

# MikroTik User Meeting

Conference. Exhibition. Workshop.

## Lifehack for router protection and network

Presenter Vyacheslav Sambursky

Mikrotik Certified Trainer



# About me

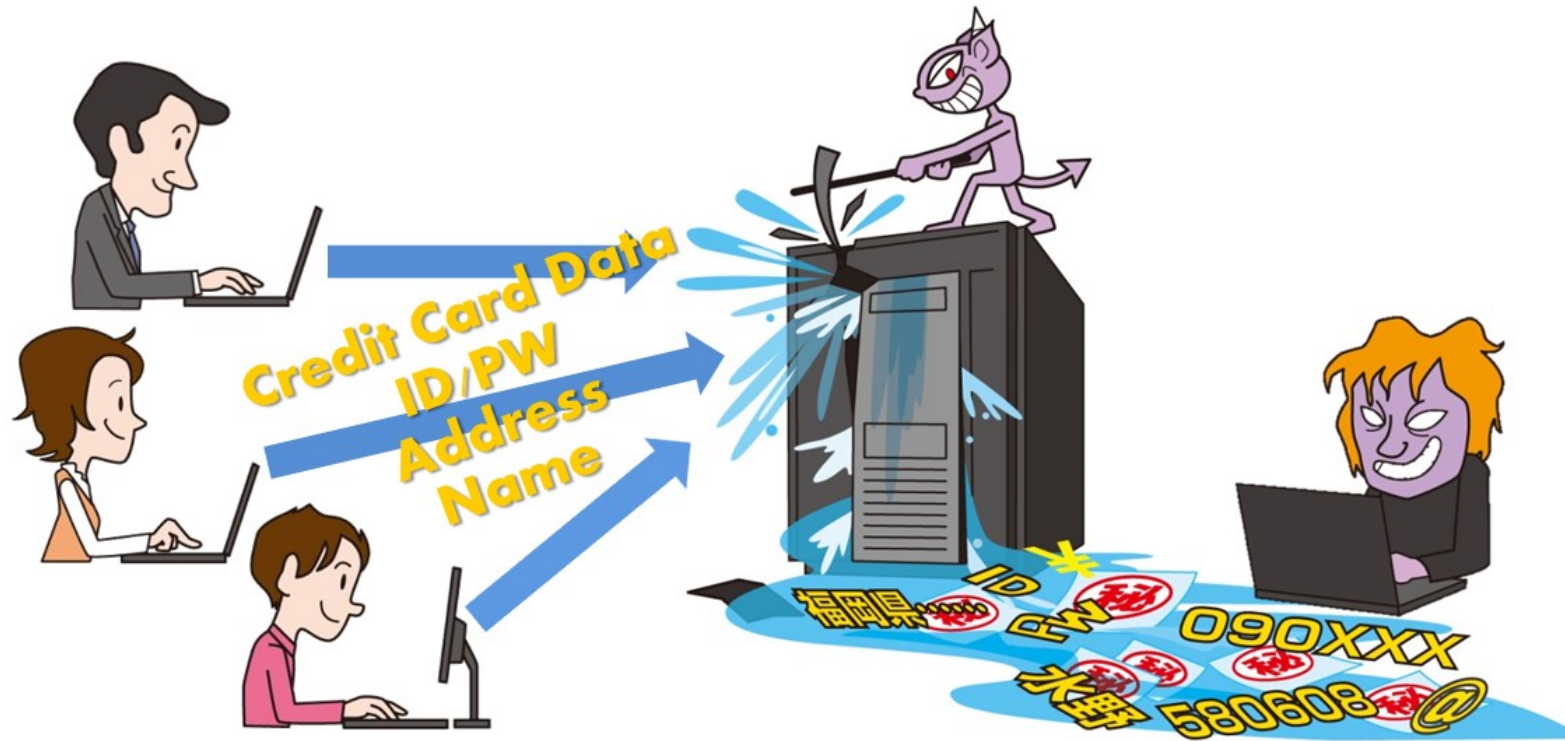
- Technical University of Moldova, 2003
- Academy of Economics Science, Master Degree, 2006
- IT Engineer from 2003
- Mikrotik Academy Trainer, 2012
- Mikrotik Trainer, 2014 Venice, European MUM.
- MUM Presentation
  - Chişinău - 2013
  - Bucureşti – 2014
  - Bucureşti – 2018

# De ce MikroTik Routerboard?

- De ce NU?
- Caracteristici generale ale routerelor Mikrotik
  - Fiabilitate
  - Opțiuni extinse
  - Flexibilitate
  - Gamă variată de soluții
  - Preț accesibil (comparativ cu giganții din clasa )
  - Hardware upgrade ușor
  - Alte

# Amenințări ale securității

- Interne – cauzate de clienții rețelei administrate de departamentul IT
- Externe – cauzate de hackeri și alte surse



# PASSWORD

- Pe echipamente se setează Parolă ( PASSWORD )
  - Local
  - Centralizat (Radius)



# PASSWORD

- Local settings.
- Creați useri cu dreptul de accesare de pe anumite adrese IP
- În caz că IP oferit de ISP este dinamic (PPPoE, LTE ...) folosiți VPN
- Utilizatorii se adaugă în meniul ***/system users***

# PASSWORD

User List

Users Groups SSH Keys SSH Private Keys Active Users

+ - ✓ ✗ [icon] [icon] AAA Find

| Name                    | Group | Allowed Address | Last Logged In       |
|-------------------------|-------|-----------------|----------------------|
| ... system default user |       |                 |                      |
| admin                   | full  |                 | Jan/02/1970 00:09:08 |

New User

Name: User1

Group: full

Allowed Address: 10.163.1.0/24

8.9.10.11

Last Logged In:

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

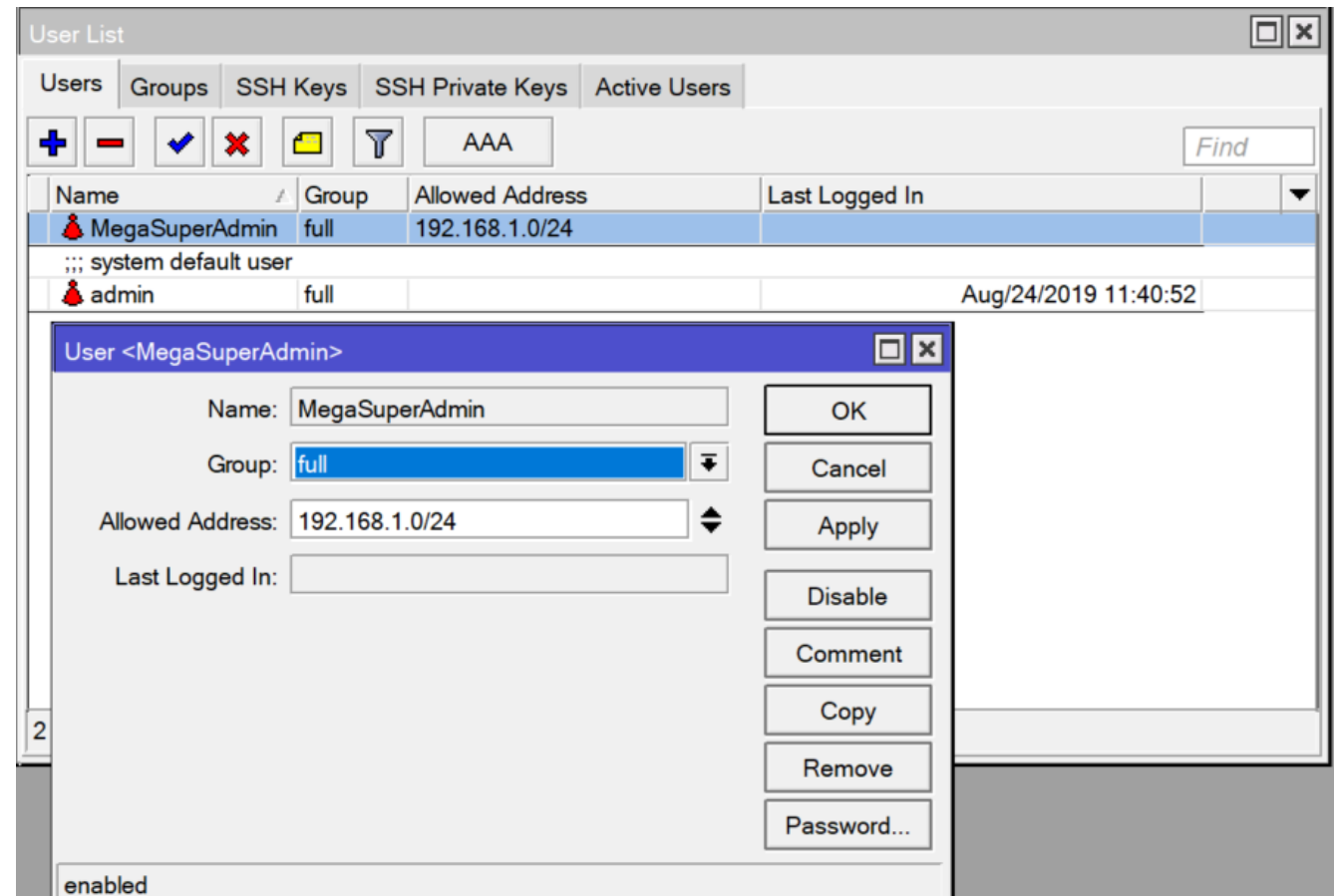
enabled

OK Cancel Apply Disable Comment Copy Remove

1 item

# Recomandări:

- Default user să fie schimbat.
- Creați un user nou cu drepturi **Full**, utilizați acest **user** pentru administrare.





# PASSWORD

- RADIUS MANAGEMENT

- Se setează RADIUS Client

[admin@MikroTik] > radius add address=192.169.100.100 secret=password  
service=login

- Setăm verificarea parolei pe serverul radius

[admin@MikroTik] > user aaa set use-radius=yes accounting=yes default-  
group=full

# PASSWORD

RADIUS Server <172.26.136.17>

General Status

Service: ☐ ppp ☒ login  
☐ hotspot ☐ wireless  
☐ dhcp ☐ ipsec  
☐ dot1x

Called ID:

Domain:

Address: 192.168.100.100

Protocol: udp

Secret: password

Authentication Port: 1812

Accounting Port: 1813

Timeout: 300 ms

☐ Accounting Backup

Realm:

Certificate: none

Src. Address:

User List

Users Groups SSH Keys SSH Private Keys Active Users

+ - ✓ ✗ [icon] AAA

| Name  | Group | Allowed Address | Last Lo |
|-------|-------|-----------------|---------|
| admin | full  |                 |         |

Login Authentication&Accounting

☒ Use RADIUS

☒ Accounting

Interim Update:

Default Group: full

Exclude Groups:

OK Cancel Apply

# Routerul este protejat ?

DA

NU



# ATAC DE TIP BRUTE FORCE

- Cele mai dese tipuri de atacuri asupra parolelor:
  - **BRUTE FORCE** - un atac prin forță brută sau o căutare exhaustivă de cheie reprezintă un atac [criptoanalitic](#), ce poate fi folosit teoretic pentru orice tip de date codificate (cu excepția datelor criptate într-un mod teoretic sigur). Această metodă constă în verificarea sistematică a tuturor [cheilor](#) posibile, până când este găsită cheia corectă.

# UPGRADE

- MAJOR CHANGES IN v6.45.1:

- 
- !) dot1x - added support for IEEE 802.1X Port-Based Network Access Control;
  - !) ike2 - added support for EAP authentication methods (eap-tls, eap-ttls, eap-peap, eap-mschapv2) as initiator;
  - !) security - fixed vulnerabilities CVE-2019-13954, CVE-2019-13955;
  - !) security - fixed vulnerabilities CVE-2019-11477, CVE-2019-11478, CVE-2019-11479;
  - !) security - fixed vulnerability CVE-2019-13074;
  - !) user - removed insecure password storage;

- **CVE-2019-13074** - a vulnerability in the FTP daemon on MikroTik routers through 6.44.3 could allow remote attackers to exhaust all available memory, causing the device to reboot because of uncontrolled resource management.
- **CVE-2019-13954, CVE-2019-13955** - Mikrotik RouterOS before 6.44.5 (long-term release tree) is vulnerable to memory exhaustion. By sending a crafted HTTP request, an authenticated remote attacker can crash the HTTP server and in some circumstances reboot the system. Malicious code cannot be injected.
- **CVE-2019-11477, CVE-2019-11478, CVE-2019-11479** - CP\_SKB\_CB(skb)->tcp\_gso\_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service.
- Sursa: <https://nvd.nist.gov/vuln/detail/CVE-2019-XXXXX>

File Edit View Search Terminal Help

Autoselected keyboard map en-us

ERROR: CredSSP: Initialize failed, do you have correct kerberos tgt initialized ?

Connection established using SSL.

WARNING: Remote desktop does not support colour depth 24; falling back to 16

root@kali: /usr/share/wordlists# hydra -t 4 -V -f -l root -P rockyou.txt rdp:// 192.168.1.1

hydra v7.6 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

hydra (http://www.thc.org/thc-hydra) starting at 2017-02-22 19:11:16

WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...

DATA] 4 tasks, 1 server, 14344399 login tries (l:l/p:14344399), ~3586099 tries per task

DATA] attacking service rdp on port 3389

ATTEMPT] target : 192.168.1.1 login "root" - pass "123456" - 1 of 14344399 [child 0]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "12345" - 2 of 14344399 [child 1]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "123456789" - 3 of 14344399 [child 2]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "password" - 4 of 14344399 [child 3]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "iloveyou" - 5 of 14344399 [child 0]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "princess" - 6 of 14344399 [child 3]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "1234567" - 7 of 14344399 [child 1]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "rockyou" - 8 of 14344399 [child 2]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "12345678" - 9 of 14344399 [child 1]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "abc123" - 10 of 14344399 [child 0]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "nicole" - 11 of 14344399 [child 3]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "daniel" - 12 of 14344399 [child 2]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "babygirl" - 13 of 14344399 [child 1]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "monkey" - 14 of 14344399 [child 0]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "lovely" - 15 of 14344399 [child 3]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "jessica" - 16 of 14344399 [child 2]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "654321" - 17 of 14344399 [child 3]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "michael" - 18 of 14344399 [child 0]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "ashley" - 19 of 14344399 [child 1]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "qwerty" - 20 of 14344399 [child 2]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "111111" - 21 of 14344399 [child 3]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "iloveu" - 22 of 14344399 [child 0]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "000000" - 23 of 14344399 [child 1]  
ATTEMPT] target : 192.168.1.1 login "root" - pass "michelle" - 24 of 14344399 [child 2]



# MIKROTIK SERVICES

- API
- API-SSL
- FTP
- SSH
- TELNET
- WINBOX
- WWW
- WWW-SSL

|   | 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

# METODE DE PROTECȚIE

- **STOP SERVICE**

- API
- API-SSL
- FTP
- SSH
- TELNET
- WINBOX
- WWW
- WWW-SSL

| IP Service List          |                          |                          |                |
|--------------------------|--------------------------|--------------------------|----------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                |
|                          | Name                     | Port                     | Available From |
|                          | api                      | 8728                     |                |
|                          | api-ssl                  | 8729                     |                |
|                          | ftp                      | 21                       |                |
|                          | ssh                      | 22                       |                |
|                          | telnet                   | 23                       |                |
|                          | winbox                   | 8291                     |                |
|                          | www                      | 80                       |                |
| X                        | www-ssl                  | 443                      |                |
| 8 items                  |                          |                          |                |

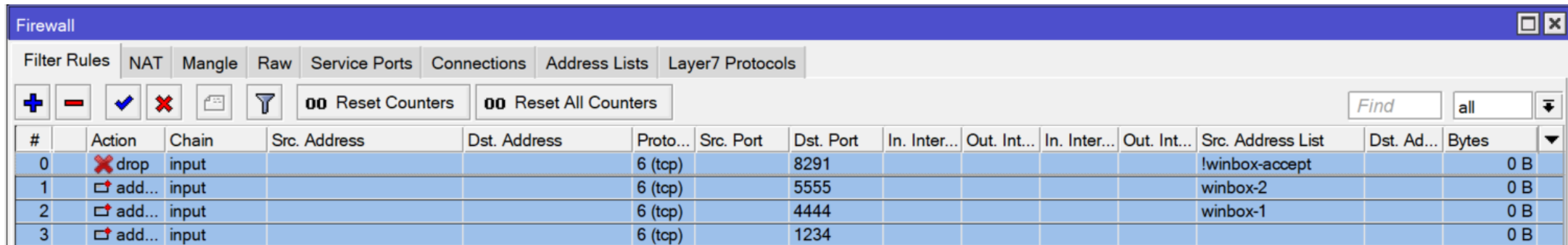
| IP Service List                     |                          |                          |                |
|-------------------------------------|--------------------------|--------------------------|----------------|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |                |
|                                     | Name                     | Port                     | Available From |
| X                                   | api                      | 8728                     |                |
| X                                   | api-ssl                  | 8729                     |                |
| X                                   | ftp                      | 21                       |                |
| X                                   | ssh                      | 22                       |                |
| X                                   | telnet                   | 23                       |                |
|                                     | winbox                   | 8291                     | 10.163.1.0/24  |
| X                                   | www                      | 80                       |                |
| X                                   | www-ssl                  | 443                      |                |
| 8 items (1 selected)                |                          |                          |                |

# Metoda 1 – Blocarea accesării multiple a aceluiași serviciu

- ip firewall filter
- add action=add-src-to-address-list address-list=blacklist address-list-timeout=5d chain=forward connection-state=new disabled=yes dst-address=8.9.10.11 dst-port=22 protocol=tcp src-address=!8.9.10.0/24 src-address-list=ssh\_stage3
- add action=add-src-to-address-list address-list=ssh\_stage3 address-list-timeout=1m chain=forward connection-state=new disabled=yes dst-address= 8.9.10.11 dst-port=22 protocol=tcp src-address-list=ssh\_stage2
- add action=add-src-to-address-list address-list=ssh\_stage2 address-list-timeout=1m chain=forward connection-state=new disabled=yes dst-address=8.9.10.11 dst-port=22 protocol=tcp src-address-list=ssh\_stage1
- add action=add-src-to-address-list address-list=ssh\_stage1 address-list-timeout=1m chain=forward connection-state=new disabled=yes dst-address=8.9.10.11 dst-port=22 protocol=tcp

# Metoda 2 – Port Knocking

- /ip firewall filter
- add action=drop chain=input dst-port=8291 protocol=tcp src-address-list=!winbox-accept
- add action=add-src-to-address-list address-list=winbox-accept address-list-timeout=1d chain=input dst-port=5555 protocol=tcp src-address-list=winbox-2
- add action=add-src-to-address-list address-list=winbox-2 address-list-timeout=1m chain=input dst-port=4444 protocol=tcp src-address-list=winbox-1
- add action=add-src-to-address-list address-list=winbox-1 address-list-timeout=1m chain=input dst-port=1234 protocol=tcp



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is selected. Below the tabs, there are buttons for adding (+), deleting (-), enabling (checkmark), disabling (X), and a filter icon. There are also buttons for 'Reset Counters' and 'Reset All Counters'. A search bar with 'Find' and 'all' is present. The main table lists four filter rules:

| # | Action   | Chain | Src. Address | Dst. Address | Proto... | Src. Port | Dst. Port | In. Inter... | Out. Int... | In. Inter... | Out. Int... | Src. Address List | Dst. Ad... | Bytes |
|---|----------|-------|--------------|--------------|----------|-----------|-----------|--------------|-------------|--------------|-------------|-------------------|------------|-------|
| 0 | ✖ drop   | input |              |              | 6 (tcp)  |           | 8291      |              |             |              |             | !winbox-accept    |            | 0 B   |
| 1 | ➡ add... | input |              |              | 6 (tcp)  |           | 5555      |              |             |              |             | winbox-2          |            | 0 B   |
| 2 | ➡ add... | input |              |              | 6 (tcp)  |           | 4444      |              |             |              |             | winbox-1          |            | 0 B   |
| 3 | ➡ add... | input |              |              | 6 (tcp)  |           | 1234      |              |             |              |             |                   |            | 0 B   |

# RISCURI LAYER 2

## CDP/MNDP Flooding

|        |                 |                   |          |          |       |    |    |          |
|--------|-----------------|-------------------|----------|----------|-------|----|----|----------|
| ether1 | 198.32.27.49    | 56:A5:91:1C:D4:04 | BBBBBPP  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 78.79.242.41    | C6:72:A0:40:0A:7A | KKKK333  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 245.232.253.126 | 02:BA:44:6C:DF:8C | WWEEEEEE | yersinia | 0.8.2 | no | 58 | 00:00:00 |
| ether1 | 56.169.185.35   | 28:CD:DC:07:8D:67 | 1111111  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 138.103.56.27   | A0:19:10:4B:86:13 | UUUU999  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 65.124.76.26    | DA:96:BF:3A:AD:60 | 8LLLLL3  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 183.102.245.57  | 22:DA:A1:4C:06:58 | KKXXXXX  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 210.231.101.116 | 1A:25:14:19:D9:4F | l11111D  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 123.223.107.3   | 52:3D:6E:02:C2:15 | Q99999L  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 180.202.148.2   | 98:BF:33:14:DF:C8 | KYYYYYG  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 219.84.66.125   | C0:02:D7:73:C7:0A | 3333JJ   | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 132.199.163.4   | 86:23:F2:24:2D:BE | EEWWWWW  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 139.226.124.118 | D4:72:E4:4E:74:64 | RR00000  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 174.39.231.24   | CA:5B:E2:4D:79:39 | 4HHHHZZ  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 233.233.49.106  | 02:05:9C:71:2A:1E | BPPPPP8  | yersinia | 0.8.2 | no | 58 | 00:00:00 |
| ether1 | 245.205.211.102 | 8C:6C:D4:0C:C3:EF | KKKXXXX  | yersinia | 0.8.2 | no | 58 | 00:00:00 |
| ether1 | 136.233.31.115  | 84:4F:16:61:B5:D4 | 00MMMMM  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 16.234.90.8     | 56:37:7C:55:76:14 | ZZZHFFF  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 182.69.91.0     | 86:E1:7C:5B:D9:DE | 222FFFF  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 174.224.125.65  | 70:E0:DF:53:B7:12 | 44LLLLL  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 189.244.152.75  | 1E:08:C7:6C:55:09 | YYBBBBB  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 167.159.115.16  | 08:F2:F8:56:B5:82 | 7777JJJ  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 155.81.185.81   | BC:8E:69:5B:6C:10 | 333KKKK  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 109.85.64.99    | 20:23:76:37:36:57 | N66666J  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 102.172.95.95   | FA:CC:66:1F:BC:22 | 8KKKKK3  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 231.33.171.102  | 5A:2A:19:5A:B2:37 | FFFXXXX  | yersinia | 0.8.2 | no | 57 | 00:00:00 |
| ether1 | 128.24.147.104  | FE:1C:39:41:9A:CE | S0000NN  | yersinia | 0.8.2 | no | 57 | 00:00:00 |










1025 items (1 selected)

www.academia-mikrotik.ro

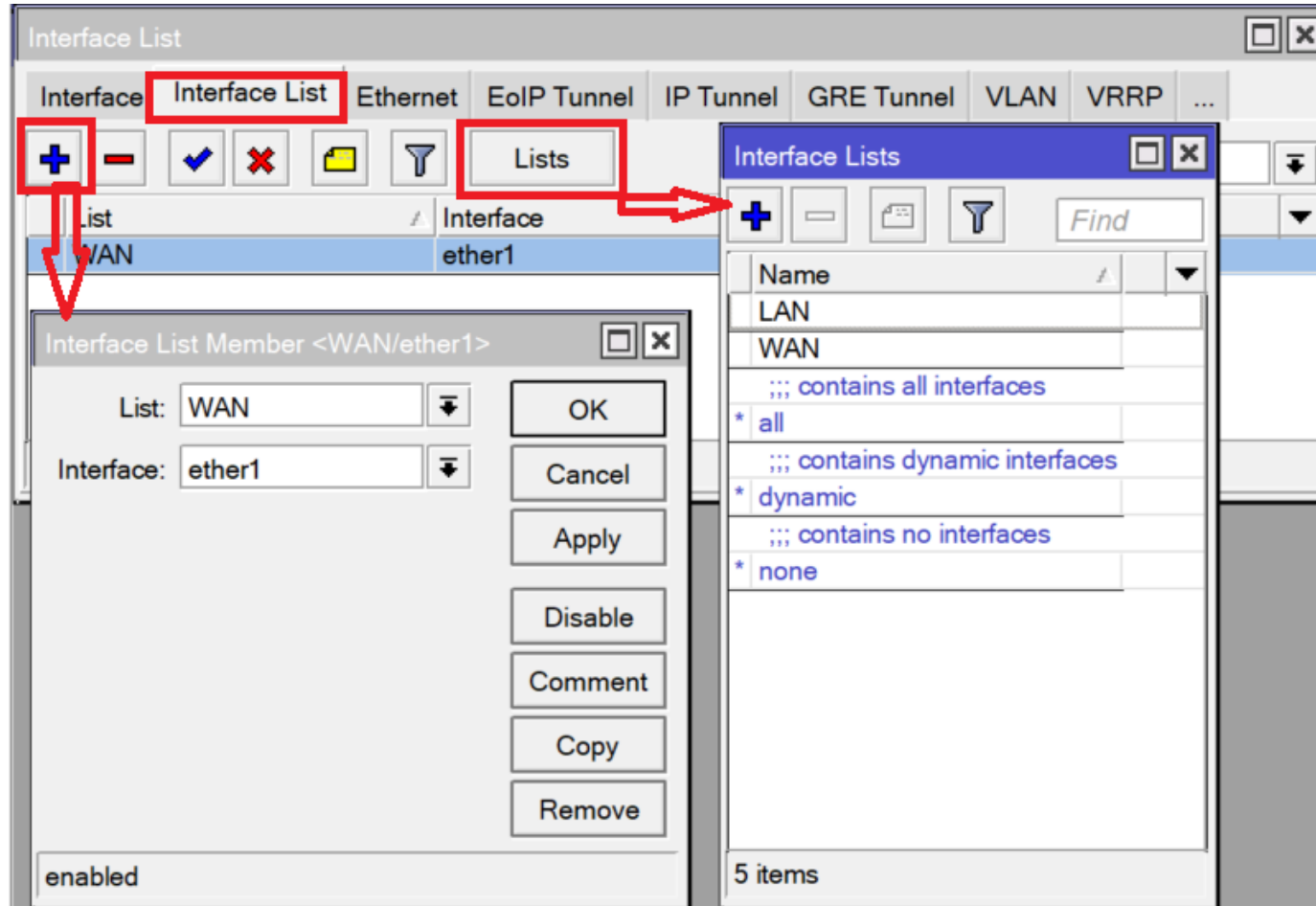
# RISCURI LAYER 2

## /ip neighbors

- Creează invizibilitate:

| Neighbor List  |                 |                    |             |          |                      |                 |      |         |
|--|-----------------|--------------------|-------------|----------|----------------------|-----------------|------|---------|
|         |                 | Discovery Settings |             |          |                      |                 |      | Find    |
| Interface  | IP Address      | MAC Address        | Identity    | Platform | Version              | Board Name      | IPv6 | Age (s) |
|  ether1 | 109.185.131.196 | 74:4D:28:A0:79:A9  | Ab          | MikroTik | 6.46beta16 (testing) | RB4011iGS+      | no   | 5       |
|  ether1 | 109.185.131.196 | 4C:5E:0C:C7:FC:A0  | MikroTik    | MikroTik | 6.43 (stable)        | RB2011UiAS-2HnD | no   | 53      |
|  ether1 | 109.185.131.196 | 64:D1:54:63:A3:86  | CORE        | MikroTik | 6.44.2 (stable)      | RB2011UiAS-2HnD | no   | 50      |
|  ether1 | 109.185.131.196 | 4C:5E:0C:6A:B3:E6  | Encore_N3   | MikroTik | 6.45.1 (stable)      | RB951Ui-2HnD    | no   | 46      |
|  ether1 | 109.185.131.196 | D4:CA:6D:36:EB:69  | Chisinau, G | MikroTik | 6.44 (stable)        | RB750           | no   | 45      |
|  ether1 | 109.185.131.196 | E4:8D:8C:D5:6E:A0  | Chisinau Hr | MikroTik | 6.44 (stable)        | RB750r2         | no   | 4       |
|  ether1 | 109.185.131.196 | D4:CA:6D:38:A1:3B  | G           | MikroTik | 6.44 (stable)        | RB750           | no   | 43      |
|  ether2 | 192.168.15.28   | CC:2D:E0:66:EC:9B  | Hall        | MikroTik | 6.45.3 (stable)      | RBwsAP5Hac2nD   | yes  | 52      |
| 8 items  |                 |                    |             |          |                      |                 |      |         |

# IP NEIGHBOURS





# /IP NEIGHBOURS

The screenshot displays two windows from the Mikrotik WinBox interface. The top window, titled "Interface List", has tabs for "Interface", "Interface List", "Ethernet", "EoIP Tunnel", "IP Tunnel", "GRE Tunnel", "VLAN", "VRRP", and "Bonding". The "Interface List" tab is active, showing a table with two columns: "List" and "Interface". The table contains three entries: "LAN" on "ether2", "LAN" on "ether3", and "WAN" on "ether1". A red box highlights the first two rows. The bottom window, titled "Neighbor List", has a "Discovery Settings" button and a "Find" search bar. It displays a table with columns: "Interface", "IP Address", "MAC Address", "Identity", "Platform", "Version", and "Board". A single entry is shown for "ether2" with IP "192.168.163.253", MAC "CC:2D:E0:66:EC:9B", Identity "Hall", Platform "MikroTik", Version "6.45.3 (stable)", and Board "RBwsAP5". A red box highlights this entry.

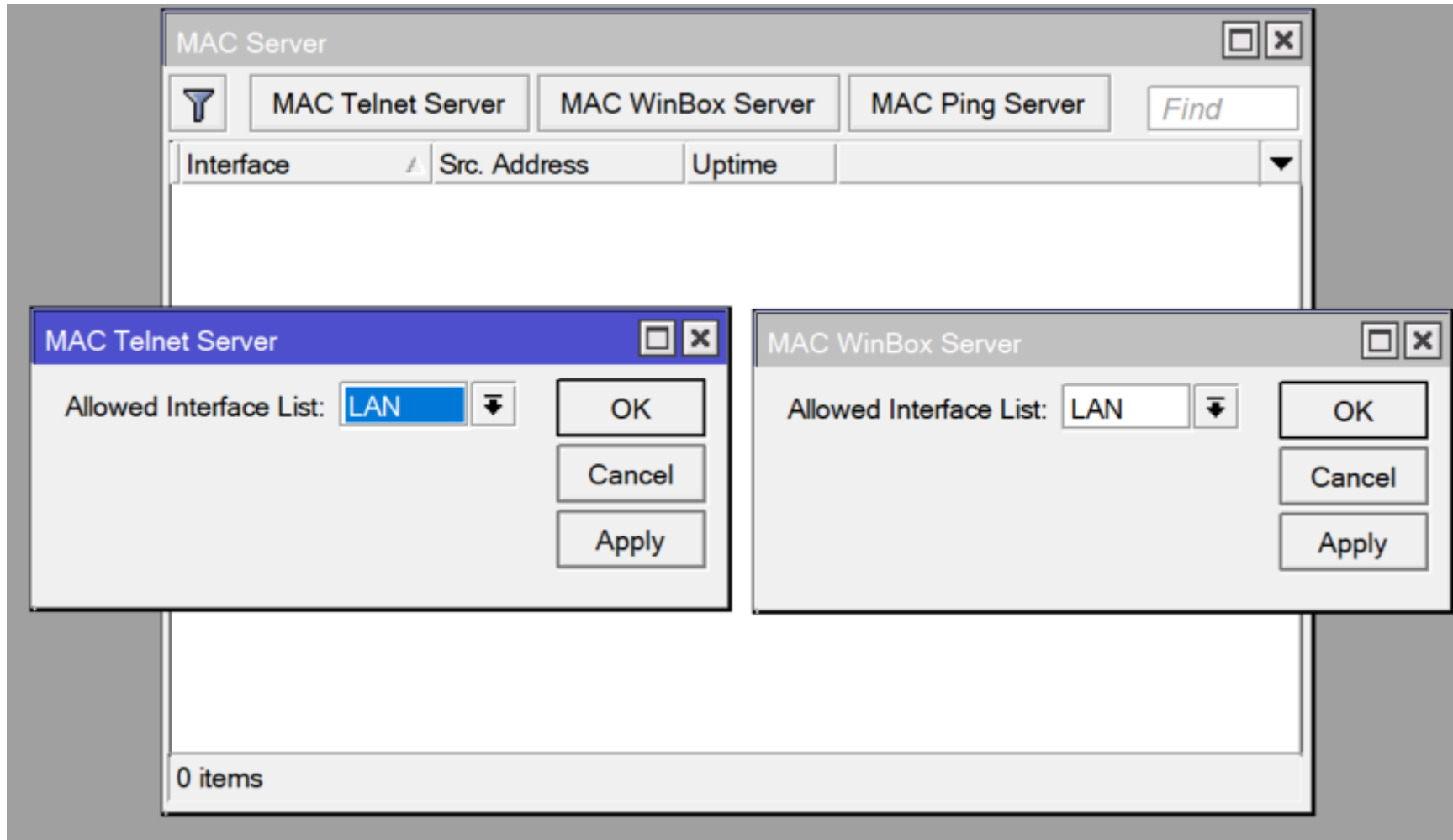
| List | Interface |
|------|-----------|
| LAN  | ether2    |
| LAN  | ether3    |
| WAN  | ether1    |

| Interface | IP Address      | MAC Address       | Identity | Platform | Version         | Board   |
|-----------|-----------------|-------------------|----------|----------|-----------------|---------|
| ether2    | 192.168.163.253 | CC:2D:E0:66:EC:9B | Hall     | MikroTik | 6.45.3 (stable) | RBwsAP5 |



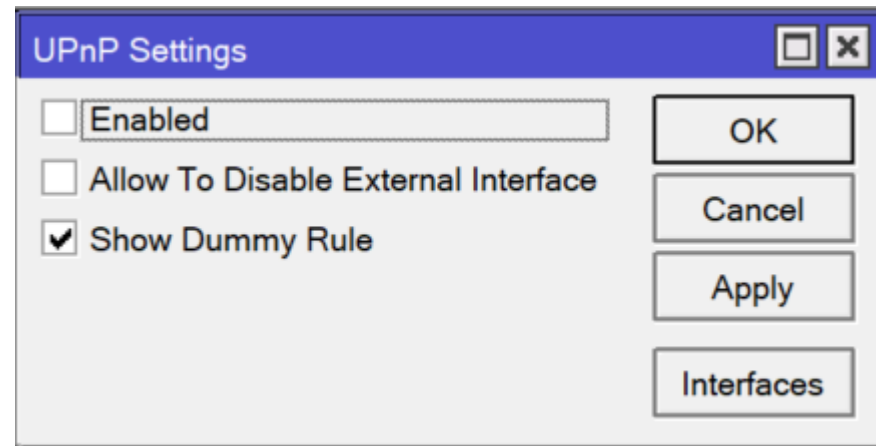
# MAC Server / MAC – TELNET și MAC - WINBOX



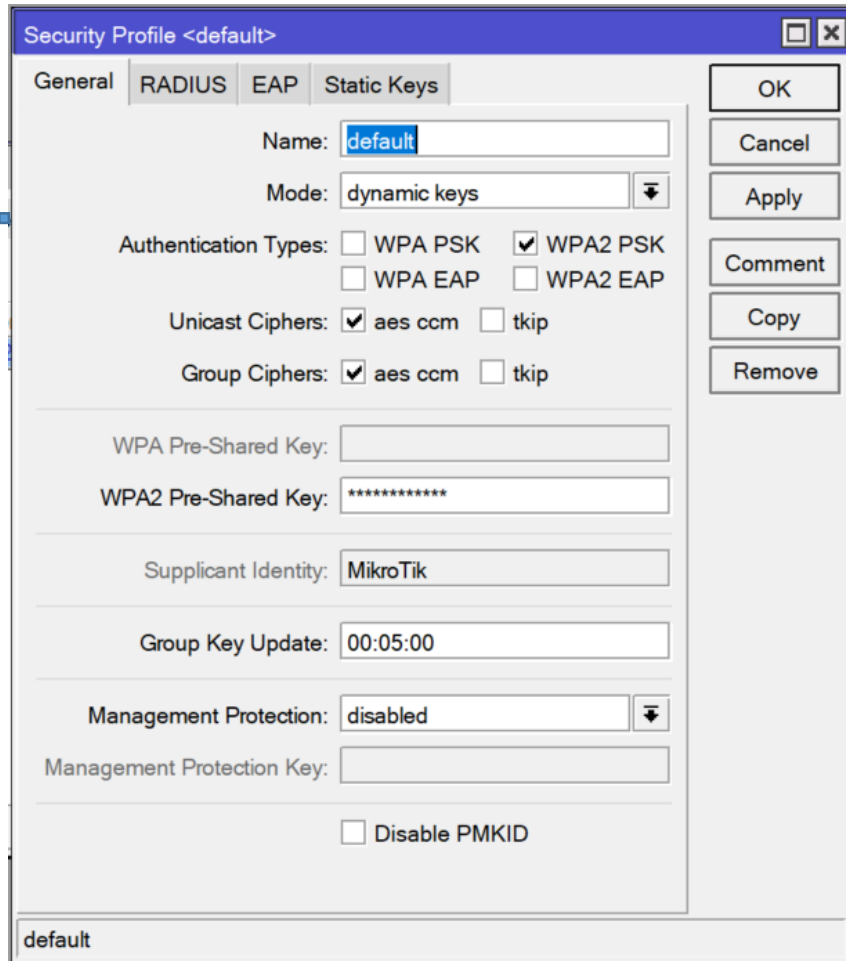
# UPnP

- UPnP – set de protocoale care permite router-ului, de a seta comenzi pentru configurarea automată a anumitor servicii sub necesitățile unei aplicații. La activarea UPnP, nu se ai poate integral de administrat routerul conform necesităților. Dezactivați UPnP.

- /ip upnp



# Wireless Security



The screenshot shows the 'Security Profile <default>' configuration window. The 'General' tab is selected. The 'Name' field is 'default'. The 'Mode' is set to 'dynamic keys'. Under 'Authentication Types', 'WPA2 PSK' is checked. Under 'Unicast Ciphers', 'aes ccm' is checked. Under 'Group Ciphers', 'aes ccm' is checked. The 'WPA Pre-Shared Key' field is empty. The 'WPA2 Pre-Shared Key' field contains '\*\*\*\*\*'. The 'Supplicant Identity' is 'MikroTik'. The 'Group Key Update' is '00:05:00'. The 'Management Protection' is 'disabled'. The 'Management Protection Key' field is empty. There is a checkbox for 'Disable PMKID' which is unchecked. On the right side of the window, there are buttons for 'OK', 'Cancel', 'Apply', 'Comment', 'Copy', and 'Remove'.

- Utilizați doar protocoale sigure: WPA2+AES
- Nu distribuiți parola oaspeților (Creați profil (SSID) pentru oaspeți.)

# VIRTUAL AP

- Interziceți trafic Layer2 între clienții conectați la același AP.
- Interziceți MNDP/CDP pe interfața wlan3 (guest)
- Activați Reply-Only pe interfața wlan3.
- Tabela ARP se va completa din DHCP

Interface <wlan3>

General Wireless WDS Status Traffic

Mode: ap bridge

Secondary Channel:

SSID: Guest

Master Interface: wlan1

Security Profile: guest

WPS Mode: disabled

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

☒ Default Authenticate

☐ Default Forward

☐ Hide SSID

Wireless Tables

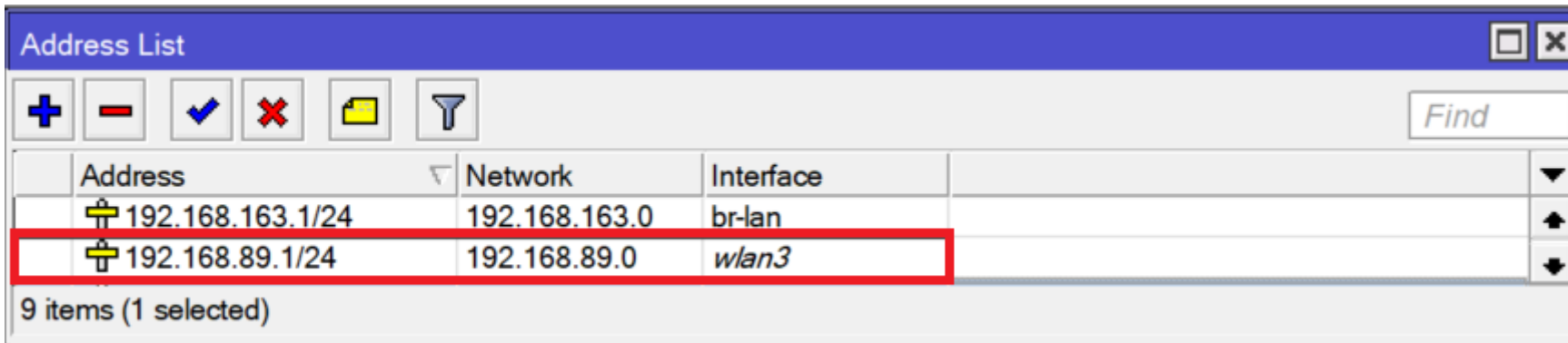
|    | Name  | Type     |
|----|-------|----------|
| RS | wlan1 | Wireless |
|    | wlan3 | Virtual  |
| S  | wlan2 | Wireless |

3 items out of 18 (1 selected)

enabled running

# DHCP MANAGEMENT

- Folosiți managementul adreselor IP
- Interziceți setarea adreselor IP manual



| Address          | Network       | Interface |
|------------------|---------------|-----------|
| 192.168.163.1/24 | 192.168.163.0 | br-lan    |
| 192.168.89.1/24  | 192.168.89.0  | wlan3     |

9 items (1 selected)

# DHCP MANAGEMENT

**DHCP Server <dhcp3>**

Generic Queues Script

Name:

Interface:  ▼

Relay:  ▼

Lease Time:

Bootp Lease Time:  ▼

Address Pool:  ▼

DHCP Option Set:  ▼

---

Src. Address:  ▼

Delay Threshold:  ▼

Src. Address:  ▼

Delay Threshold:  ▼

---

Authoritative:  ▼

Bootp Support:  ▼

Client MAC Limit:  ▼

Use RADIUS:  ▼

---

☐ Always Broadcast

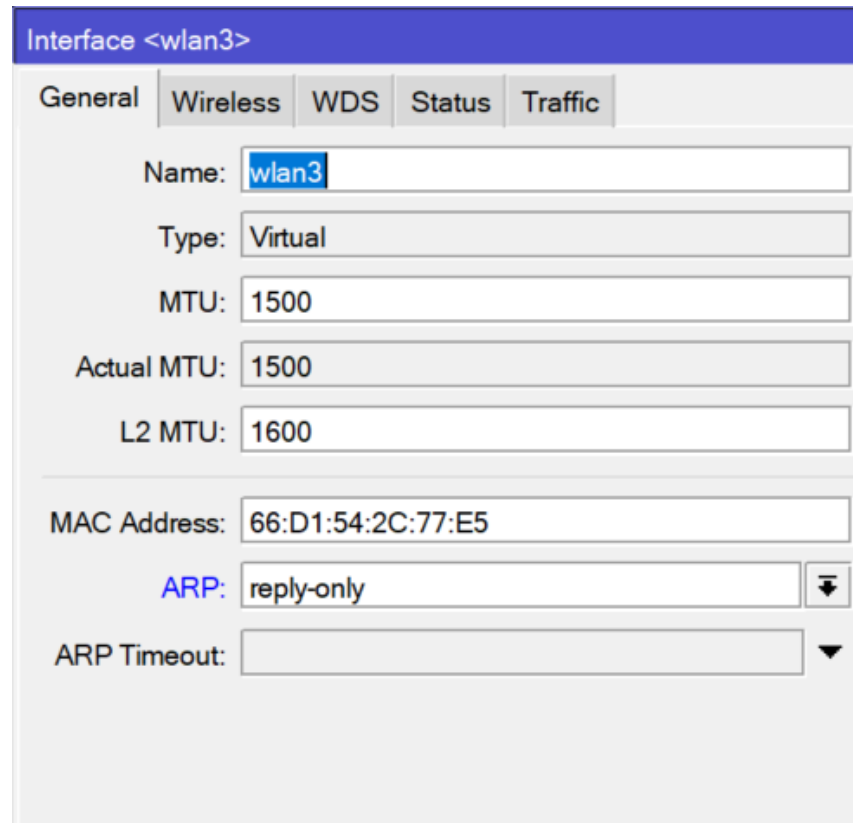
☒ [Add ARP For Leases](#)

☒ Use Framed As Classless

☒ Conflict Detection

# ARP REPLY-ONLY

- Răspunde doar cererilor ce vin de la perechile de IP/MAC listate în tabela ARP



Interface <wlan3>

General | Wireless | WDS | Status | Traffic

Name: wlan3

Type: Virtual

MTU: 1500

Actual MTU: 1500

L2 MTU: 1600

MAC Address: 66:D1:54:2C:77:E5

ARP: reply-only

ARP Timeout:

# IZOLAREA REȚELEI WIRELESS GUEST

- Metoda 1 – Firewall. Neajunsuri – consumă resursele routerului.
- Metoda 2 – Routing.

Route List

Routes Nextops **Rules** VRF

**+**

| #                | Src. Address    | Dst. Address    | Routing Mark | Interface | Action      | Table |
|------------------|-----------------|-----------------|--------------|-----------|-------------|-------|
| ::: Guest to LAN |                 |                 |              |           |             |       |
| 0                | 192.168.89.0/24 | 192.168.88.0/24 |              |           | unreachable | main  |
| 1                | 192.168.88.0/24 | 192.168.89.0/24 |              |           | unreachable | main  |

Policy Routing Rule <>

Src. Address: 192.168.88.0/24

Dst. Address: 192.168.89.0/24

Routing Mark:

Interface:

Action: unreachable

Table: main

OK Cancel Apply Disable Comment Copy Remove

enabled

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

**+**

| # | Action | Chain   | Src. Address    | Dst. Address  | Proto... | Src. Port | Dst. Port | In. In |
|---|--------|---------|-----------------|---------------|----------|-----------|-----------|--------|
| 0 | drop   | forward | 192.168.89.0/24 | 192.168.88... |          |           |           |        |

Firewall Rule <192.168.89.0/24->192.168.88.0/24>

General Advanced Extra Action Statistics

Chain: forward

Src. Address: 192.168.89.0/24

Dst. Address: 192.168.88.0/24

OK Cancel Apply Disable



**FlashStart®**  
INTERNET PROTECTION

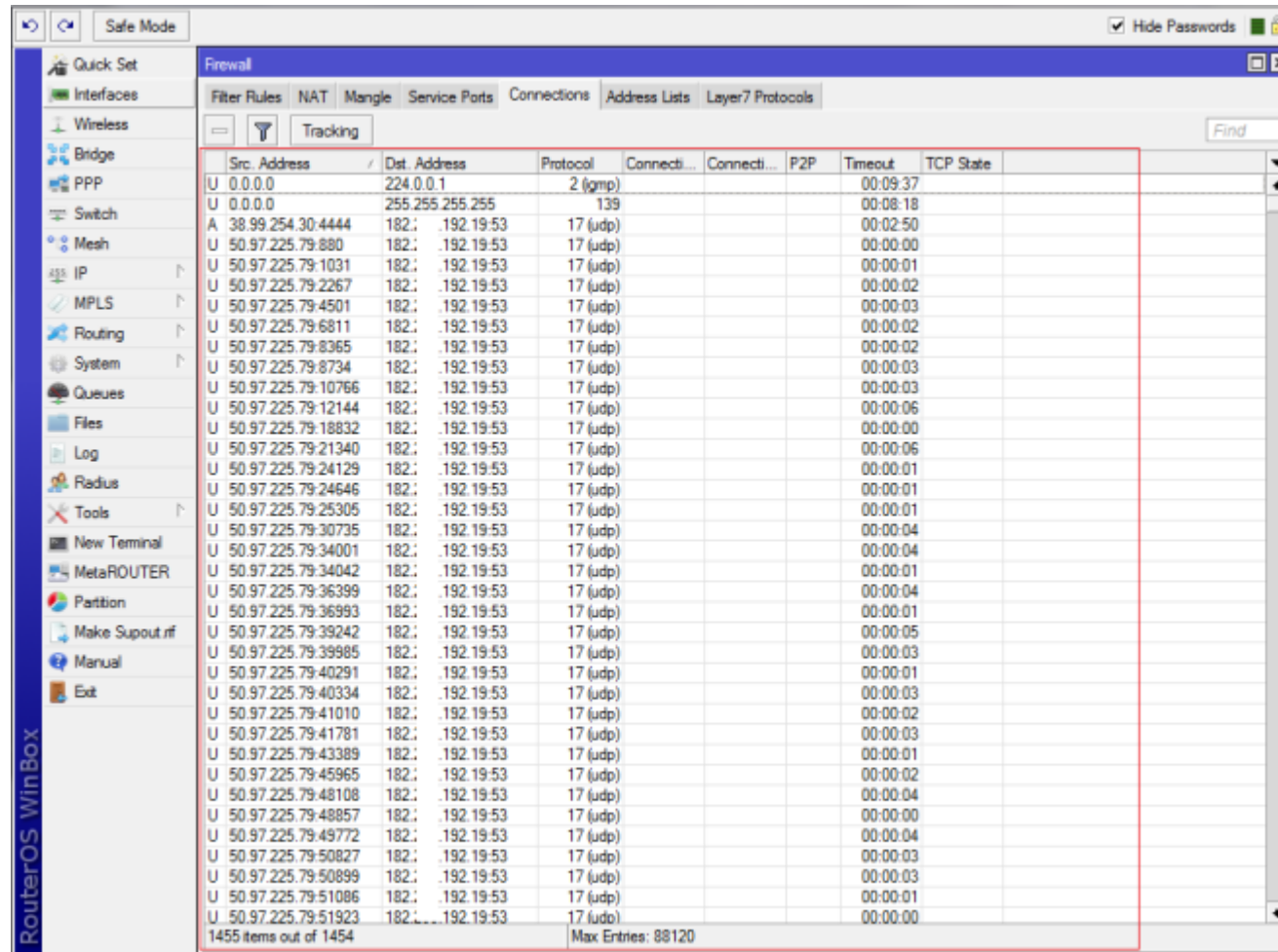


The malware  
& content **filter**

# DNS REBINDING

- Utilizarea serviciilor aditionale pentru filtrarea traficului în baza cererilor DNS.
- Setări necesare pentru redirectionarea traficului.
- `/ip dns set servers=server.flashstart.com allow-remote-request=yes`
- `/ip firewall nat add chain=dstnat protocol=udp dst-port=53 action=redirect to-ports=53`

# DNS REBINDING



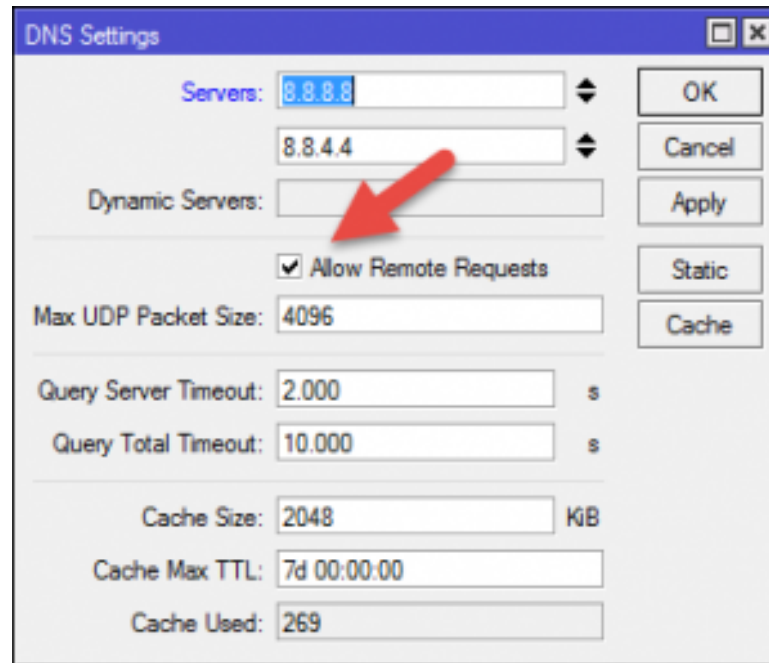
The screenshot shows the Mikrotik WinBox interface with the Firewall Connections tab selected. The table displays a list of active connections, including source and destination addresses, protocols, connection counts, and timeouts. The connections are primarily UDP traffic to 192.19.53, which is typical for DNS rebinding attacks.

| Src. Address         | / | Dst. Address    | Protocol | Connecti... | Connecti... | P2P | Timeout  | TCP State |
|----------------------|---|-----------------|----------|-------------|-------------|-----|----------|-----------|
| U 0.0.0.0            | / | 224.0.0.1       | 2 (icmp) |             |             |     | 00:09:37 |           |
| U 0.0.0.0            | / | 255.255.255.255 | 139      |             |             |     | 00:08:18 |           |
| A 38.99.254.30.4444  | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:02:50 |           |
| U 50.97.225.79.880   | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:00 |           |
| U 50.97.225.79.1031  | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:01 |           |
| U 50.97.225.79.2267  | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:02 |           |
| U 50.97.225.79.4501  | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:03 |           |
| U 50.97.225.79.6811  | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:02 |           |
| U 50.97.225.79.8365  | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:02 |           |
| U 50.97.225.79.8734  | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:03 |           |
| U 50.97.225.79.10766 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:03 |           |
| U 50.97.225.79.12144 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:06 |           |
| U 50.97.225.79.18832 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:00 |           |
| U 50.97.225.79.21340 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:06 |           |
| U 50.97.225.79.24129 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:01 |           |
| U 50.97.225.79.24646 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:01 |           |
| U 50.97.225.79.25305 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:01 |           |
| U 50.97.225.79.30735 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:04 |           |
| U 50.97.225.79.34001 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:04 |           |
| U 50.97.225.79.34042 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:01 |           |
| U 50.97.225.79.36399 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:04 |           |
| U 50.97.225.79.36993 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:01 |           |
| U 50.97.225.79.39242 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:05 |           |
| U 50.97.225.79.39985 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:03 |           |
| U 50.97.225.79.40291 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:01 |           |
| U 50.97.225.79.40334 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:03 |           |
| U 50.97.225.79.41010 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:02 |           |
| U 50.97.225.79.41781 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:03 |           |
| U 50.97.225.79.43389 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:01 |           |
| U 50.97.225.79.45965 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:02 |           |
| U 50.97.225.79.48108 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:04 |           |
| U 50.97.225.79.48857 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:00 |           |
| U 50.97.225.79.49772 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:04 |           |
| U 50.97.225.79.50827 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:03 |           |
| U 50.97.225.79.50899 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:03 |           |
| U 50.97.225.79.51086 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:01 |           |
| U 50.97.225.79.51923 | / | 182.: 192.19.53 | 17 (udp) |             |             |     | 00:00:00 |           |

1455 items out of 1454 Max Entries: 88120

# DNS BINDING

- Dacă este strict necesară folosirea Allow remote request



# DNS BINDING

- > ip firewall filter add chain=input protocol=udp dst-port=53 in-interface-list=WAN action=drop

Firewall Rule <53>

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol: ☐ 17 (udp)

Src. Port:

Dst. Port: ☐ 53

Any. Port:

In. Interface:

Out. Interface:

In. Interface List: ☐ WAN

Out. Interface List:





Primul centru de instruire MikroTik în România. Fondat în 2014

Sediu: Braşov, str. Orizontului 6, tel: +40 364 086 906.

email: [office@academia-mikrotik.ro](mailto:office@academia-mikrotik.ro)

[www.academia-mikrotik.ro](http://www.academia-mikrotik.ro)

D. J. Balbás.