

A woman with blonde hair tied back is sitting at a desk, looking at a laptop. She is holding a small network device (possibly a switch or router) in her left hand, and a cable is plugged into it. The laptop screen displays a network configuration interface. In the foreground, there is a stack of four white network devices (switches or routers) with blue ports. A blue cable is coiled next to them. The background is a plain wall.

TOP10 RouterOS configuration mistakes

Presenter – Andis Arins



2

- MikroTik Consultant at [WISP TRACON](#) / [router.lv](#)
- MikroTik / Microsoft certified trainer
- Member of the board in Latvian Internet Association
- Review expert for EU in future networking research

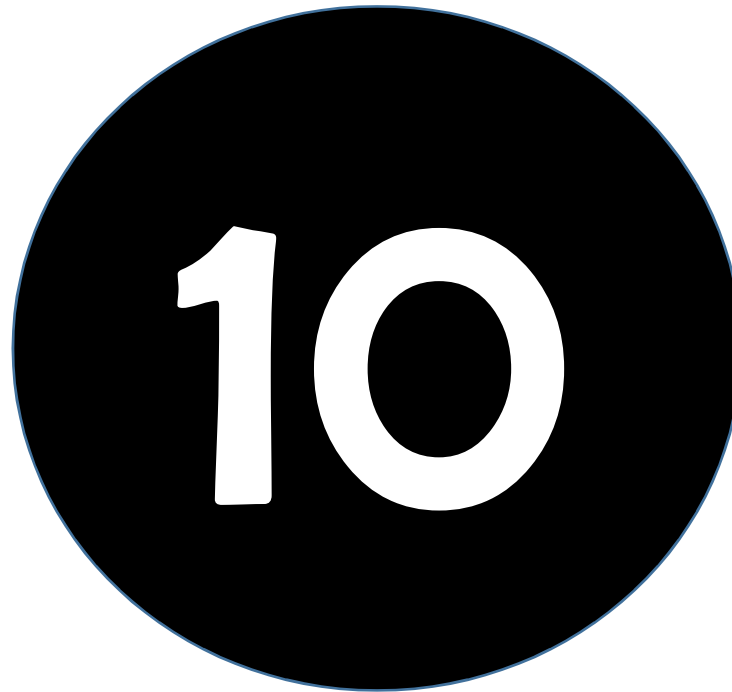
[andis\[at\]router.lv](mailto:andis[at]router.lv)

www.linkedin.com/in/andisarins

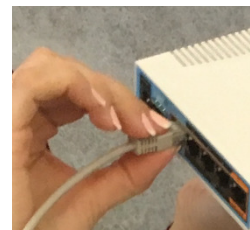
The same IP on multiple interfaces



3



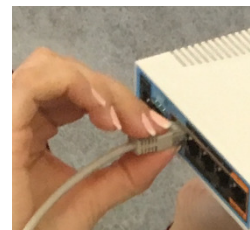
The same IP on multiple interfaces



4

Address List			
			
	Address	Network	Interface
	 10.0.0.1/24	10.0.0.0	ether1
	 10.0.0.1/24	10.0.0.0	ether2

The same IP on multiple interfaces



5

```
[admin@MUM16TX-AA] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS          NETWORK    INTERFACE
0   10.0.0.1/24       10.0.0.0   ether1
1   10.0.0.1/24       10.0.0.0   ether2
[admin@MUM16TX-AA] >
[admin@MUM16TX-AA] >
[admin@MUM16TX-AA] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
#   DST-ADDRESS      PREF-SRC  GATEWAY            DISTANCE
0 ADC 10.0.0.0/24       10.0.0.1   ether1              0
      -              -          ether2
```

survival strategy: MAC telnet or
connection from different network

Lack of monitoring



6



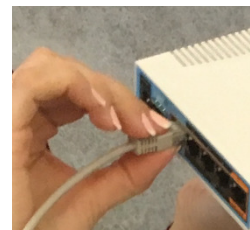
Lack of monitoring



7

- What is the health of my router?
- Is it reachable from everywhere it should?
- Isn't it overloaded ?

Lack of monitoring



8

System Health

Fan Mode:

Use Fan:

Voltage:

CPU Temperature:

Board Temperature:

Board Temperature 2:

Power Consumption:

Active Fan:

Fan Speed:

Fan2 Speed:

Fan3 Speed:

Fan4 Speed:

PSU1 Voltage:

PSU1 Current:

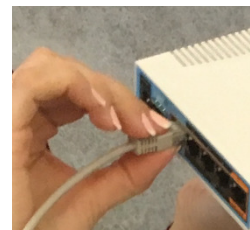
PSU2 Voltage:

PSU2 Current:

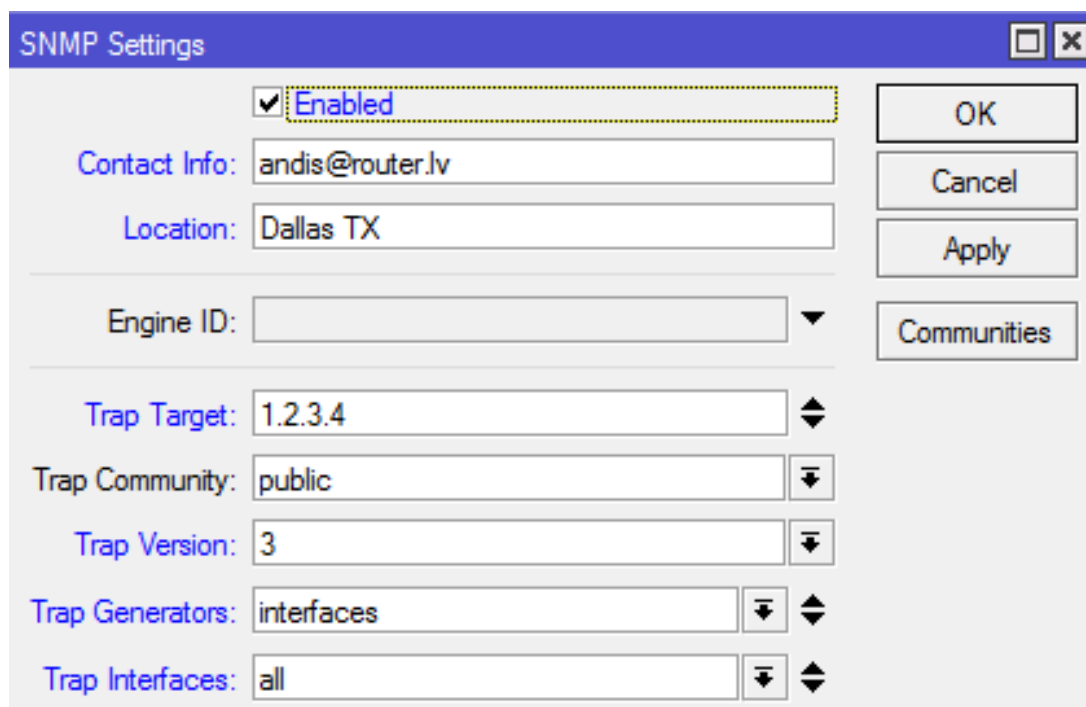
```
[admin@ccr1072] > /system health print
cpu-overtmp-check: yes
cpu-overtmp-threshold: 100C
cpu-overtmp-startup-delay: 1m
cpu-temperature: 39C
power-consumption: 55.2W
board-temperature1: 28C
board-temperature2: 27C
board-temperature3: 32C
psu1-voltage: 12V
psu2-voltage: 0V
psu1-current: 4.6A
psu2-current: 0A
fan1-speed: 4724RPM
fan2-speed: 4518RPM
fan3-speed: 4724RPM
fan4-speed: 4627RPM
```

```
[admin@ccr1072] > /system health print oid
active-fan: .1.3.6.1.4.1.14988.1.1.3.9.0
voltage: .1.3.6.1.4.1.14988.1.1.3.8.0
temperature: .1.3.6.1.4.1.14988.1.1.3.10.0
processor-temperature: .1.3.6.1.4.1.14988.1.1.3.11.0
current: .1.3.6.1.4.1.14988.1.1.3.13.0
power-consumption: .1.3.6.1.4.1.14988.1.1.3.12.0
psu1-state: .1.3.6.1.4.1.14988.1.1.3.15.0
psu2-state: .1.3.6.1.4.1.14988.1.1.3.16.0
```


Lack of monitoring



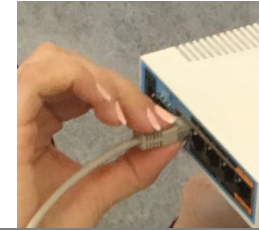
9

A screenshot of a 'SNMP Settings' configuration window. The window has a blue title bar with the text 'SNMP Settings' and standard window controls. The main area contains several fields: 'Contact Info' with the value 'andis@router.lv', 'Location' with 'Dallas TX', 'Engine ID' with a dropdown arrow, 'Trap Target' with '1.2.3.4', 'Trap Community' with 'public', 'Trap Version' with '3', 'Trap Generators' with 'interfaces', and 'Trap Interfaces' with 'all'. On the right side, there are four buttons: 'OK', 'Cancel', 'Apply', and 'Communities'. The 'Enabled' checkbox is checked and highlighted with a yellow dashed border.

IP - SNMP

/snmp> send-trap
for proactive
action

Lack of monitoring

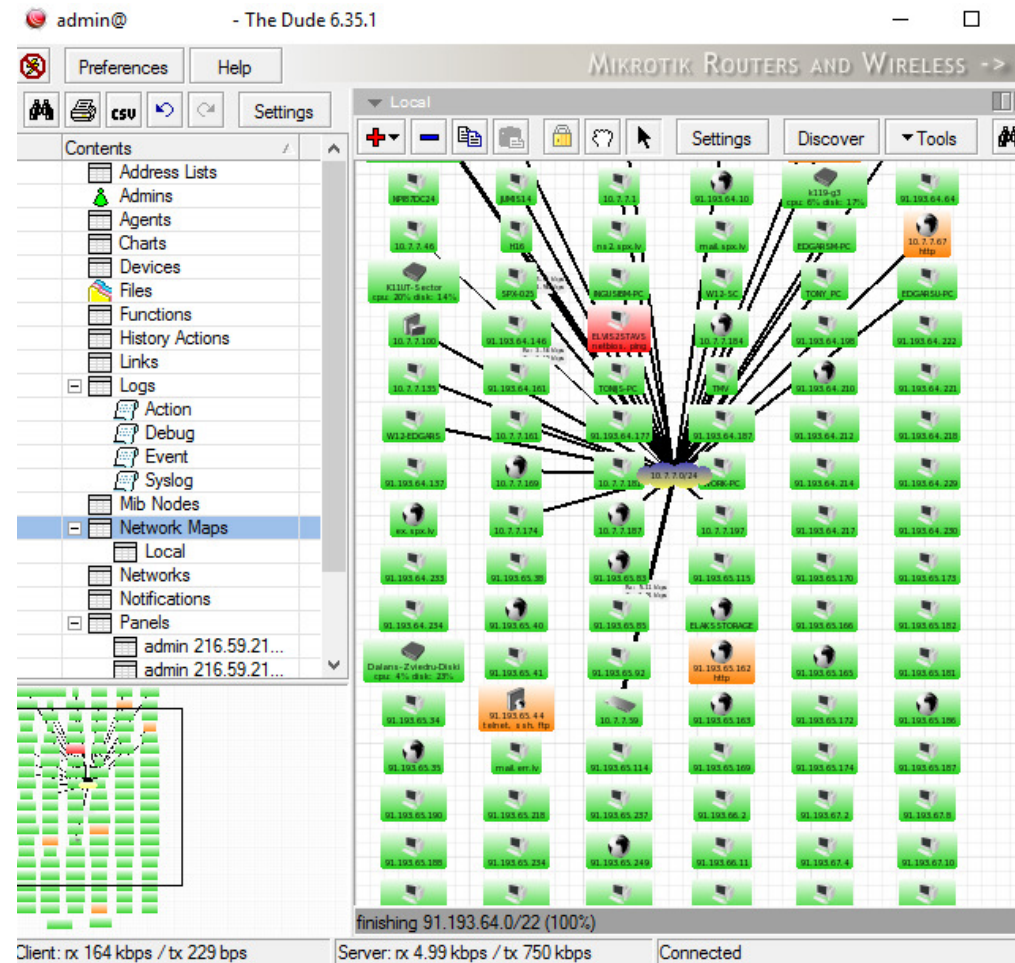


10

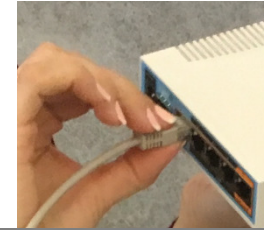
The Dude

you can monitor and
manage your devices

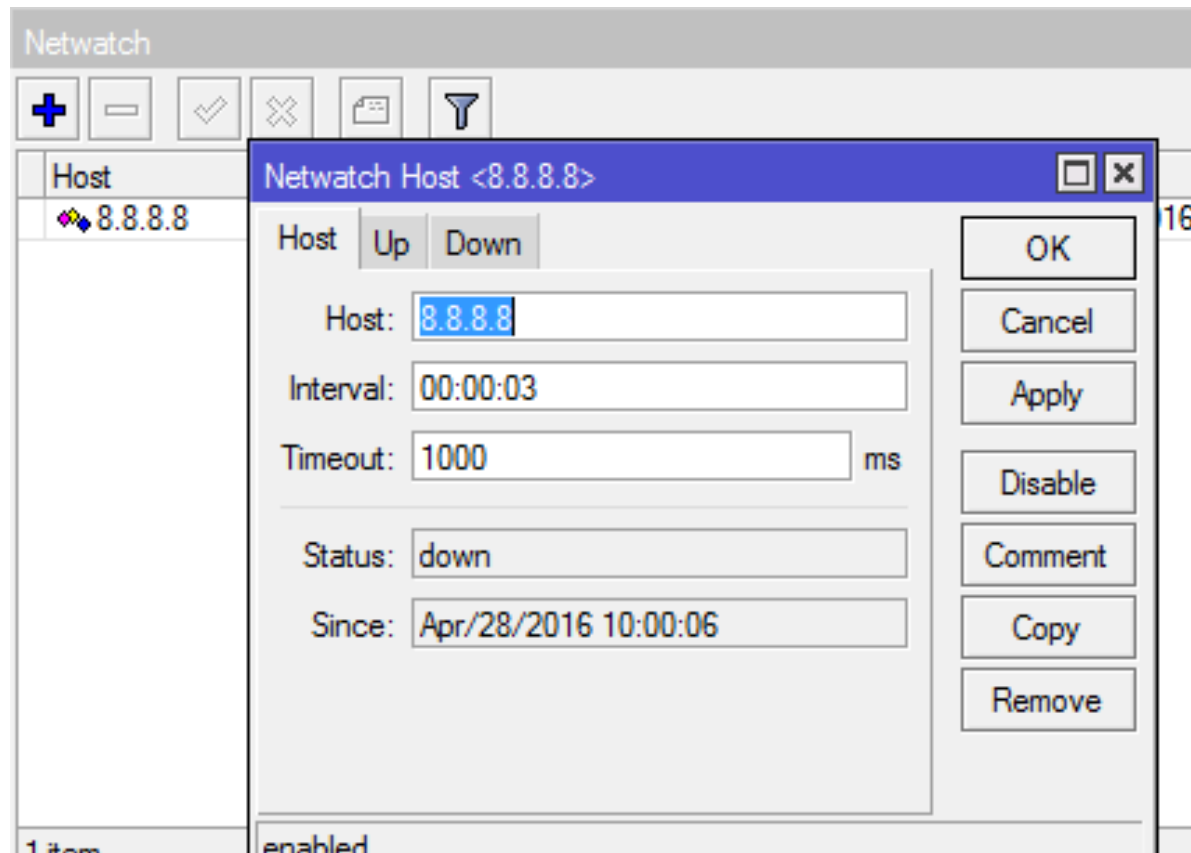
new features since
RouterOS 6.34



Lack of monitoring

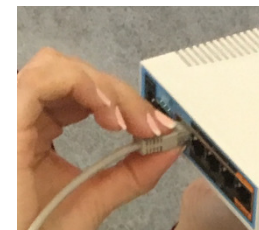


11

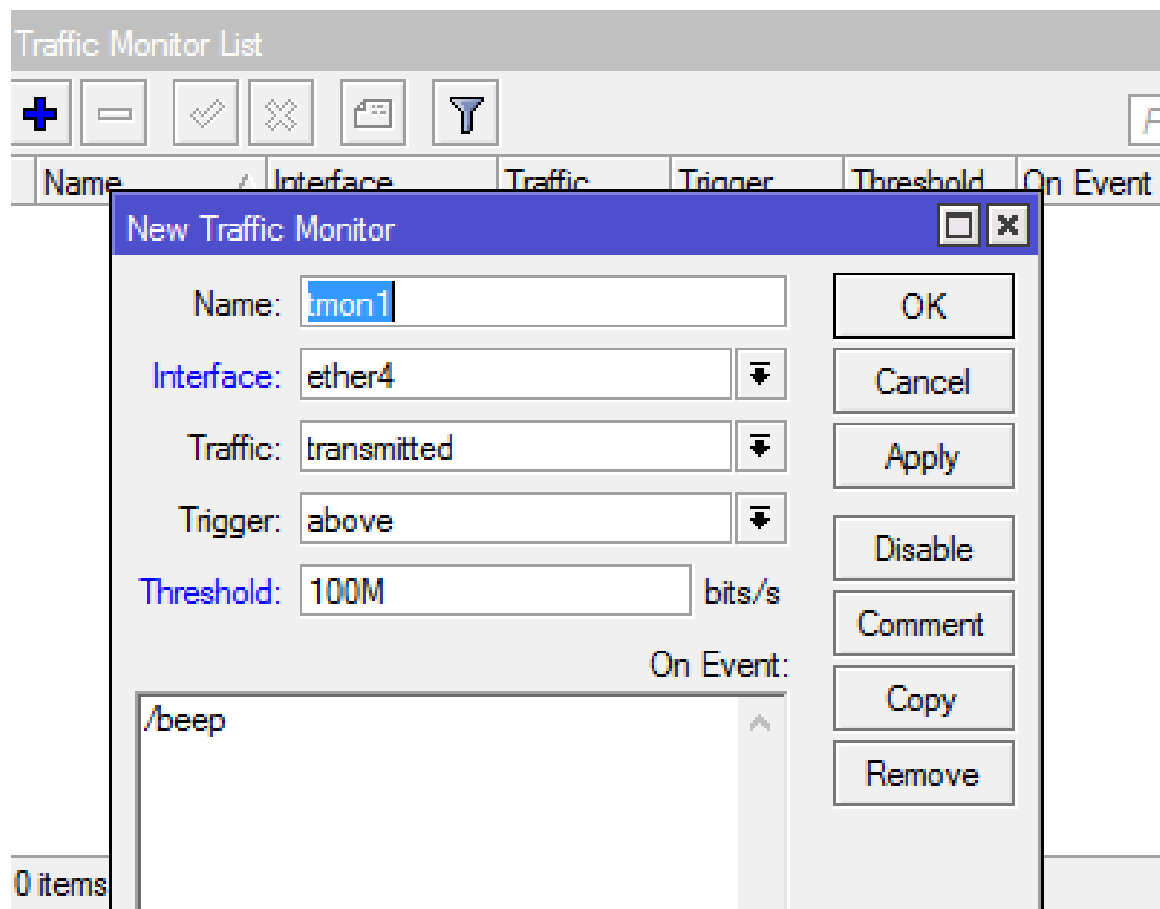


tools-
netwatch

Lack of monitoring

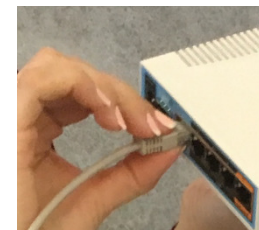


12



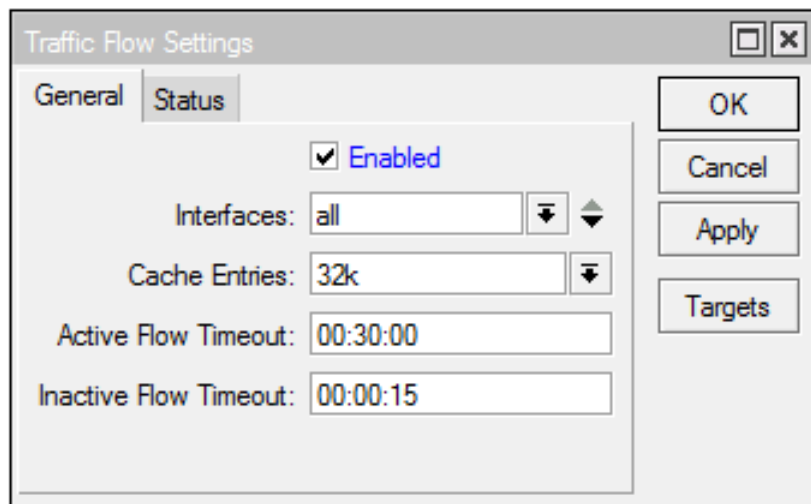
tools-
Traffic monitor

Lack of monitoring



13

IP- Traffic Flow



Traffic Flow Settings

General Status

☒ Enabled

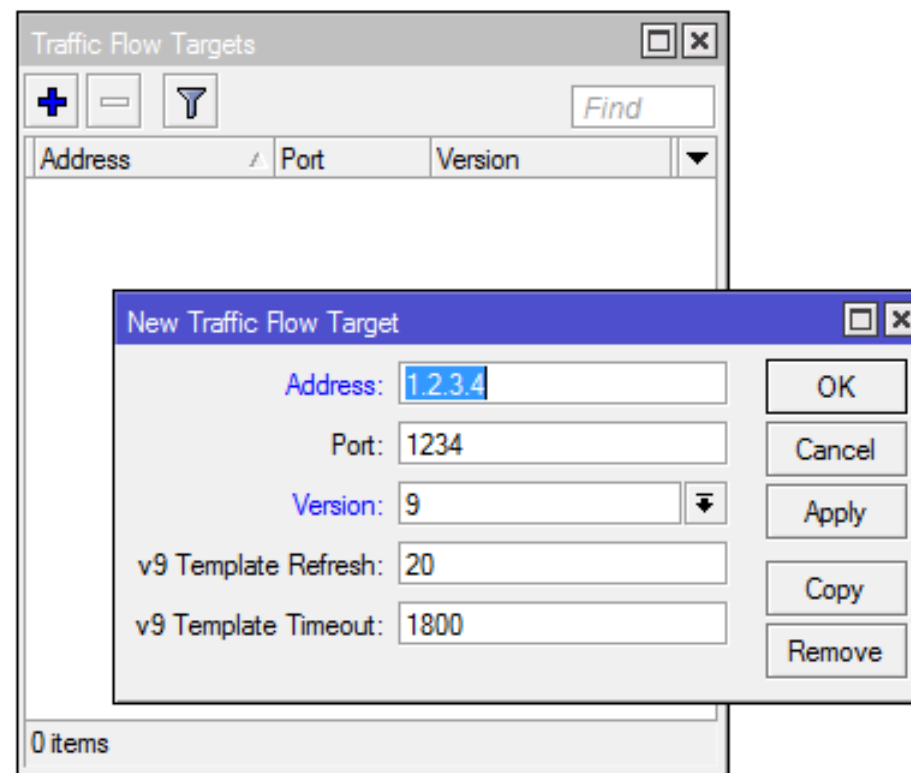
Interfaces: all

Cache Entries: 32k

Active Flow Timeout: 00:30:00

Inactive Flow Timeout: 00:00:15

OK Cancel Apply Targets



Traffic Flow Targets

+ - Y Find

Address	Port	Version
---------	------	---------

0 items

New Traffic Flow Target

Address: 1.2.3.4

Port: 1234

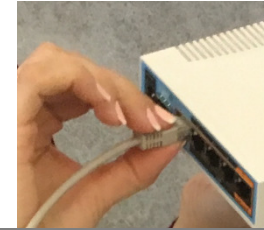
Version: 9

v9 Template Refresh: 20

v9 Template Timeout: 1800

OK Cancel Apply Copy Remove

Lack of monitoring

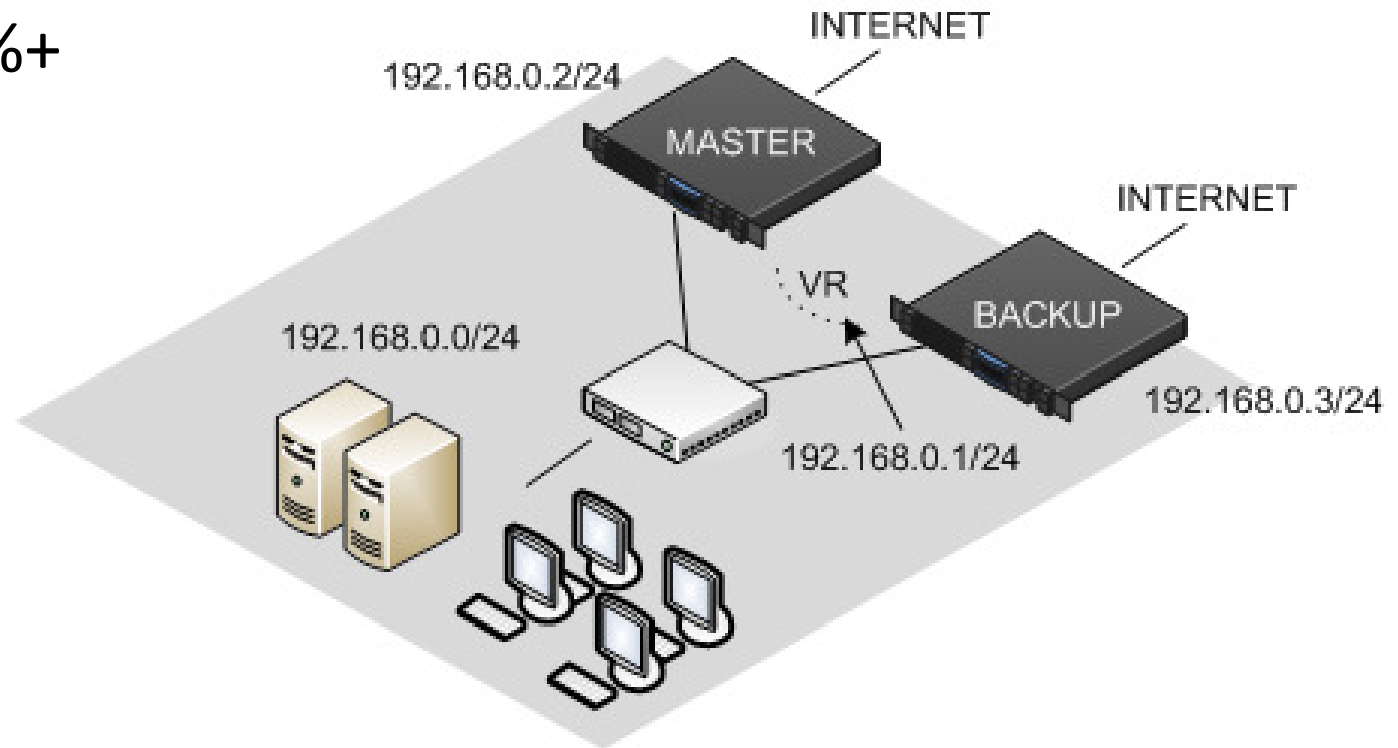


14

Also HA solutions without monitoring may fail one day

VRRP for 99.9%+
availability

0.365 days or
8.76 hours
down in year



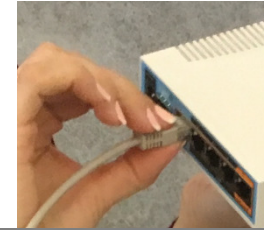
DNS issues



15



DNS issues



16

DNS Settings

Servers: 8.8.8.8

Dynamic Servers:

☒ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

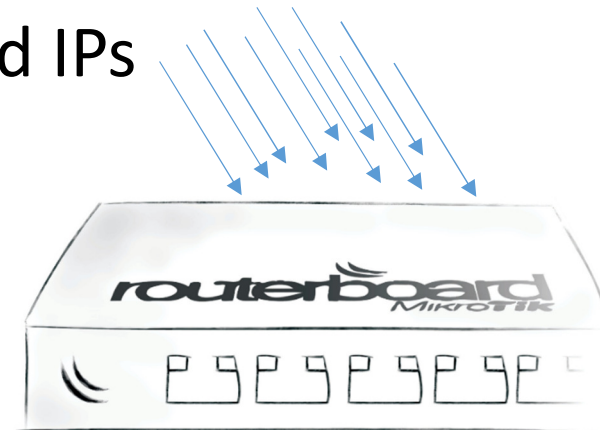
Cache Size: 2048 KB

Cache Max TTL: 7d 00:00:00

Cache Used: 8

OK Cancel Apply Static Cache

Many requests from
spoofed IPs



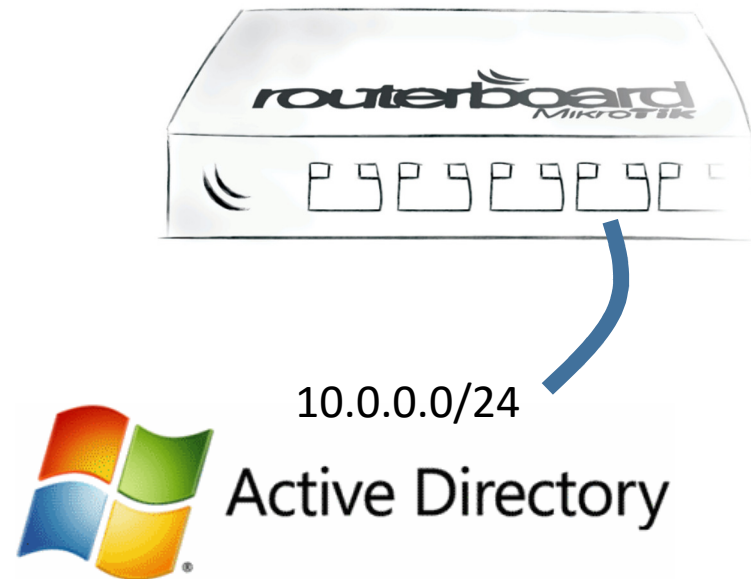
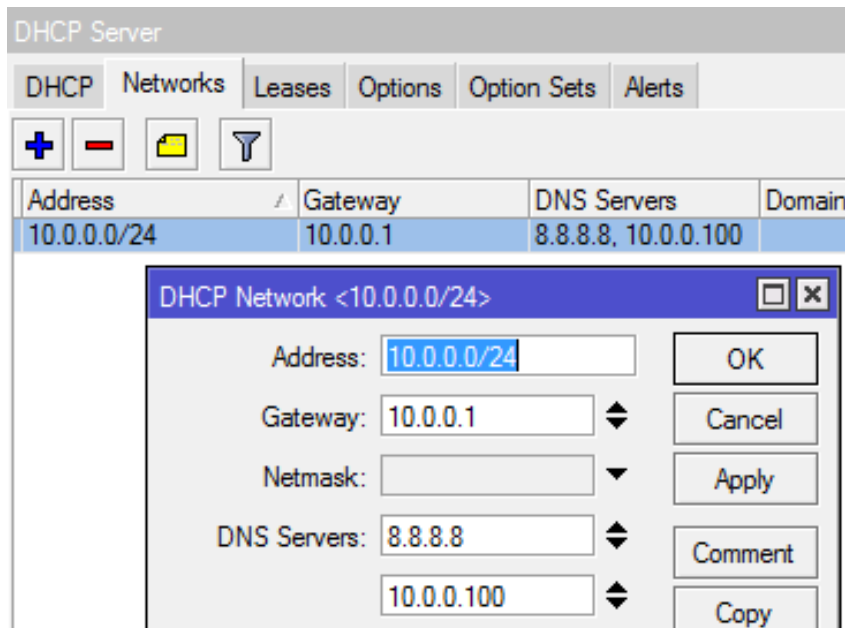
VICTIM

```
#
/ip firewall filter
add action=drop chain=input connection-state=new dst-port=53 in-interface=\
ether1-INTERNET protocol=udp
add action=drop chain=input connection-state=new dst-port=53 in-interface=\
ether1-INTERNET protocol=tcp
```

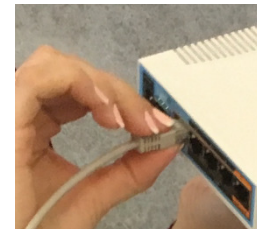
DNS issues



17



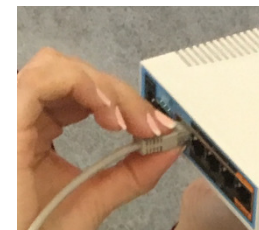
Firewall inefficiency



18



Firewall inefficiency



19

internet



123.123.123.123
webserver

Firewall							
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols							
+ - ✓ ✗ 📁 🔍 00 Reset Counters 00 Reset All Counters Find							
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port
0	✓ acc...	forward	123.123.123.123	0.0.0.0/0			
1	✓ acc...	forward	1.1.1.1	123.123.123.123			
2	✓ acc...	forward	2.2.2.2	123.123.123.123			
3	✓ acc...	forward	3.3.3.3	123.123.123.123			
4	✓ acc...	forward	4.4.4.4	123.123.123.123			
5	✓ acc...	forward	5.5.5.5	123.123.123.123			
6	✓ acc...	forward	6.6.6.6	123.123.123.123			
7	✓ acc...	forward	7.7.7.7	123.123.123.123			
8	✓ acc...	forward	0.0.0.0/0	123.123.123.123	6 (tcp)		80,443
9	✗ drop	forward	0.0.0.0/0	123.123.123.123			

NAT issues



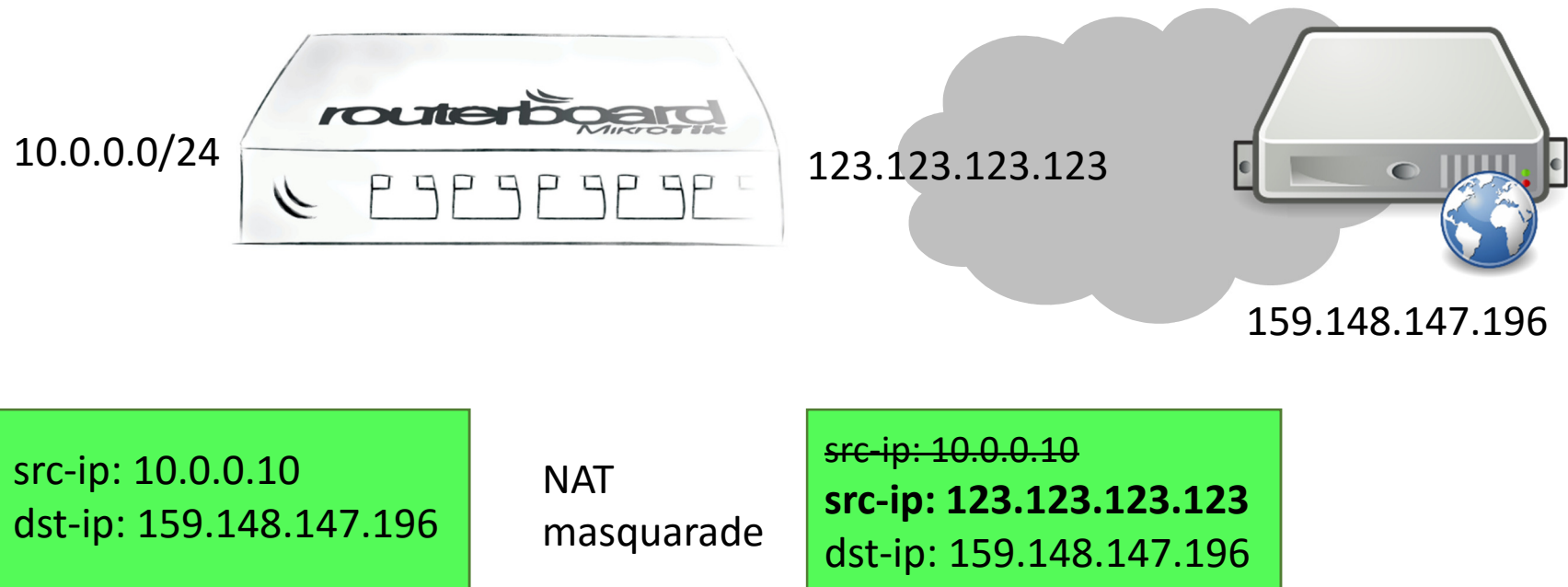
20



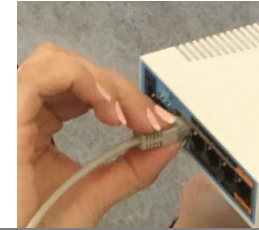
NAT issues



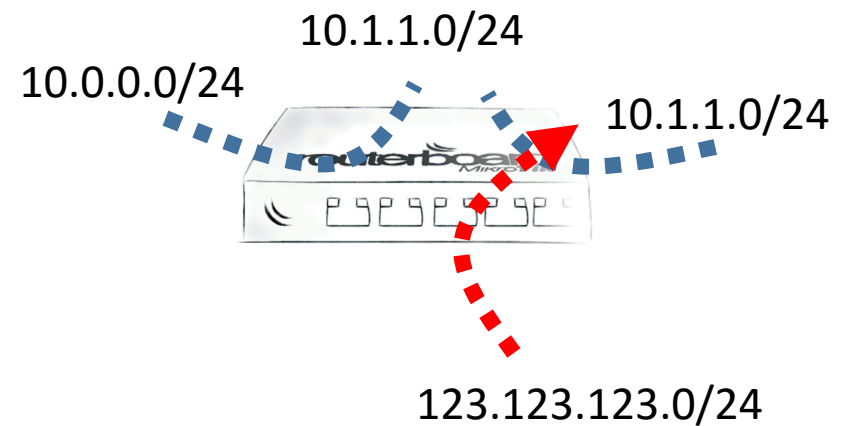
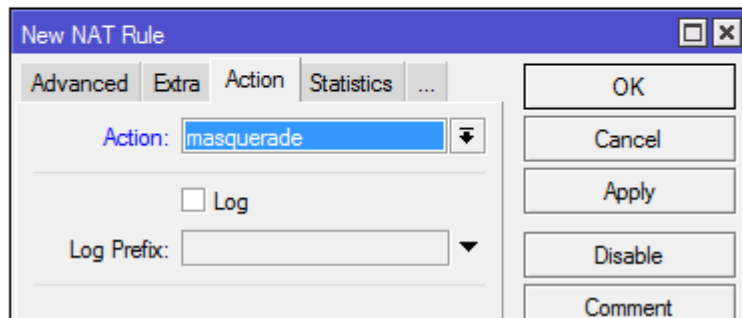
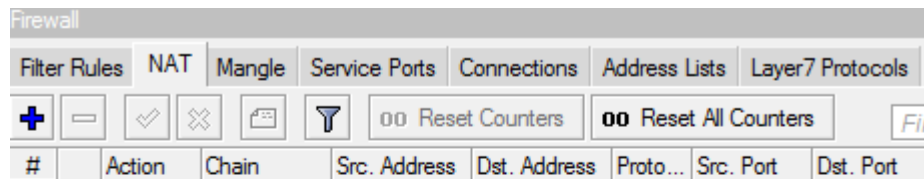
21



NAT issues



22



bad

```
/ip firewall nat
add action=masquerade chain=srcnat
```

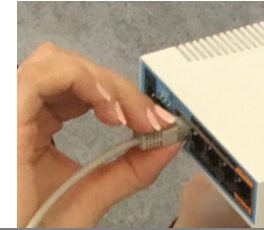
ok

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1-INTERNET
```

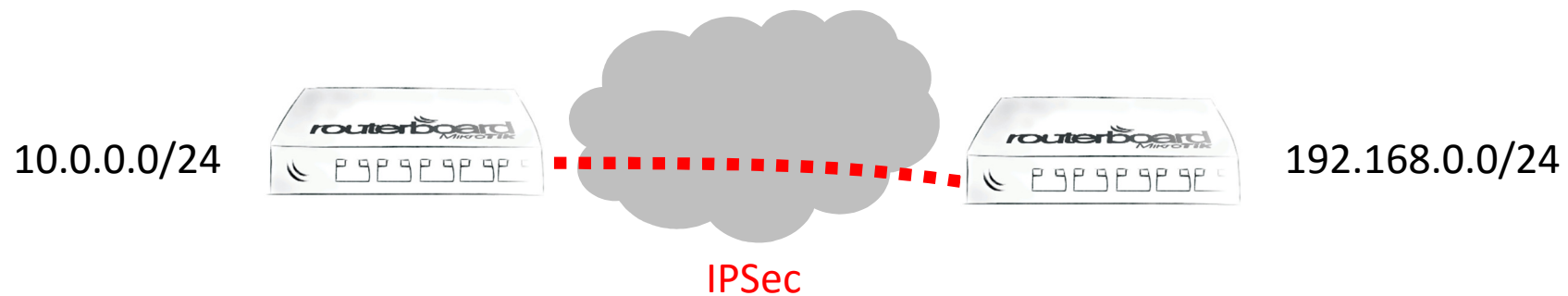
ok

```
/ip firewall filter
add action=drop chain=forward connection-state=new dst-address=\
10.0.0.0/24 in-interface=ether1-INTERNET
```

NAT issues



23



```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=\
  ether1-INTERNET src-address=10.0.0.0/24

/ip firewall nat
add chain=srcnat dst-address=192.168.0.0/24 src-address=\
  10.0.0.0/24
add action=masquerade chain=srcnat out-interface=\
  ether1-INTERNET src-address=10.0.0.0/24
```

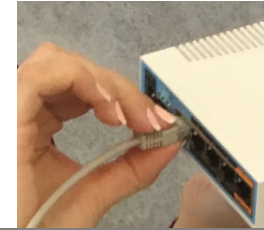

Allowed IP Spoofing



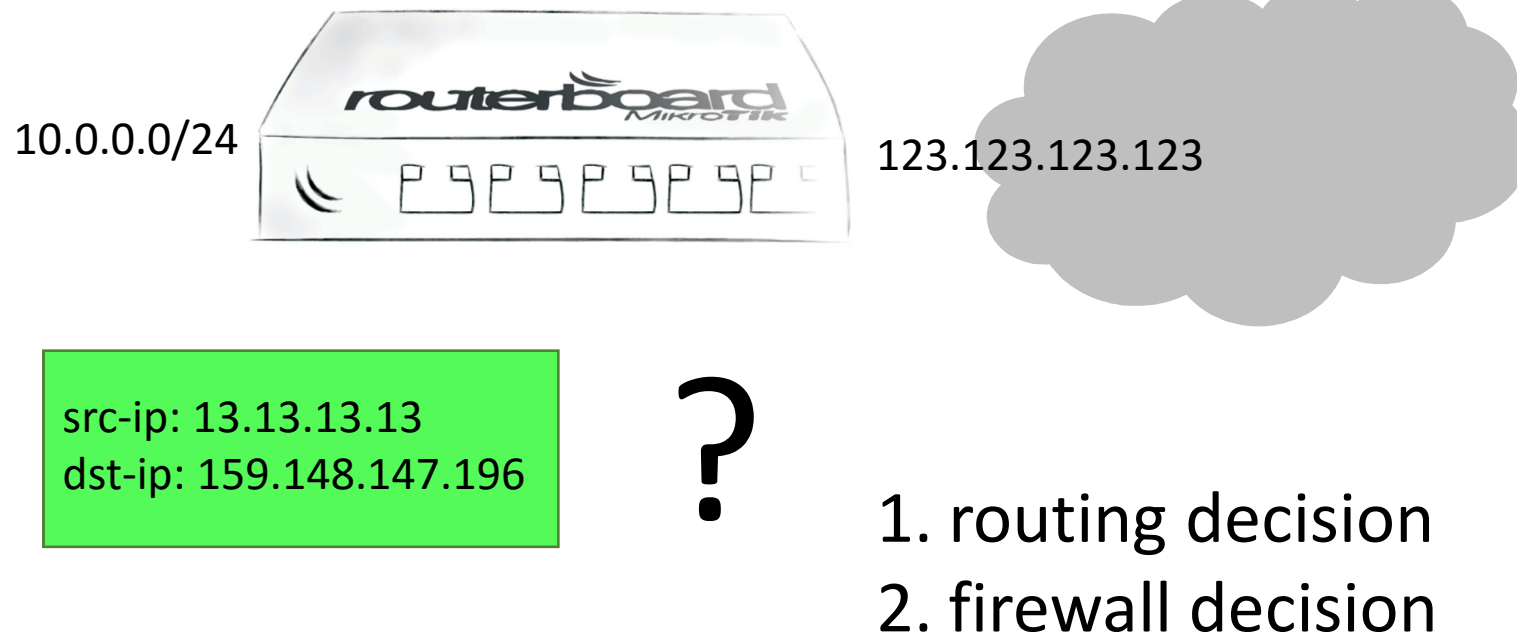
24



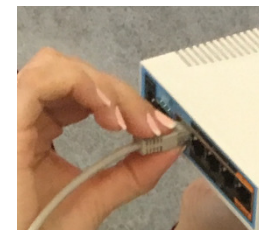
Allowed IP Spoofing



25

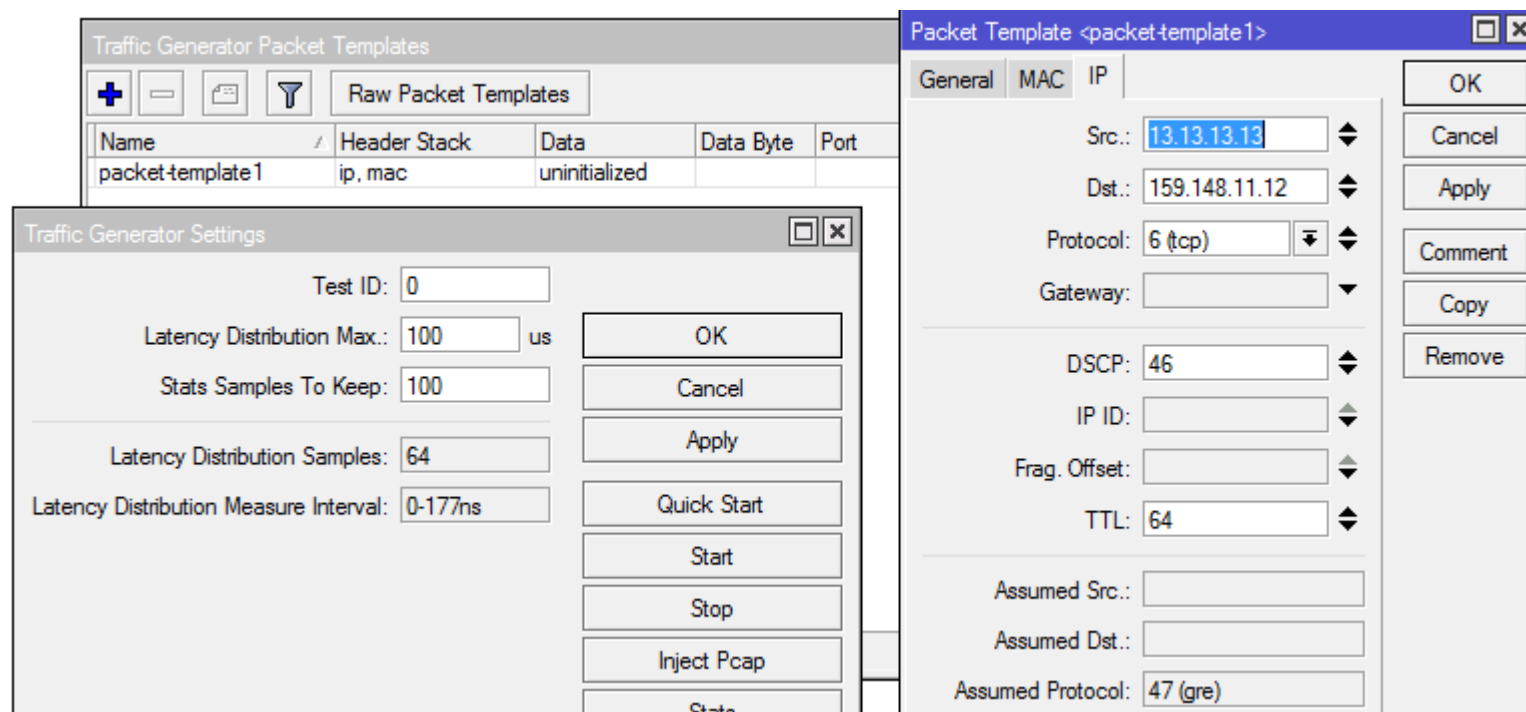


Allowed IP Spoofing

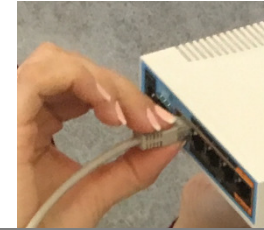


26

Tools- Traffic Generator



Allowed IP Spoofing



27

Test your network <https://spoofer.caida.org/>

☐ **Firewall as a service in SDN OpenFlow network**

Andis Arins

Information, Electronic and Electrical Engineering (AIEEE), 2015 IEEE 3rd
Workshop on Advances in

Year: 2015

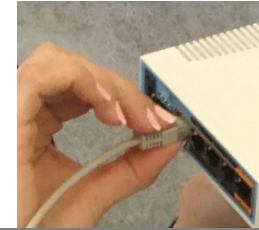
Pages: 1 - 5, DOI: [10.1109/AIEEE.2015.7367309](https://doi.org/10.1109/AIEEE.2015.7367309)

IEEE Conference Publications

► Abstract ((html))  (307 Kb) ©

<http://ieeexplore.ieee.org/>

Allowed IP Spoofing



28

IP Settings

☒ IP Forward

☒ Send Redirects

☐ Accept Redirects

☒ Secure Redirects

☐ Accept Source Route

☒ Allow Fast Path

☒ Route Cache

RP Filter: 

Max Neighbor Entries:

ARP Timeout:

ICMP Rate Limit:

☐ IPv4 Fast Path Active

IPv4 Fast Path Packets:

IPv4 Fast Path Bytes:

☐ IPv4 Fasttrack Active

IPv4 Fasttrack Packets:

IPv4 Fasttrack Bytes:

OK Cancel Apply

10.0.0.0/24



src-ip: 13.13.13.13
dst-ip: 159.148.147.196



routing
decision

Bridge issues



29

4

Bridge issues

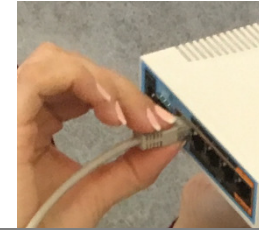


30

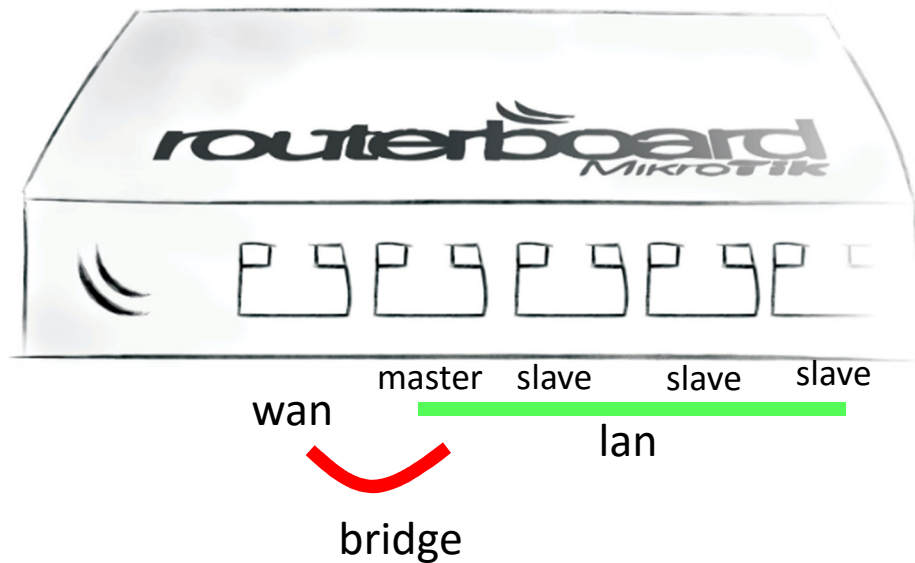


```
/interface bridge
add name=bridge1-switch-without
/interface bridge port
add bridge=bridge1-switch-without interface=ether2
add bridge=bridge1-switch-without interface=ether1-INTERNET
```

Bridge issues



31



Bridge						
Bridge Ports Filters NAT Hosts						
+ - ✓ ✕ [] []						
Interface	Bridge	Priority (h...	Path Cost	Horizon	Role	
::: defconf ether2-master	bridge	80	10		designated port	
::: defconf sfp 1	bridge	80	10		disabled port	
::: defconf wlan 1	bridge	80	10		disabled port	
::: defconf wlan 2	bridge	80	10		disabled port	

```
/interface ethernet
set [ find default-name=ether2 ] name=ether2-master
set [ find default-name=ether3 ] master-port=ether2-master
set [ find default-name=ether4 ] master-port=ether2-master
set [ find default-name=ether5 ] master-port=ether2-master
```


Bridge issues



32

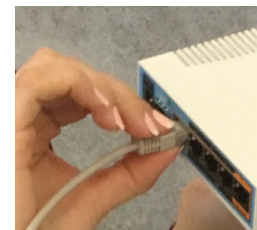


bridge-lan

DHCP Server					
DHCP Networks Leases Options Option Sets Alerts					
+ - ✓ ✕ ⏏ DHCP Config DHCP Setup					
Name	Interface	Lease Time	Address Pool	Add AR...	
defconf	ether3	00:10:00	default-dhcp	no	

DHCP-Server on individual port, not on bridge itself

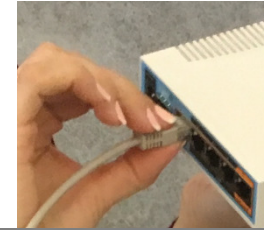
PoE issues



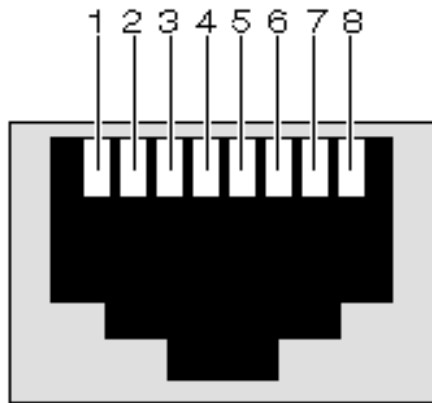
33



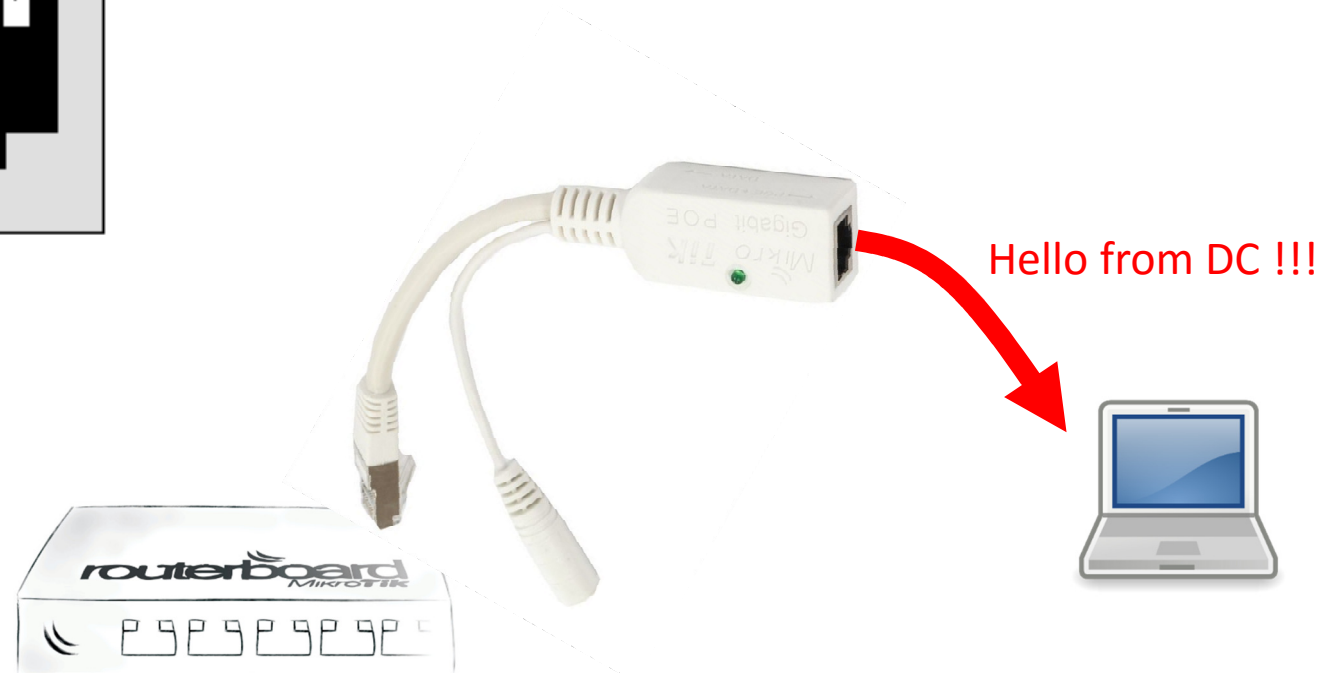
PoE issues



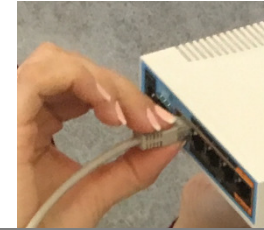
34



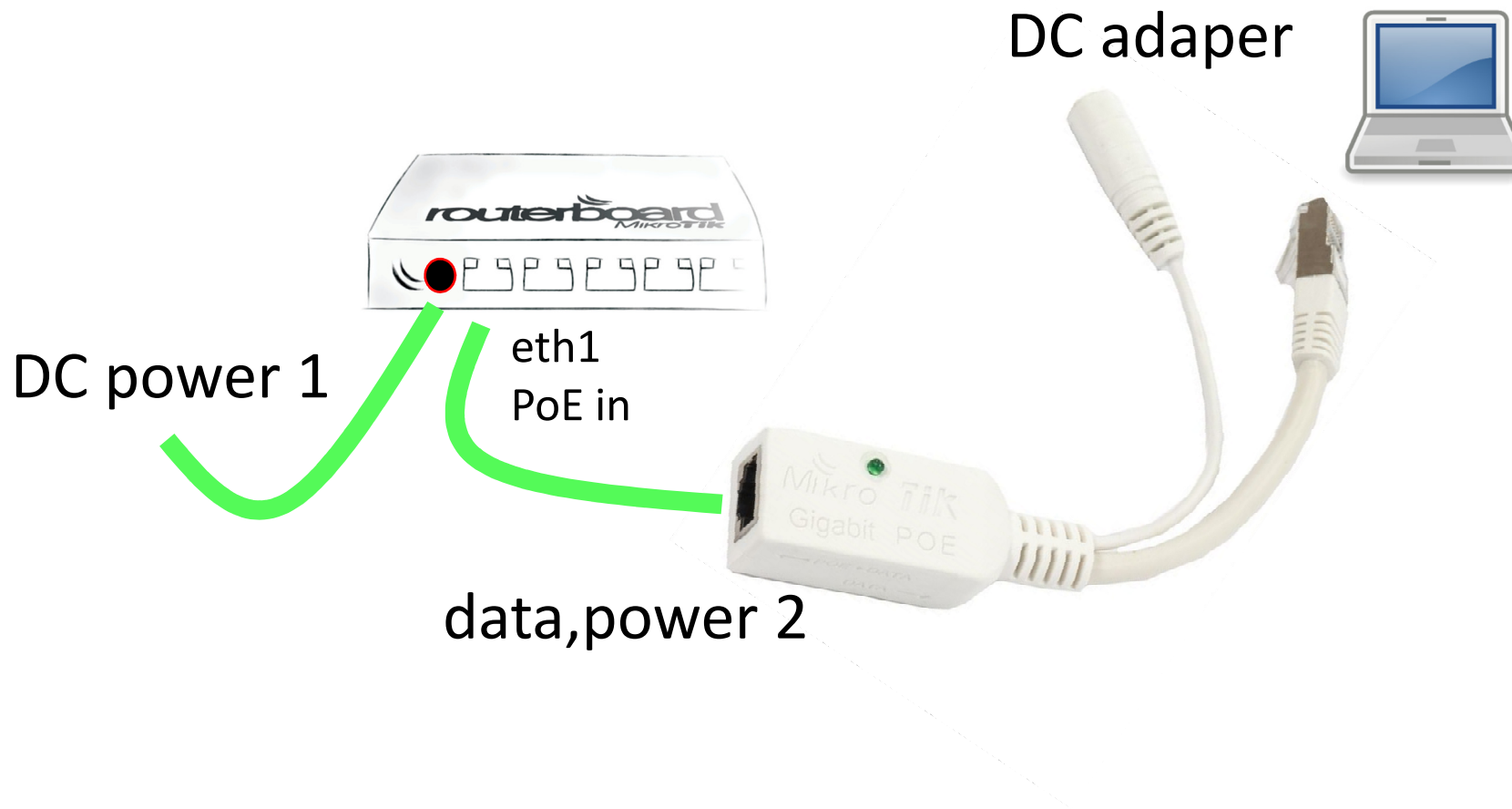
Mikrotik PoE standart
(4,5pin +) (7,8pin -)



PoE issues



35



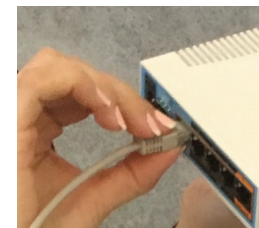
Waiting for hackers



36



Waiting for hackers



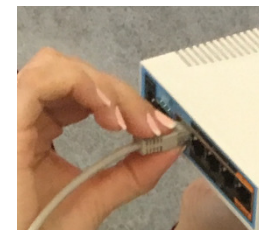
37

IP Service List				
☒	☐	☐		
	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

Dude (if installed) port 2211

Apr/28/2016 14:28:53	memory	system, error, critical	login failure for user admin from 208.67.1.187 via ssh
Apr/28/2016 14:28:55	memory	system, error, critical	login failure for user root from 208.67.1.187 via ssh
Apr/28/2016 14:28:56	memory	system, error, critical	login failure for user admin from 208.67.1.187 via ssh
Apr/28/2016 14:28:57	memory	system, error, critical	login failure for user test from 208.67.1.187 via ssh
Apr/28/2016 14:28:58	memory	system, error, critical	login failure for user root from 208.67.1.187 via ssh
Apr/28/2016 14:29:00	memory	system, error, critical	login failure for user vagrant from 208.67.1.187 via ssh
Apr/28/2016 14:29:01	memory	system, error, critical	login failure for user pi from 208.67.1.187 via ssh
Apr/28/2016 14:29:02	memory	system, error, critical	login failure for user root from 208.67.1.187 via ssh
Apr/28/2016 14:29:04	memory	system, error, critical	login failure for user ubnt from 208.67.1.187 via ssh
Apr/28/2016 14:29:05	memory	system, error, critical	login failure for user telnet from 208.67.1.187 via ssh
Apr/28/2016 14:29:06	memory	system, error, critical	login failure for user device from 208.67.1.187 via ssh
Apr/28/2016 14:29:08	memory	system, error, critical	login failure for user public from 208.67.1.187 via ssh
Apr/28/2016 14:29:09	memory	system, error, critical	login failure for user admin from 208.67.1.187 via ssh
Apr/28/2016 14:29:10	memory	system, error, critical	login failure for user sysadm from 208.67.1.187 via ssh
Apr/28/2016 14:29:11	memory	system, error, critical	login failure for user write from 208.67.1.187 via ssh
Apr/28/2016 14:29:13	memory	system, error, critical	login failure for user Manager from 208.67.1.187 via ssh
Apr/28/2016 14:29:14	memory	system, error, critical	login failure for user echo from 208.67.1.187 via ssh
Apr/28/2016 14:29:15	memory	system, error, critical	login failure for user guest from 208.67.1.187 via ssh
Apr/28/2016 14:29:17	memory	system, error, critical	login failure for user vcr from 208.67.1.187 via ssh
Apr/28/2016 14:29:18	memory	system, error, critical	login failure for user scmadmin from 208.67.1.187 via ssh
Apr/28/2016 14:29:19	memory	system, error, critical	login failure for user admin from 208.67.1.187 via ssh
Apr/28/2016 14:29:20	memory	system, error, critical	login failure for user admin from 208.67.1.187 via ssh
Apr/28/2016 14:29:22	memory	system, error, critical	login failure for user diag from 208.67.1.187 via ssh
Apr/28/2016 14:29:23	memory	system, error, critical	login failure for user unknown from 208.67.1.187 via ssh
Apr/28/2016 15:33:52	memory	system, error, critical	login failure for user root from 220.124.151.130 via ssh
Apr/28/2016 15:33:55	memory	system, error, critical	login failure for user root from 220.124.151.130 via ssh
Apr/28/2016 15:33:57	memory	system, error, critical	login failure for user root from 220.124.151.130 via ssh

Waiting for hackers



38

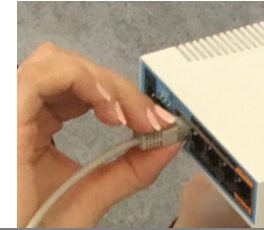
Firewall												
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols												
+ - ✓ ✗ 📄 🔍 00 Reset Counters 00 Reset All Counters Find input												
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Int...	Bytes	Packets	
::: drop Invalid connections												
0	✗ drop	input								184 B	3	
::: allow Established connections												
1	✓ accept	input								342.3 KiB	5 010	
::: allow remote administration from mikrotik office. here could come also other whitelists												
2	✓ accept	input	159.148.147.0/24							0 B	0	
::: allow pings ICMP												
3	✓ accept	input			1 (icmp)					0 B	0	
::: allow DNS requests from LAN. Here could be any other services like VPN from internet, Proxy, OSPF etc												
4	✓ accept	input			17 (udp)		53	!ether3-wan		2652 B	36	
5	✓ accept	input	192.168.200.0/24					!ether3-wan		7.9 KiB	88	
::: drop everything else												
6	✗ drop	input								6.3 KiB	48	

```

/ip firewall filter
add action=drop chain=input comment="drop Invalid connections" connection-state=invalid
add chain=input comment="allow Established connections" connection-state=established
add chain=input comment="allow remote administration from mikrotik office. here could come also other whitelists" \
src-address=159.148.147.0/24
add chain=input comment="allow pings ICMP" protocol=icmp
add chain=input comment=\
"allow DNS requests from LAN. Here could be any other services like VPN from internet, Proxy, OSPF etc" dst-port=53 \
in-interface=!ether3-wan protocol=udp
add chain=input in-interface=!ether3-wan src-address=192.168.200.0/24
add action=drop chain=input comment="drop everything else"

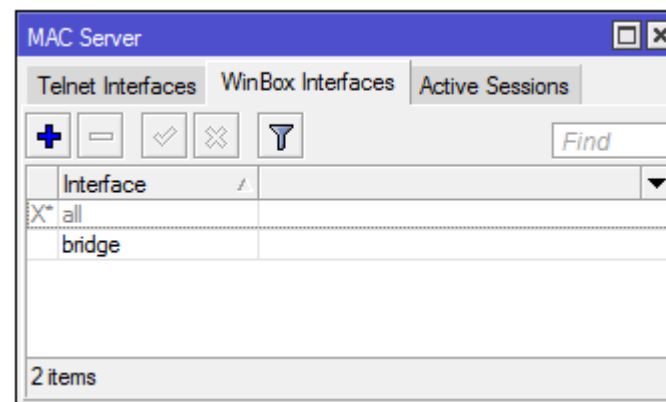
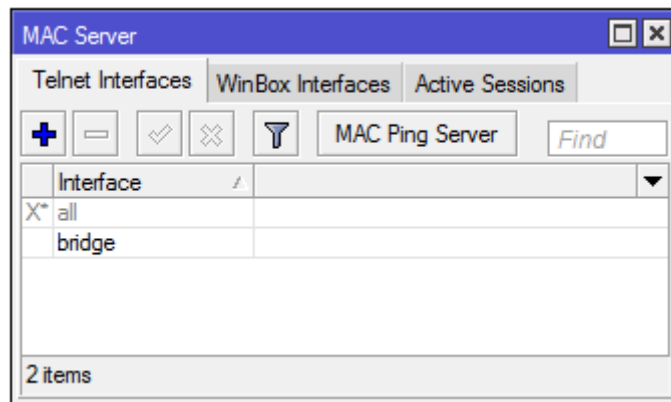
```

Waiting for hackers



39

MAC telnet/winbox server on all interfaces



default configuration allows MAC access only from initial bridge

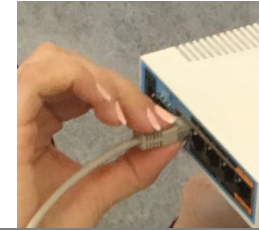
Try to Guess ...



40



admin / no password



41

```
[admin@MikroTik] > /system routerboard print
routerboard: yes
        model: RouterBOARD 941-2nD
  serial-number: 5F5E0563B341
  firmware-type: qca9531L
factory-firmware: 3.24
current-firmware: 3.33
upgrade-firmware: 3.33
[admin@MikroTik] > /user export
# apr/28/2016 09:31:07 by RouterOS 6.35.1
# software id = DIPN-Z4TN
#
/user
add comment="system default user" group=full name=admin
```

User List

Users	Groups	SSH Keys	SSH Private Keys	Active Users
+ - ✓ ✗ [icon] [icon] AAA				
Name	Group	Allowed Address	Last Logged In	
... system default user				
admin	full		Apr/28/2016 16:09:19	

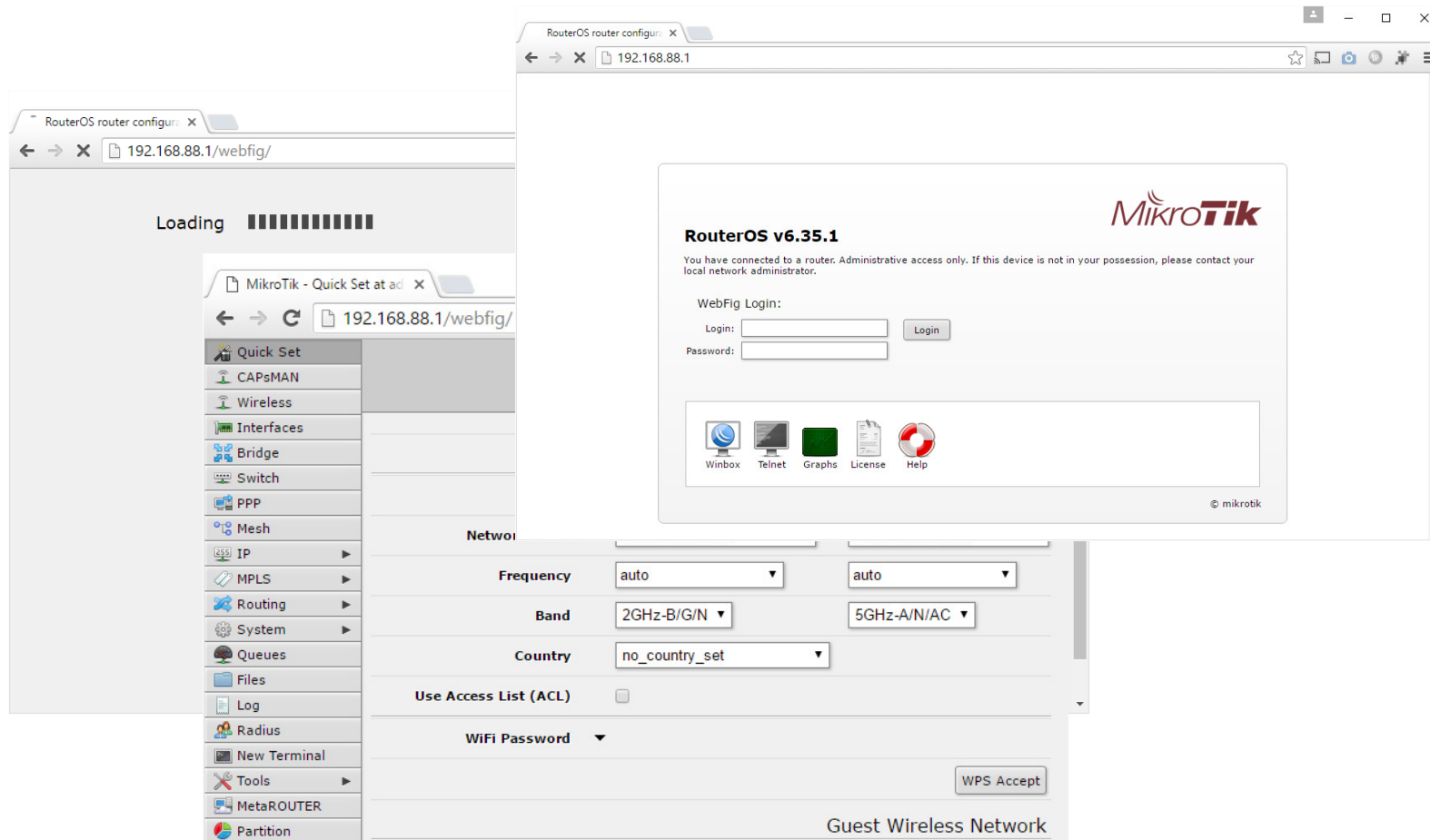
User <admin>

Name: admin	OK
Group: full	Cancel
Allowed Address:	Apply
Last Logged In: Apr/28/2016 16:09:19	Disable

admin / no password



42



That's it!

