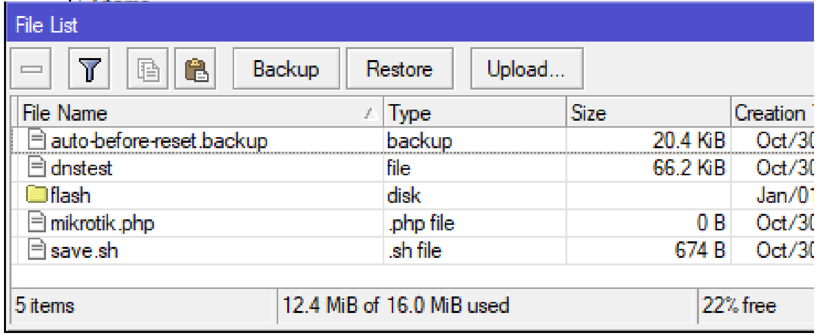
:98:72 (MUM_Albania) - WinBox v6.43.4 on wsAP ac lite (mipsbe)

hboard

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

User List

| Name | Group | Allowed Address | Last Logged In |
|---|---|---|---|
| ::: system default user | | | |
| admin | read | | Oct/30/201 |
| router | full | | |

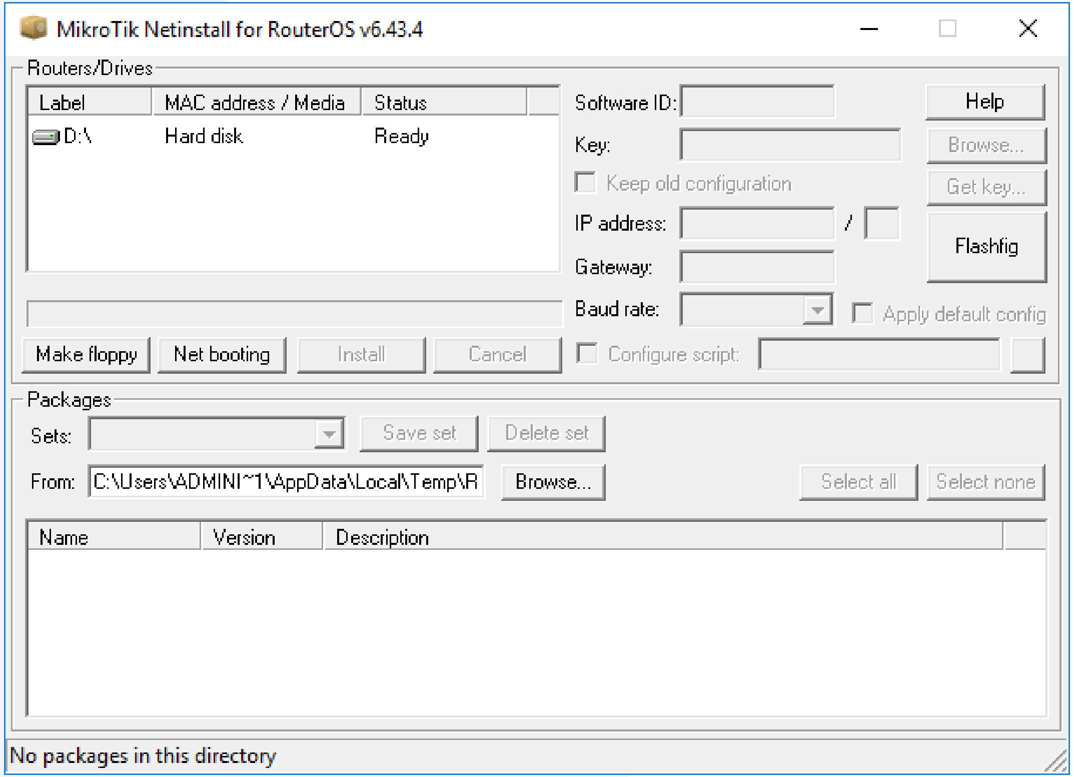


File List

| File Name | Type | Size | Creation |
|---|---|---|---|
| auto-before-reset.backup | backup | 20.4 KiB | Oct/3 |
| dnstest | file | 66.2 KiB | Oct/3 |
| flash | disk | | Jan/0 |
| mikrotik.php | .php file | 0 B | Oct/3 |
| save.sh | .sh file | 674 B | Oct/3 |

5 items | 12.4 MiB of 16.0 MiB used | 22% free

# Zgjidhja



MikroTik Netinstall for RouterOS v6.43.4

Routers/Drives

| Label | MAC address / Media | Status |
|---|---|---|
| D:\ | Hard disk | Ready |

Packages

From: C:\Users\ADMINI~1\AppData\Local\Temp\R

| Name | Version | Description |
|---|---|---|

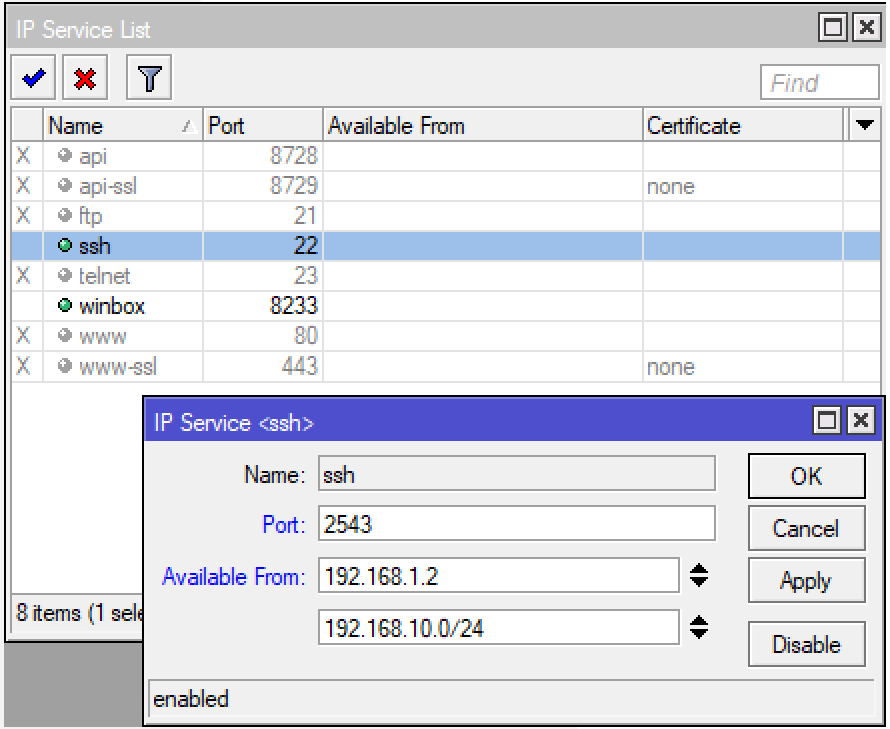
No packages in this directory

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



IP Service List

|  | Name | Port | Available From | Certificate |
|---|---|---|---|---|
| X | api | 8728 |  |  |
| X | api-ssl | 8729 |  | none |
| X | ftp | 21 |  |  |
|  | ssh | 22 |  |  |
| X | telnet | 23 |  |  |
|  | winbox | 8233 |  |  |
| X | www | 80 |  |  |
| X | www-ssl | 443 |  | none |

8 items (1 sele

IP Service <ssh>

Name: ssh

Port: 2543

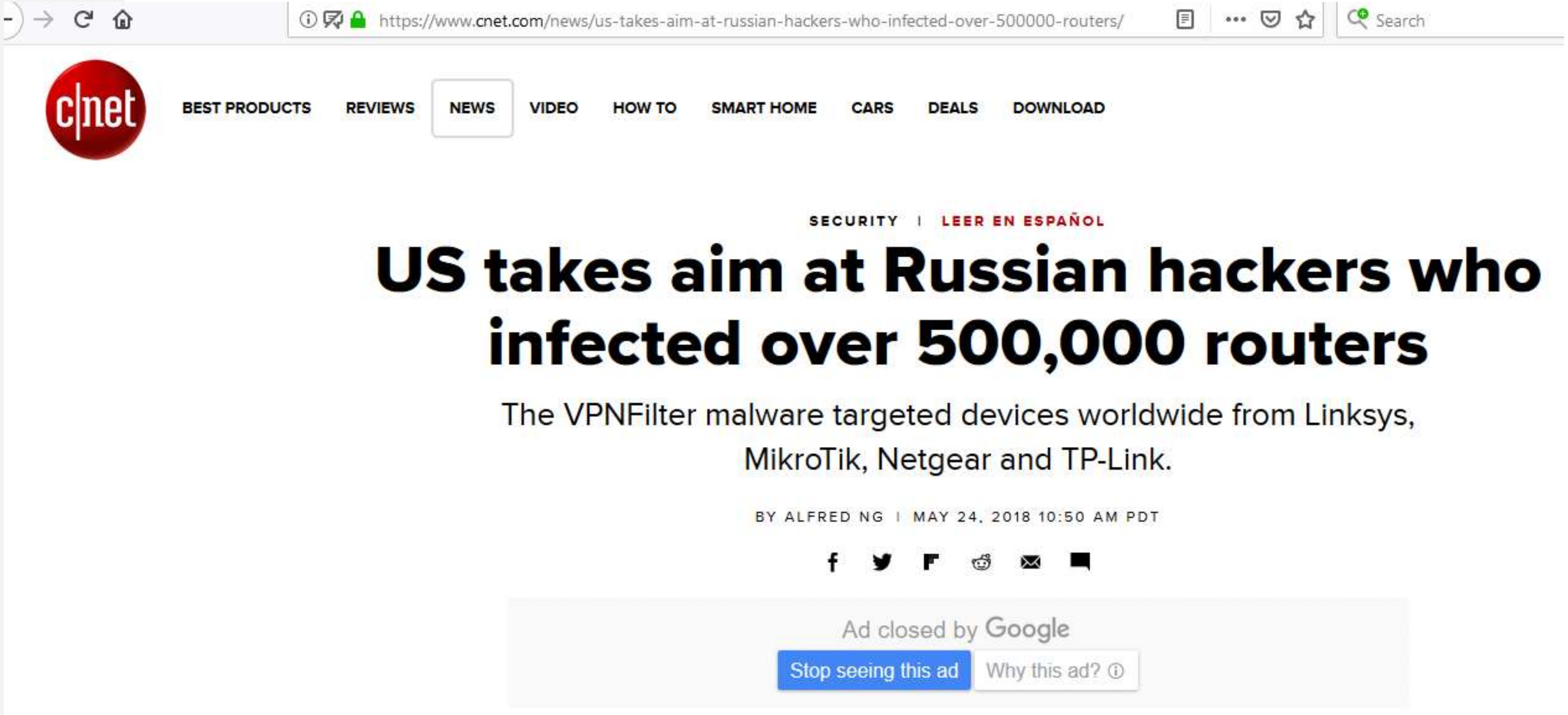
Available From: 192.168.1.2

192.168.10.0/24

enabled

- 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.

# Me shume info



https://www.cnet.com/news/us-takes-aim-at-russian-hackers-who-infected-over-500000-routers/
Search
cnet
BEST PRODUCTS
REVIEWS
NEWS
VIDEO
HOW TO
SMART HOME
CARS
DEALS
DOWNLOAD

SECURITY | LEER EN ESPAÑOL

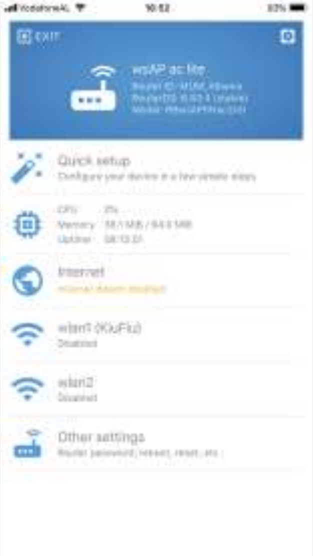
## US takes aim at Russian hackers who infected over 500,000 routers

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

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

# WINBOX në IPHONE

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



VodafoneAL 10:52 83%

EXIT

wsAP ac lite
[illegible]

Quick setup
Configure your device in a few simple steps

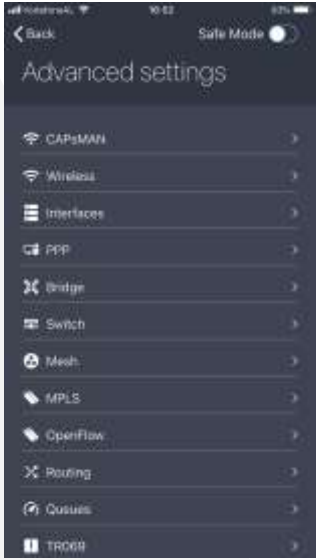
CPU: 2%
Memory: 58.1 MiB / 64.0 MiB
Uptime: 08:13:01

Internet
[illegible]

wlan1 (KiuFiu)
Disabled

wlan2
Disabled

Other settings
Router password, reboot, reset, etc.

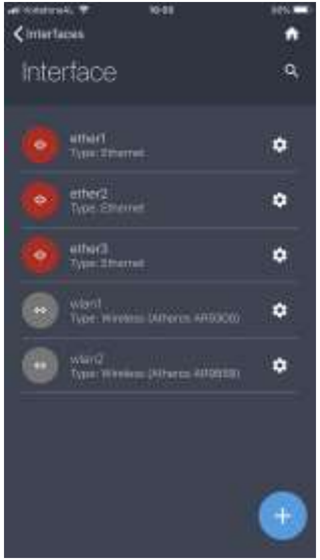


VodafoneAL 10:52 83%

Back — Safe Mode

Advanced settings

- CAPsMAN
- Wireless
- Interfaces
- PPP
- Bridge
- Switch
- Mesh
- MPLS
- OpenFlow
- Routing
- Queues
- TR069



VodafoneAL 10:53

Interfaces

Interface

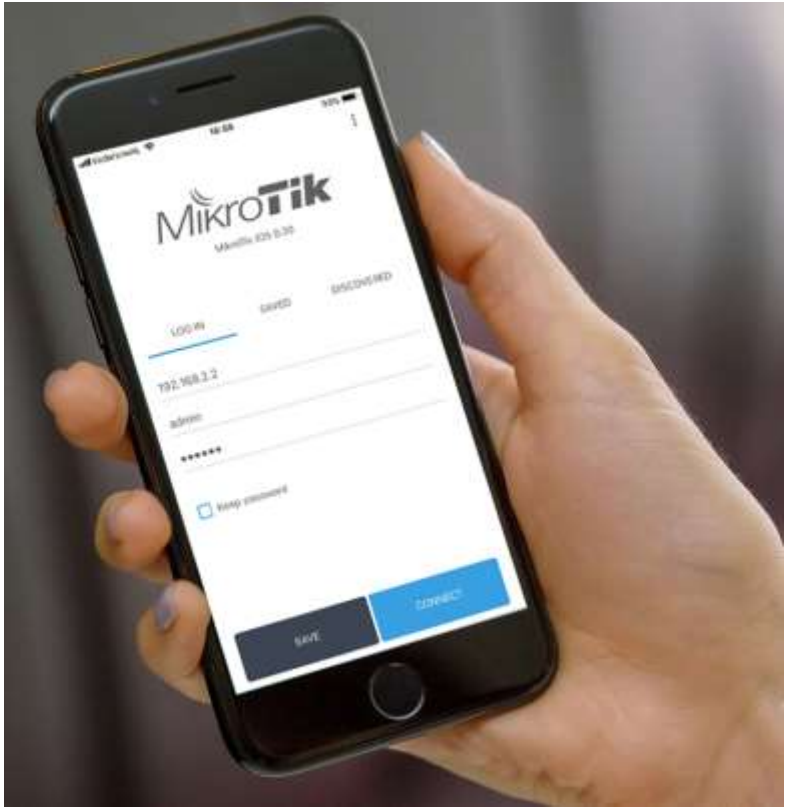
ether1
Type: Ethernet

ether2
Type: Ethernet

ether3
Type: Ethernet

wlan1
Type: Wireless (Atheros AR9300)

wlan2
Type: Wireless (Atheros AR9888)



# FALEMINDERIT PER VEMENDJEN!

**Pyetje?**

erioni@gmail.com