

The real story

A hidden security audit of a misconfigured public Wi-Fi network

Nikita Tarikin

Certified network engineer
MikroTik PRO, Russia 



Nikita Tarikin

Certified network engineer
MikroTik PRO, Russia 

MTCNA 90%

MTCRE 93%

MTCWE 84%

MTCTCE 76%

MTCUME 90%



Outsourcing MikroTik network engineering

1. Designing enterprise class networks
2. Building high-performance, reliable, hacker-proof networks
3. Security and performance audit of existing networks
4. Monitoring and maintaining critical infrastructure
5. Troubleshooting and consulting
6. Remote support 24/7/365

MTCNA 90%

MTCRE 93%

MTCWE 84%

MTCTCE 76%

MTCUME 90%

Contact me

Web: tarikin.com

E-mail: nikita@tarikin.com

Facebook: fb.com/tarikin

Instagram: [@tarikin](https://www.instagram.com/tarikin)

Telegram: t.me/tarikin



Introduction

Introduction

— — —

Location:

Summer vacation. Somewhere very far away from civilization. Rented private house somewhere on the seaside.

Time: Summer 2017

Connectivity:

- Broadband cable not available
- 3G/LTE signal is completely unavailable
- 2G/EDGE signal is available

Issue: SOS! We are offline!



Mama, we are offline!!!!1

Mama,
we are F%CKN offline!!!!

Googling hard ...

A few kilometers from our house we found a country club house with available Wi-Fi facilities* .

** Wi-Fi availability is mentioned on the booking website*



[Round 1]

Explore

Came with laptop to check email ...



Reserved a private table in restaurant:

- Do you have a Wi-Fi here?
- Yes, sure! Would you like to order something? The wifi password will be at the end of your bill.
- Mineral water please.



Came to check **email** Wi-Fi speed ☐☐



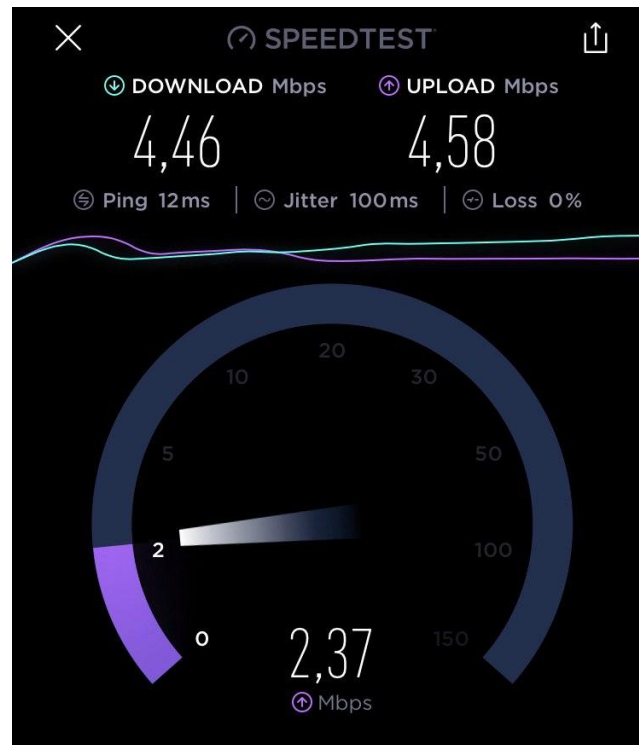
Speedtest:

Download: 4.46Mbit/sec

Upload: 4.58Mbit/sec

Ping: 12ms

Jitter: 100ms



4.5 Mbit/sec

Yeaaahooo!

Mama, we are back online!

4.5 Mbit/sec

4.5 Mbit/sec - already better than our 2G, but still.. We need a bit more :)

- Lady, why is your Internet connectivity so slow?
- Slow? Nobody's complained about it before..



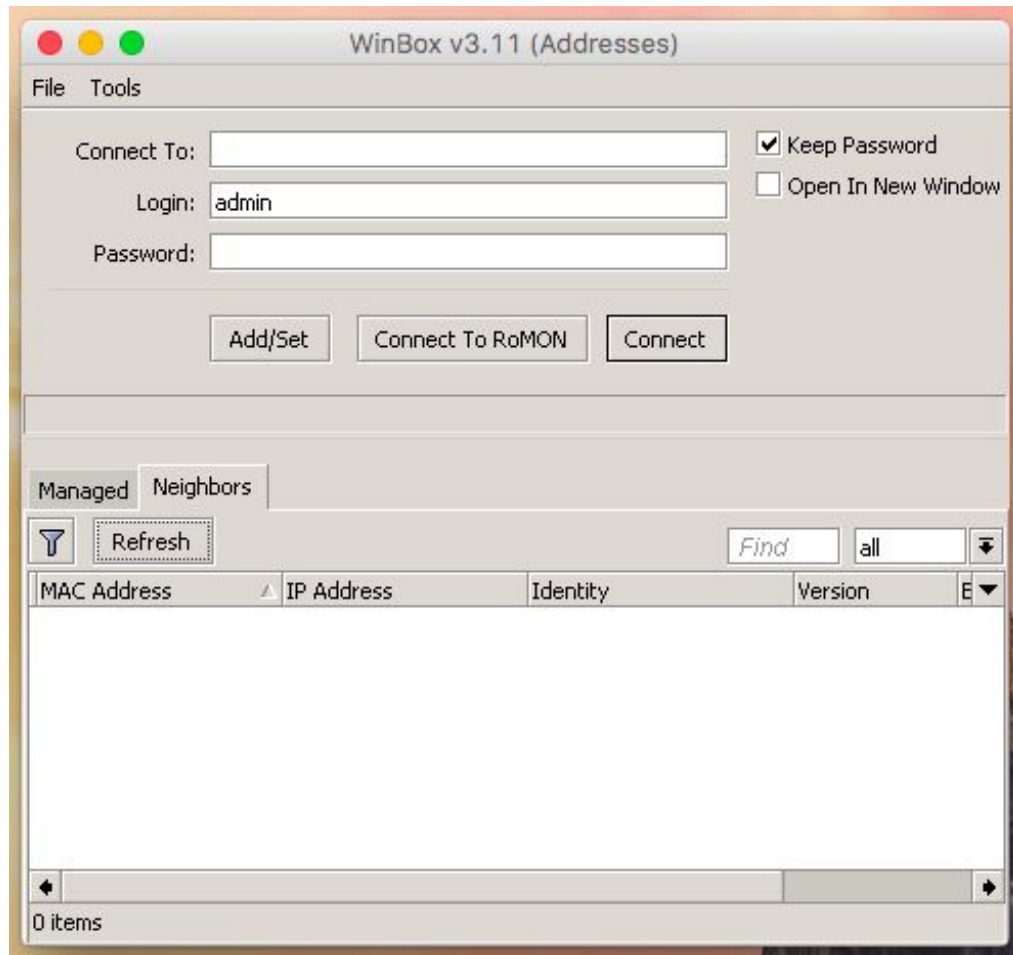
RouterBoard ?

```
arp -a
```

```
gw: 10.0.2.1
```

```
mac: 00:19:5B:0B:17:A2
```

D-Link.



[Round 2]

Aiming the target

Always on WiFi enabled: **false**

Always on WiFi enabled: **connecting ...**

MikroTik SXT Lite2. I always keep it in my backpack.



Always on WiFi enabled: CONNECTED!

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels

00 Reset

Radio Name	MAC Address	Interface	Uptime	AP	...	Last Activi...	Tx/Rx Signal ...	Tx Rate	Rx Rate
E48D8C	13	E4:8D:8C: :13	wlan1	00:02:25	yes	no	0.170 -91/-82	5.5Mbps	1Mbps

1 item (1 selected)

AP Client <E4:8D:8C: :13>

General 802.1x Signal Nstreme NV2 Statistics

Last Activity: 0.170 s

Tx/Rx Signal Strength: -91/-82 dBm

Tx/Rx Signal Strength Ch0: -91/-85 dBm

Tx/Rx Signal Strength Ch1: -86 dBm

Tx/Rx Signal Strength Ch2:

Signal To Noise: 23 dB

Tx/Rx CCQ: 73/78 %

P Throughput: 3417 kbps

- Signal Strengths

Rate	Strength	Last Measured
2Mbps	-83	00:00:11.22
1Mbps	-82	00:00:00.04
5.5M...	-82	00:00:11.02
11Mbps	-82	00:00:00.46
6Mbps	-81	00:00:00.99

OK

Remove

Reset

Copy to Access List

Copy to Connect List

Ping

MAC Ping

Telnet

MAC Telnet

Torch

AP Client <E4:8D:8C: :13>

General 802.1x Signal Nstreme NV2 Stati

Last Activity: 0.170 s

Tx/Rx Signal Strength: -91/-82 dBm

Tx/Rx Signal Strength Ch0: -91/-85 dBm

Tx/Rx Signal Strength Ch1: -86 dBm

Tx/Rx Signal Strength Ch2:

Signal To Noise: 23 dB

Tx/Rx CCQ: 73/78 %

Always on WiFi enabled: **CONNECTED!**

The screenshot displays the Mikrotik WinBox interface. The main window shows the 'Wireless Tables' section with the 'Connect List' tab selected. A table lists the active wireless connections:

Radio Name	MAC Address	Interface	Uptime	AP	...	Last Activi...	Tx/Rx Signal ...	Tx Rate	Rx Rate
E48D8C	13 E4:8D:8C: :13	wlan1	00:03:25	yes	no	0.000	-93/-82	5.5Mbps	1Mbps

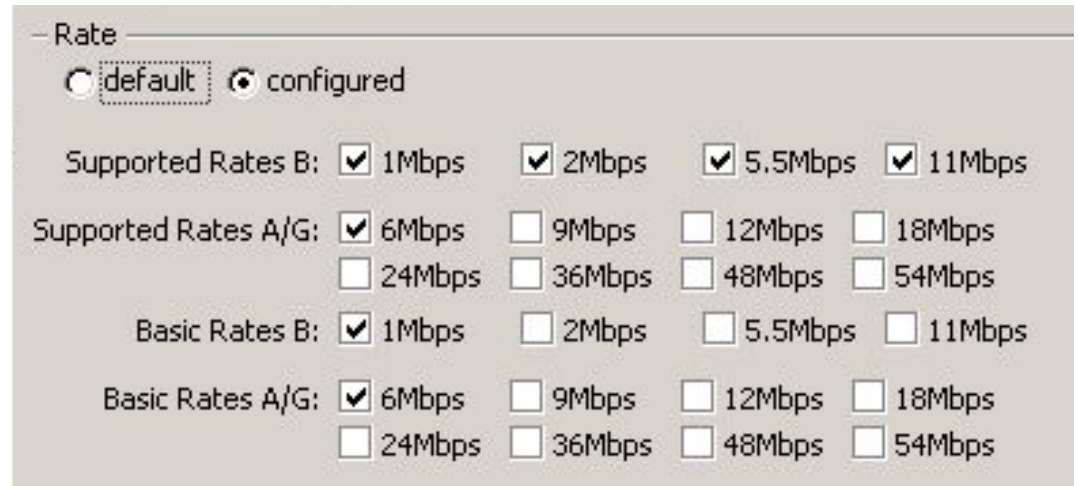
An 'Interface <wlan1>' dialog box is open, showing the 'Wireless' tab. The 'Rate' section is expanded, and the 'configured' radio button is selected. The following rate settings are visible:

- Supported Rates B: 1Mbps, 2Mbps, 5.5Mbps, 11Mbps
- Supported Rates A/G: 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps
- Basic Rates B: 1Mbps, 2Mbps, 5.5Mbps, 11Mbps
- Basic Rates A/G: 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps

The dialog box includes standard control buttons: OK, Cancel, Apply, Disable, Comment, Simple Mode, and Torch.

Always on WiFi enabled: **CONNECTED!**

Disable all unnecessary **wireless modulation** in this case for more **stable connectivity** on long distance
#MTCWE

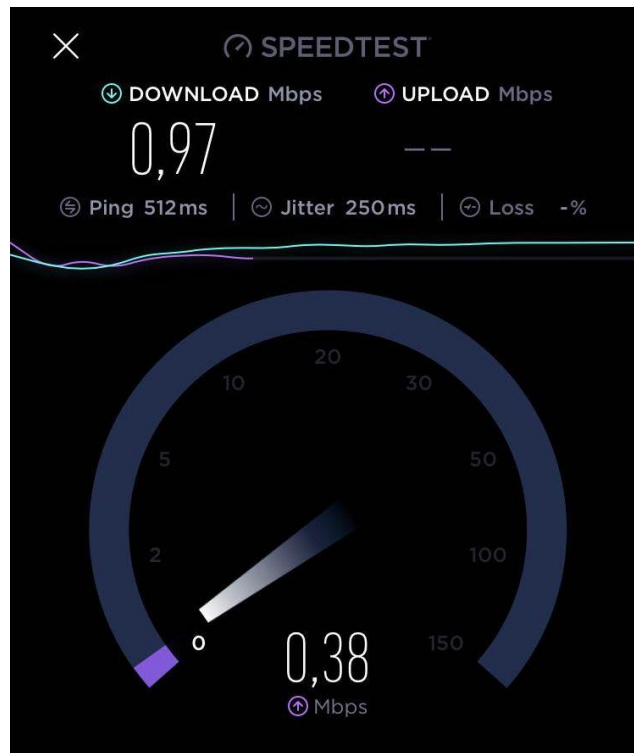


Always on WiFi enabled: TRUE!

FREE Wi-Fi is better than FREE beer!

Speedtest measured 1 Mbit/sec!

```
Request timeout for icmp_seq 8
64 bytes from 8.8.8.8: icmp_seq=9 ttl=57 time=65.080 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=57 time=130.025 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=57 time=60.378 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=57 time=78.101 ms
Request timeout for icmp_seq 13
Request timeout for icmp_seq 14
```



Always on WiFi enabled: TRUE



Nikita Tarikin

MikroTik Certified
Wireless Engineer
86 level



[Round 3]

Boosting the signal

Always on WiFi enabled: ... but too slow!



VS



Always on WiFi enabled: ... but too slow!



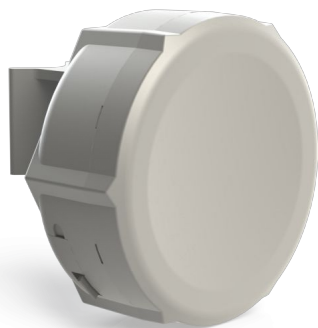
SXT Lite2

VS



QRT 2

Always on WiFi enabled: ... but too slow!



SXT Lite2

Tx-power: 27 dBm (500mW)
Antenna gain: 10 dBi
Beam: 60 degree

VS



QRT 2

Tx-power: 35 dBm (3200mW)
Antenna gain: 17 dBi
Beam: 22 degree

Always on WiFi enabled: 2 Mbit/s

Wireless Tables

Interfaces Nstreame Dual Access List Registration Connect List Security Profiles Channels

00 Reset

Radio Name	MAC Address	Interface	Uptime	AP	...	Last Activi...	Tx/Rx Signal ...	Tx Rate	Rx Rate
E48D8C	13	E4:8D:8C: :13	wlan1	00:01:31	yes	no	0.000 -81/-77	24Mbps	24Mbps

1 item (1 selected)

AP Client <E4:8D:8C: :13>

General 802.1x Signal Nstreame NV2 Statistics

Last Activity: 0.000 s

Tx/Rx Signal Strength: -81/-77 dBm

Tx/Rx Signal Strength Ch0: -81/-81 dBm

Tx/Rx Signal Strength Ch1: -81 dBm

Tx/Rx Signal Strength Ch2:

Signal To Noise: 32 dB

Tx/Rx CCQ: 88/86 %

P Throughput: 17713 kbps

- Signal Strengths

Rate	Strength	Last Measured
1Mbps	-77	00:00:00.03
2Mbps	-77	00:01:20.68
11Mbps	-76	00:01:07.25
6Mbps	-76	00:01:25.02
24Mbps	-76	00:00:00.59
5.5M...	-75	00:01:08.16
12Mbps	-74	00:01:07.55
9Mbps	-73	00:01:08.39
18Mbps	-73	00:01:07.34

AP Client <E4:8D:8C: :13>

General 802.1x Signal Nstreame NV2 Statistics

Last Activity: 0.000 s

Tx/Rx Signal Strength: -81/-77 dBm

Tx/Rx Signal Strength Ch0: -81/-81 dBm

Tx/Rx Signal Strength Ch1: -81 dBm

Tx/Rx Signal Strength Ch2:

Signal To Noise: 32 dB

Tx/Rx CCQ: 88/86 %

P Throughput: 17713 kbps

- Signal Strengths

Rate	Strength	Last Measured
1Mbps	-77	00:00:00.03
2Mbps	-77	00:01:20.68
11Mbps	-76	00:01:07.25
6Mbps	-76	00:01:25.02
24Mbps	-76	00:00:00.59
5.5M...	-75	00:01:08.16
12Mbps	-74	00:01:07.55
9Mbps	-73	00:01:08.39
18Mbps	-73	00:01:07.34

4.5 Mbit/sec

Speedtest:

Download: 4.46Mbit/sec

Upload: 4.58Mbit/sec

Ping: 12ms

Jitter: 100ms



[Round 4]

Audit

Let's see
what's under
the hood ...

Scanner (Running)

Interface: wlan1

Background Scan

Start

Stop

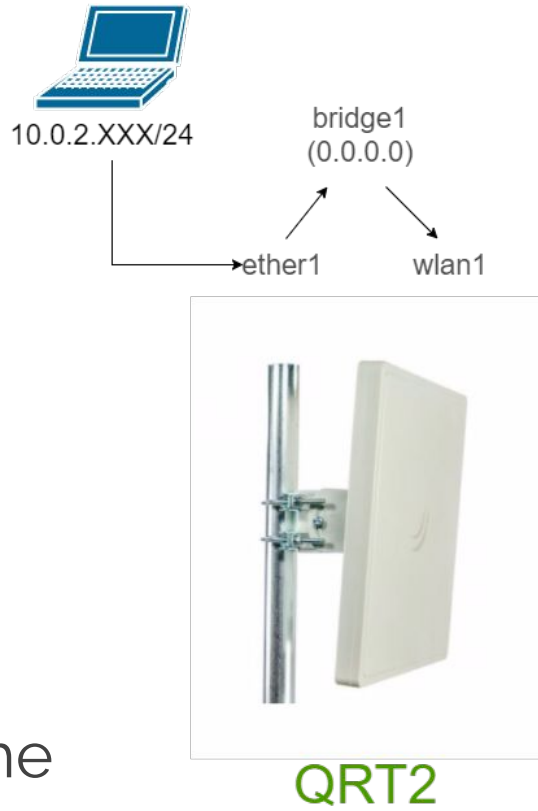
Close

Connect

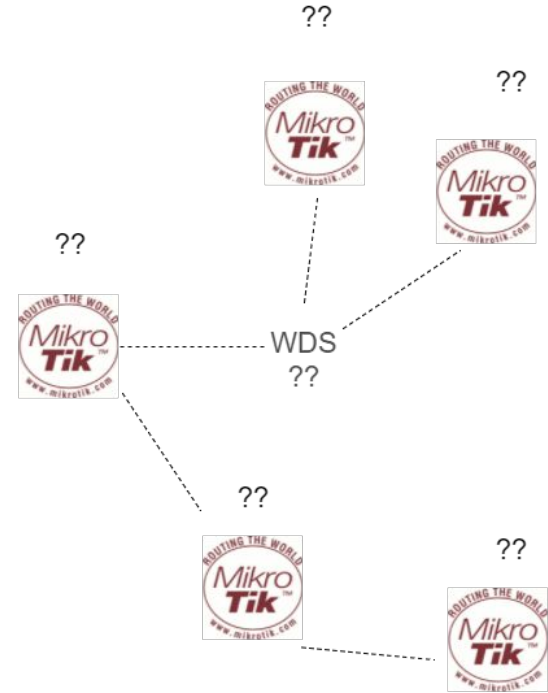
New Window

	Address	SSID	Channel	Signal...	Noise ...	Signal To...	Radio Na...	Router...	
APRB	E4:8D:8C: :13	M a_WiFi_Free	2412/20/g	-78	-110	32	E48D8C...	6.36.4	
APRB	E4:8D:8C: :AD	M a_WiFi_Free	2412/20/g	-80	-110	30	E48D8C...	6.36.4	
APRB	E4:8D:8C: :26	M a_WiFi_Free	2412/20/g	-81	-110	29	E48D8C...	6.36.4	
AP	00:0E:8F: :8A		2412/20/gn	-84	-110	26			
APRB	E4:8D:8C: :3B	M a_WiFi_Free	2412/20/g	-88	-110	22	E48D8C...	6.36.4	
AP	10:FE:ED: :41		2437/20/gn	-91	-115	24			
AP	C4:A8:1D: :18		2422/20/gn	-92	-114	22			
APRB	E4:8D:8C: :45	M a_WiFi_Free	2412/20/g	-94	-110	16	E48D8C...	6.36.4	

8 items



~4 KM



Under the hood ...

Connect To:

Login:

Password:

Session:

Note:

Group:

RoMON Agent:

Keep Password

Secure Mode

Autosave Session

Open In New Window

Managed Neighbors

MAC Address	IP Address	Identity	Version	Board
6C:3B:6B: :99	0.0.0.0	MikroTik	6.39.2 (stable)	RBQRTG-25...

Under the hood ...

	A	B
1	00:19:5B: :A2	10.0.2.1
2	E4:8D:8C: :13	10.0.2.118
3	E4:8D:8C: :AD	10.0.2.131
4	E4:8D:8C: :26	10.0.2.94
5	E4:8D:8C: :3A	10.0.2.68
6		



QRT2

~4 KM

E4:8D:8C:###:###:13

E4:8D:8C:###:###:AD

??

E4:8D:8C:###:###:3A

??



WDS
??

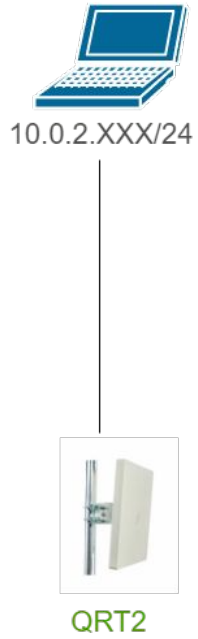


??

E4:8D:8C:###:###:26

??



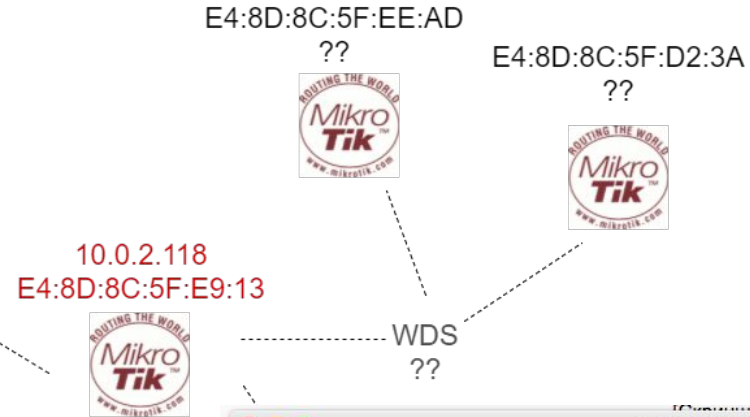


NO ping

NO webfig

NO discovery

NO winbox



10.0.2.118

```
1. ping 10.0.2.118 (ping)
→ ~ ping 10.0.2.118
PING 10.0.2.118 (10.0.2.118): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
Request timeout for icmp_seq 8
Request timeout for icmp_seq 9
Request timeout for icmp_seq 10
Request timeout for icmp_seq 11
```

QRT

2

**NO
DISCOVERY**

10.0.2.118

The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar menu with categories like CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, Routing, System, Queues, Files, Log, Radius, Tools, and New Terminal. The main window displays the 'Neighbor List' window, which has two tabs: 'Neighbors' and 'Discovery Interfaces'. The 'Neighbors' tab is active, showing a table with the following data:

Interface	IP Address	MAC Address	Identity	Platform	Version
bridge1	10.0.2.12	00:00:00:00:00:00			

The status bar at the bottom of the window indicates '1 item'.

RouterOS MAC PING

E4:8D:8C:##:##:13

10.0.2.118

E4:8D:8C:##:##:13
10.0.2.118

The screenshot shows a network configuration interface with a 'Neighbors' tab and a 'Discovery Interfaces' sub-tab. A table lists the interface 'bridge1' with IP address '10.0.2.12' and MAC address '00:00:00:00:00:00'. A 'Ping' dialog box is open, showing the 'General' tab. The 'Ping To' field is set to 'E4:8D:8C:##:##:13', the 'Interface' is 'bridge1', and the 'Packet Count' is '1000'. The 'Timeout' is '1000 ms'. Below the dialog box, a table displays the results of the ping test.

Seq #	Host	Time	Reply Size	TTL	Status
0	E4:8D:8C:##:##:13	3ms	64		
1	E4:8D:8C:##:##:13	2ms	64		
2	E4:8D:8C:##:##:13	4ms	64		
3	E4:8D:8C:##:##:13	2ms	64		
4	E4:8D:8C:##:##:13	344ms	64		
5	E4:8D:8C:##:##:13	2ms	64		
6	E4:8D:8C:##:##:13	4ms	64		
7	E4:8D:8C:##:##:13	3ms	64		
8	E4:8D:8C:##:##:13	5ms	64		
9	E4:8D:8C:##:##:13	5ms	64		
10	E4:8D:8C:##:##:13	7ms	64		



10.0.2.XXX/24

NO ping
NO webfig
NO discovery
NO winbox



QRT2

E4:8D:8C:##:##:13

10.0.2.118

mac-ping OK

10.0.2.118
E4:8D:8C:##:##:13



E4:8D:8C:##:##:AD



E4:8D:8C:##:##:3A



WDS



E4:8D:8C:##:##:26



```
Terminal
MMM      MMM  III  KKK  KKK  RRR  RRR  000000  TTT

MikroTik RouterOS 6.39.2 (c) 1999-2017      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 a second [Tab] gives possible options

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

[admin@MikroTik] > /tool mac-telnet E4:8D:8C:####:13
Login: admin
Password: █
```

E4:8D:8C:####:13

10.0.2.118

User: admin

Password: Admin@123

E4:8D:8C:##:##:13

10.0.2.118



```
Terminal
MMM      MMM  III  KKK  KKK  RRR  RRR  000000  TTT

MikroTik RouterOS 6.39.2 (c) 1999-2017      http://www.i
```

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

[Tab]       Completes the command/word. If the
            a second [Tab] gives possible options

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

[admin@MikroTik] > /tool mac-telnet E4
Login: admin
Password: █
```

```
Terminal

MikroTik RouterOS 6.36.4 (c) 1999-2016      http://www.mikrotik.com

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

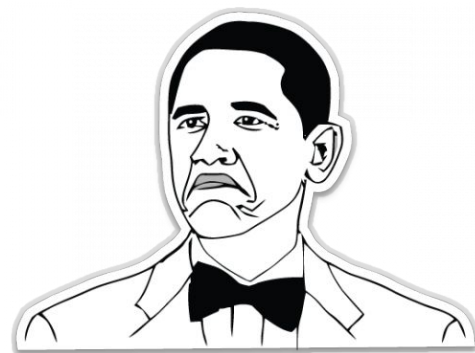
[Tab]       Completes the command/word. If the
            a second [Tab] gives possible options

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

[admin@MikroTik] > /user set admin password=123
not enough permissions (9)
[admin@MikroTik] > █
```

E4:8D:8C:##:##:13

10.0.2.118



```
Terminal
[admin@MikroTik] > /system routerboard print
  routerboard: yes
    model: RouterBOARD Metal 2SHPn
  serial-number: [REDACTED]
  firmware-type: [REDACTED]
  factory-firmware: 1.00
  current-firmware: 1.00
  upgrade-firmware: 1.00
[admin@MikroTik] > /user print
Flags: X - disabled
#  NAME                GROUP                ADDRESS                LAST-LOGGED-IN
0  ;;: system default user
   admin                test
1  zabbix                full
[admin@MikroTik] > /user active print
Flags: R - radius, M - by-romon
#  WHEN                NAME                ADDRESS                VIA
0  [REDACTED] [REDACTED] admin                6C:3B:6B:[REDACTED]:99  mac-telnet
[admin@MikroTik] > █
```

E4:8D:8C:5F:E9:13

10.0.2.118

```
Terminal
[admin@MikroTik] > /system routerboard print
routerboard: yes
model: RouterBOARD Metal 2SHPn
serial-number:
firmware-type:
factory-firmware:
current-firmware:
upgrade-firmware:
[admin@MikroTik] > /user print
Flags: X - disabled
# NAME GROUP ADDRESS LAST-LOGGED-IN
0 ;;; system default user
admin test
1 zabbix full
[admin@MikroTik] > /user active print
Flags: R - radius, M - by-romon
# WHEN NAME ADDRESS VIA
0 admin 6C:3B:6B: mac-telnet
[admin@MikroTik] >
```

E4:8D:8C:##:##:13

10.0.2.118

RouterBoard
Metal 2SHPn

RouterBoard RBMetal2SHPn



E4:8D:8C:##:##:13

10.0.2.118

Tx-power:	32 dBm (3200mW)
Antenna gain:	6 dBi
Beam:	omni-directional
Chains:	1


```
Terminal
[admin@MikroTik] > /system routerboard print
routerboard: yes
model: RouterBOARD Metal 2SHPn
serial-number:
firmware-type:
factory-firmware:
current-firmware:
upgrade-firmware:
[admin@MikroTik] > /user print
Flags: X - disabled
# NAME GROUP ADDRESS LAST-LOGGED-IN
0 ;;; system default user
admin test
1 zabbix full
[admin@MikroTik] > /user active print
Flags: R - radius, M - by-romon
# WHEN NAME ADDRESS VIA
0 admin 6C:3B:6B: :99 mac-telnet
[admin@MikroTik] >
```

E4:8D:8C:##:##:13

10.0.2.118

User: admin
Group: test??

```
Terminal
[admin@MikroTik] > /system routerboard print
routerboard: yes
model: RouterBOARD Metal 2SHPn
serial-number:
firmware-type:
factory-firmware:
current-firmware:
upgrade-firmware:
[admin@MikroTik] > /user print
Flags: X - disabled
#  NAME                GROUP                ADDRESS                LAST-LOGGED-IN
0  ;;; system default user
   admin                test
1  zabbix                full
[admin@MikroTik] > /user active print
Flags: R - radius, M - by-romon
#  WHEN                NAME                ADDRESS                VIA
0  admin                6C:3B:6B:          :99                    mac-telnet
[admin@MikroTik] >
```

E4:8D:8C:##:##:13

10.0.2.118

User: zabbix
Group: full

```
Terminal
[admin@MikroTik] > /user group print
0 name="read" policy=local,telnet,ssh,reboot,read,test,winbox,password,web,sniff,sensitive,
  api,romon,!ftp,!write,!policy,!dude
  skin=default
1 name="write" policy=local,telnet,ssh,reboot,read,write,test,winbox,password,web,sniff,
  sensitive,api,romon,!ftp,!policy,!dude
  skin=default
2 name="full" policy=local,telnet,ssh,ftp,reboot,read,write,policy,test,winbox,password,web,
  sniff,sensitive,api,romon,dude
  skin=default
3 name="test" policy=telnet,read,test,winbox,!local,!ssh,!ftp,!reboot,!write,!policy,
  !password,!web,!sniff,!sensitive,!api,!romon,!dude
  skin=default
[admin@MikroTik] >
```

E4:8D:8C:##:##:13

10.0.2.118

winbox

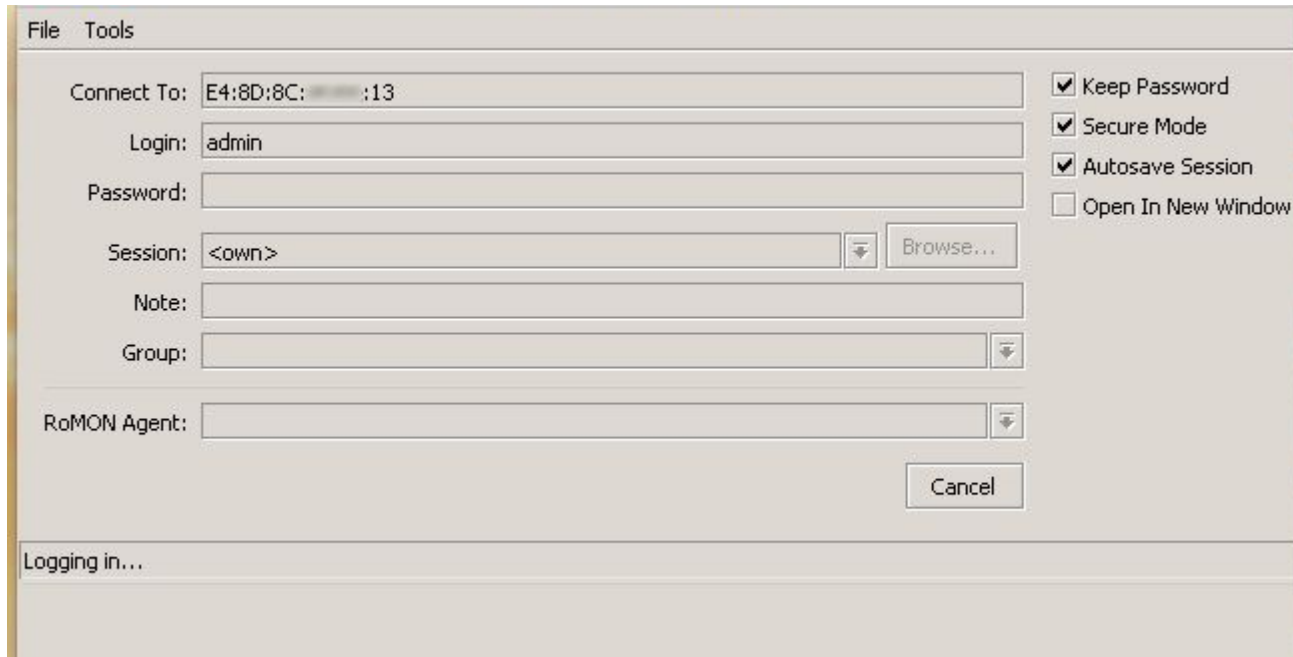
```
Terminal
[admin@MikroTik] > /user group print
0 name="read" policy=local,telnet,ssh,reboot,read,test,winbox,password,web,sniff,sensitive,api,romon,!ftp,!write,!poll
  skin=default
1 name="write" policy=local,telnet,sensitive,api,romon,!ftp,!write,!poll
  skin=default
2 name="full" policy=local,telnet,sniff,sensitive,api,romon,!ftp,!write,!poll
  skin=default
3 name="test" policy=telnet,read,!password,!web,!sniff,!server
  skin=default
[admin@MikroTik] >
```

```
Terminal
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] > /tool mac-server print
Flags: X - disabled, * - default
# INTERFACE
0 * all
[admin@MikroTik] > /tool mac-server
mac-winbox ping sessions add disable edit enable
[admin@MikroTik] > /tool mac-server mac-winbox print
Flags: X - disabled, * - default
# INTERFACE
0 * all
[admin@MikroTik] >
```

E4:8D:8C:##:##:13
10.0.2.118

mac-winbox: * all

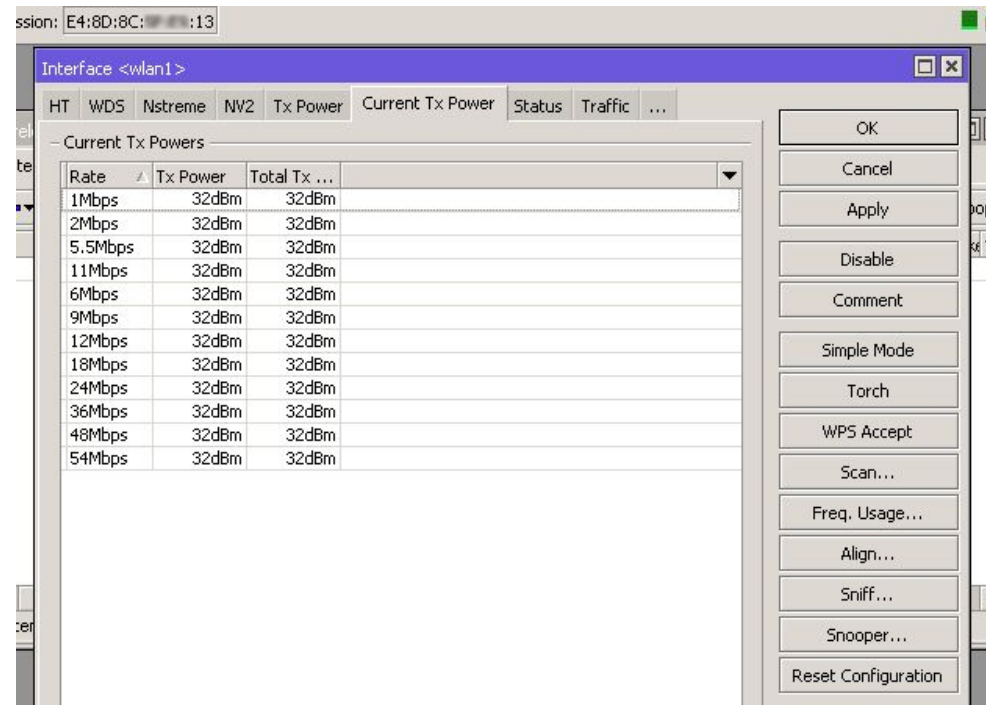
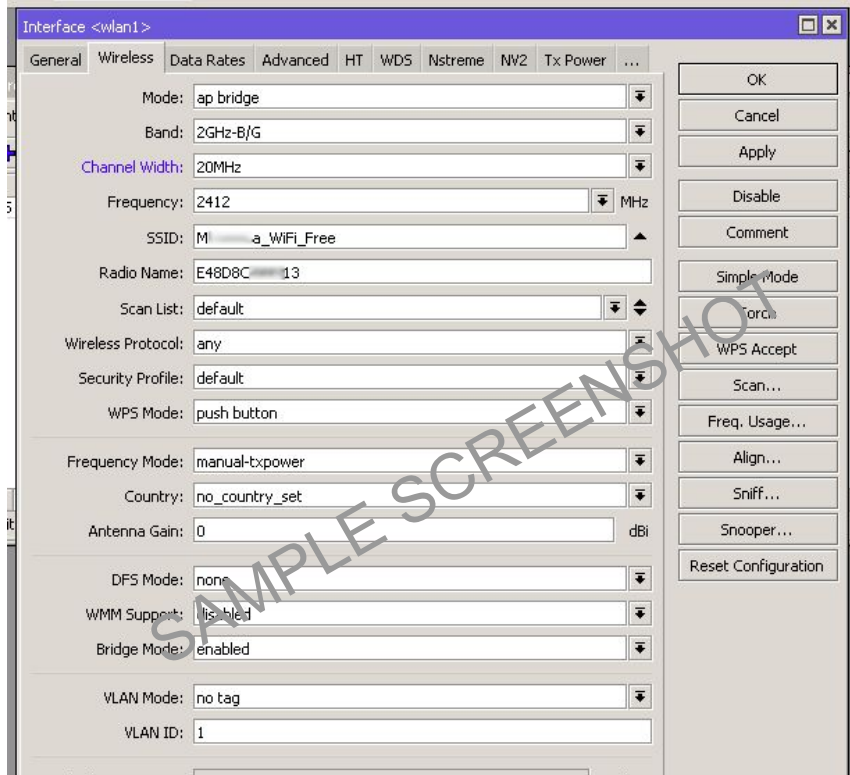
Continue to Winbox



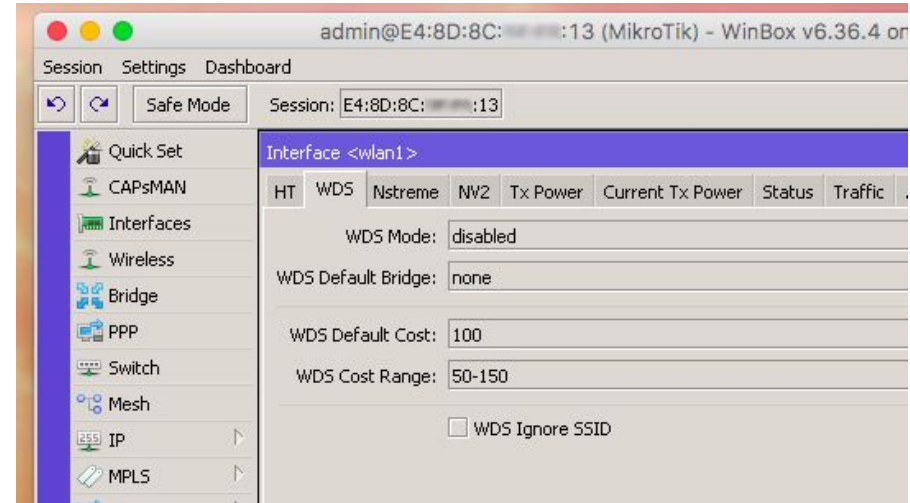
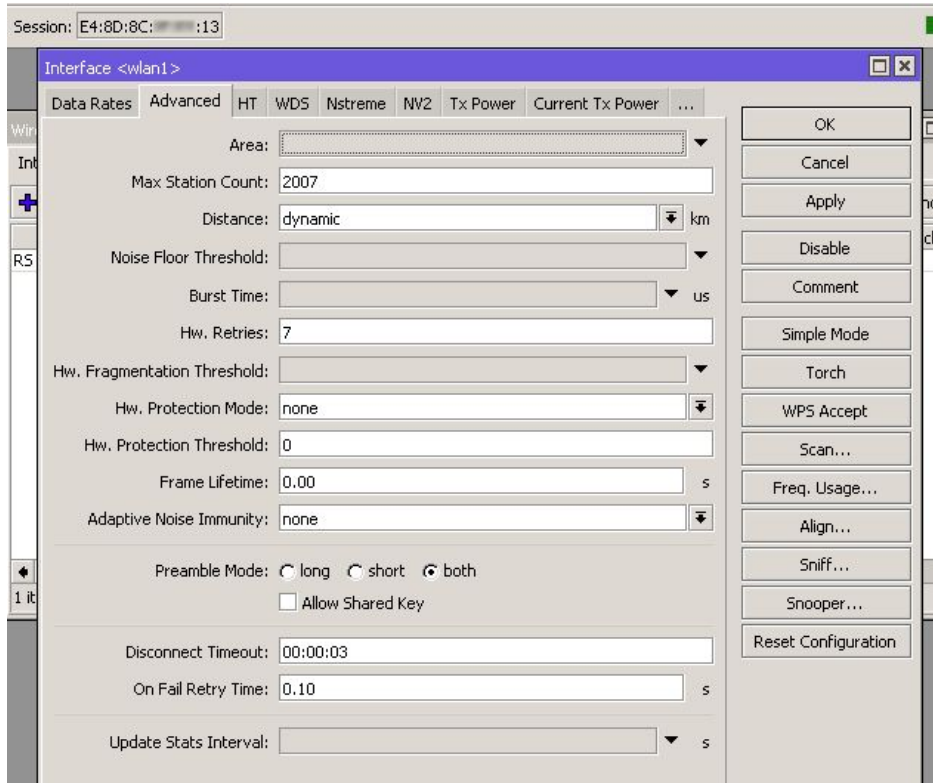
E4:8D:8C:####:13

10.0.2.118

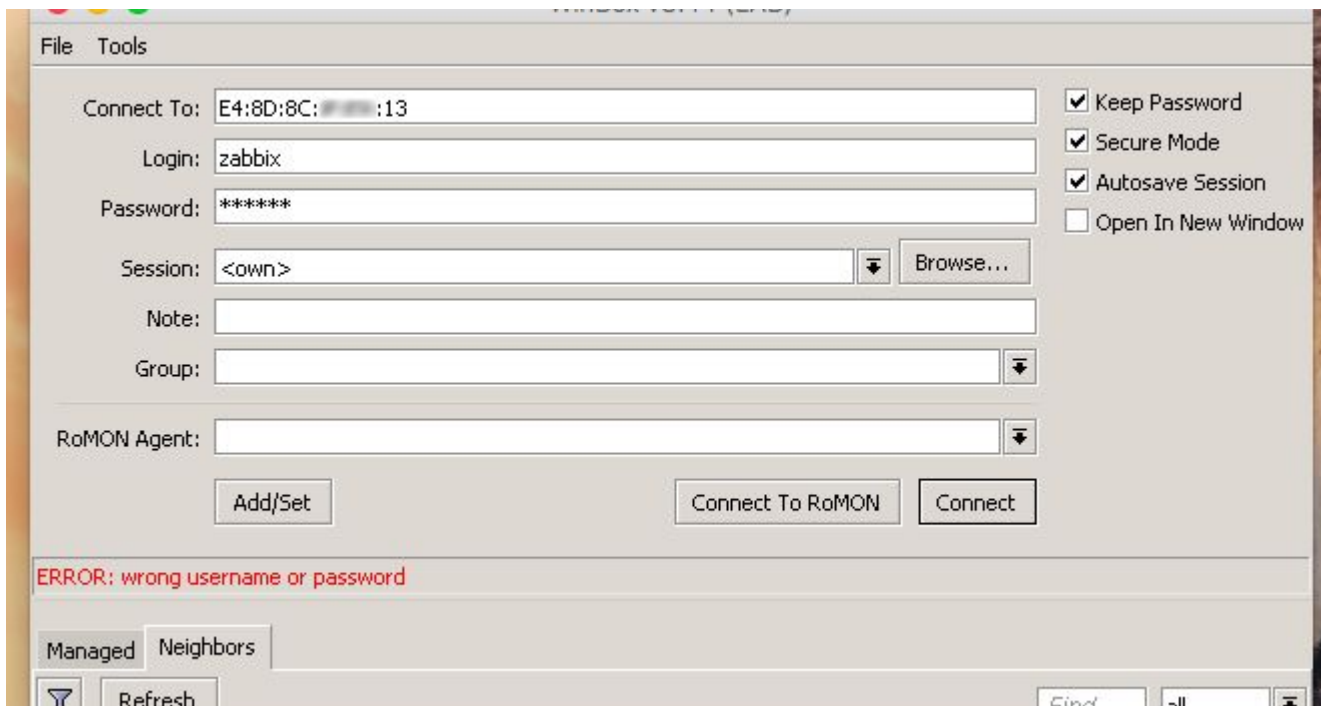
Always on WiFi enabled: ... but too slow!



Always on WiFi enabled: ... but too slow!

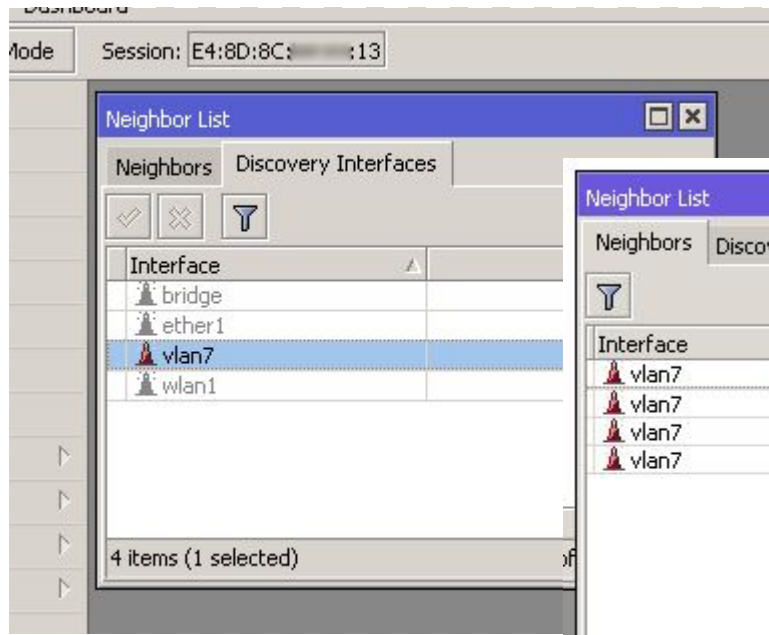


WDS: disabled



E4:8D:8C:####:13

10.0.2.118



Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6
vlan7		4C:5E:0C: :A0	MikroTik	MikroTik	6.36.4 (...)	RB750UPr2	no
vlan7		E4:8D:8C: :AC	MikroTik	MikroTik	6.36.4 (...)	RBMetal2...	no
vlan7		E4:8D:8C: :25	MikroTik	MikroTik	6.36.4 (...)	RBMetal2...	no
vlan7		E4:8D:8C: :3A	MikroTik	MikroTik	6.36.4 (...)	RBMetal2...	no

E4:8D:8C:##:##:13

10.0.2.118



QRT2

10.0.2.118
E4:8D:8C:##:##:13



Metal

discovery
OK

vlan7

NO
discovery

10.0.2.131
E4:8D:8C:##:##:AD



Metal

vlan7

10.0.2.68
E4:8D:8C:##:##:3A



Metal

vlan7



hEX PoE lite

vlan7



Metal

10.0.2.94
E4:8D:8C:##:##:26



Metal

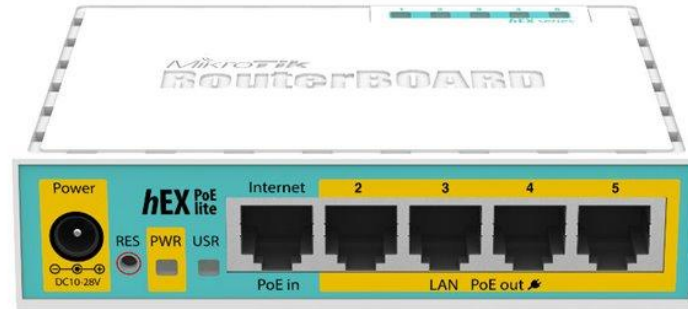
??

E4:8D:8C:##:##:13

10.0.2.118

RouterBoard

RB750UPr2



CPU:

650MHz

RAM:

64MB

PoE-out:

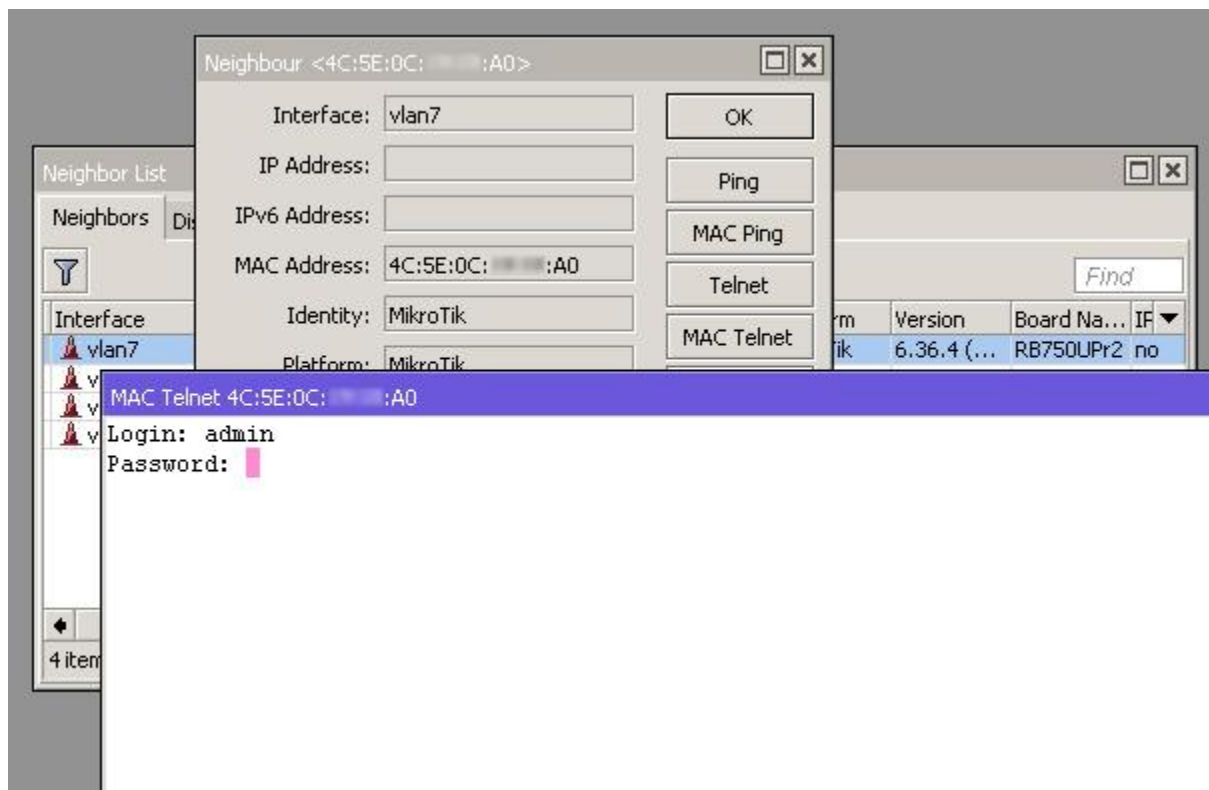
2-5 ports (2A max total)

PoE-in:

ether1

Trying to ~~hack~~ hug the hEX PoE lite

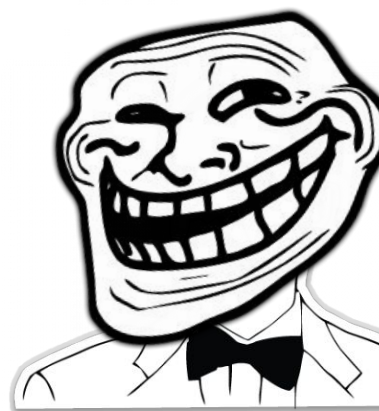
4C:E5:0C:##:##:A0



4C:E5:0C:###:###:A0

```
MAC Telnet 4C:5E:0C:###:AO
# software id =
#
/interface ethernet
set [ find default-name=ether2 ] master-port=ether1
set [ find default-name=ether3 ] master-port=ether1
set [ find default-name=ether4 ] master-port=ether1
set [ find default-name=ether5 ] master-port=ether1
/ip neighbor discovery
set ether1 discover=no
set ether2 discover=no
set ether3 discover=no
set ether4 discover=no
set ether5 discover=no
/interface vlan
add interface=ether1 name=vlan7 vlan-id=7
/system routerboard settings
set cpu-frequency=650MHZ protected-routerboot=disabled
[admin@MikroTik] >
```

4C:E5:0C:###:AO




```
MAC Telnet 4C:5E:0C:###:##:AO
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] > /file print
# NAME                TYPE                SIZE  CREATION-TIME
0 flash                disk
1 pub                  directory
2 MikroTik-2017...    backup              56  1918
3 MikroTik-2017...    backup              56  1918
4 MikroTik-2017...    backup              51  1918
5 MikroTik-2017...    backup              51  1918
6 l.rsc                script
7 zabbix.rsc           script              5785
8 flash/skins          directory
```

4C:E5:0C:##:##:AO

The screenshot shows a Mikrotik WinBox interface. In the background, a table lists interfaces: 'vlan7' and 'vlan7'. A 'MAC Telnet' window is open, displaying a terminal session. The terminal shows the following commands and output:

```
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] > /interface print
Flags: D - dynamic, X - disabled, R - running,
S - slave
#   NAME      TYPE
0  R ether1    ether
1  RS ether2   ether
2  RS ether3   ether
3  RS ether4   ether
4  RS ether5   ether
5  R vlan7     vlan

[admin@MikroTik] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS      NETWORK      INTERFACE
[admin@MikroTik] >
```

4C:E5:0C:##:##:AO

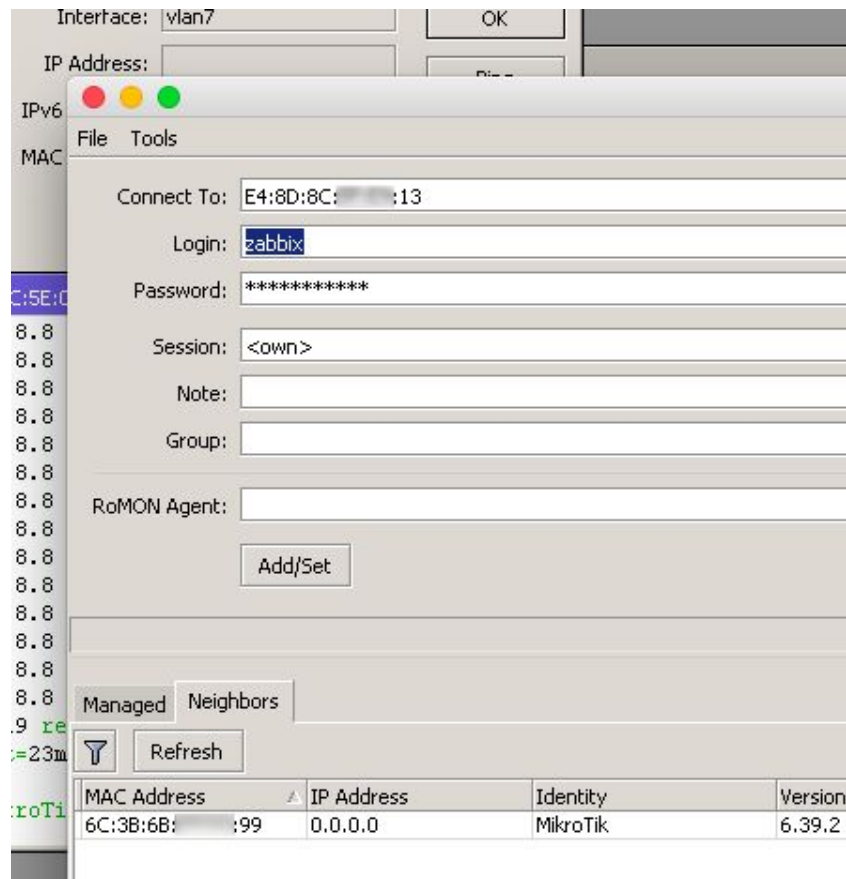
```
MAC Telnet 4C:5E:0C:###:AO
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] > /ip dhcp-client add interface=ether1 disabled=no
[admin@MikroTik] > /ip dhcp-client print
Flags: X - disabled, I - invalid
#  INTERFACE      USE ADD-DEFAULT-ROUTE STATUS      ADDRESS
0  ether1          yes yes                bound      10.0.2.54/24
[admin@MikroTik] > ping 8.8.8.8
SEQ HOST          SIZE TTL TIME  STATUS
0 8.8.8.8         56 55 23ms
1 8.8.8.8         56 55 23ms
2 8.8.8.8         56 55 23ms
3 8.8.8.8         56 55 23ms
4 8.8.8.8         56 55 23ms
5 8.8.8.8         56 55 23ms
```

4C:E5:0C:###:AO

You have new mail...

```
15 /user
16 add name=zabbix password=4W1WBQS4mJob group=full disabled=no
```





E4:8D:8C:##:##:13

Interface: vlan7 OK

IP Address: []

IPv6 []

MAC []

Connect To: E4:8D:8C:####:13

Login: zabbix

Password: *****

Session: <own>

Note: []

Group: []

RoMON Agent: []

Add/Set

Managed Neighbors

Refresh

MAC Address	IP Address	Identity	Version
6C:3B:6B:####:99	0.0.0.0	MikroTik	6.39.2

zabbix@E4:8D:8C:####:13 (MikroTik) -

Session Settings Dashboard

Safe Mode Session: E4:8D:8C:####:13

- Quick Set
- CAPS MAN
- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- MPLS
- Routing

User List

Users Groups SSH Keys SSH Private Keys Active Users

AAA

Name	Group	Allowed Address	Last
;; system	default	user	
admin	test		
zabbix	full		



E4:8D:8C:####:13

QRT2 wireless scanner (Running)

Scanner (Running)

Interface: wlan1

Background Scan

Start

Stop

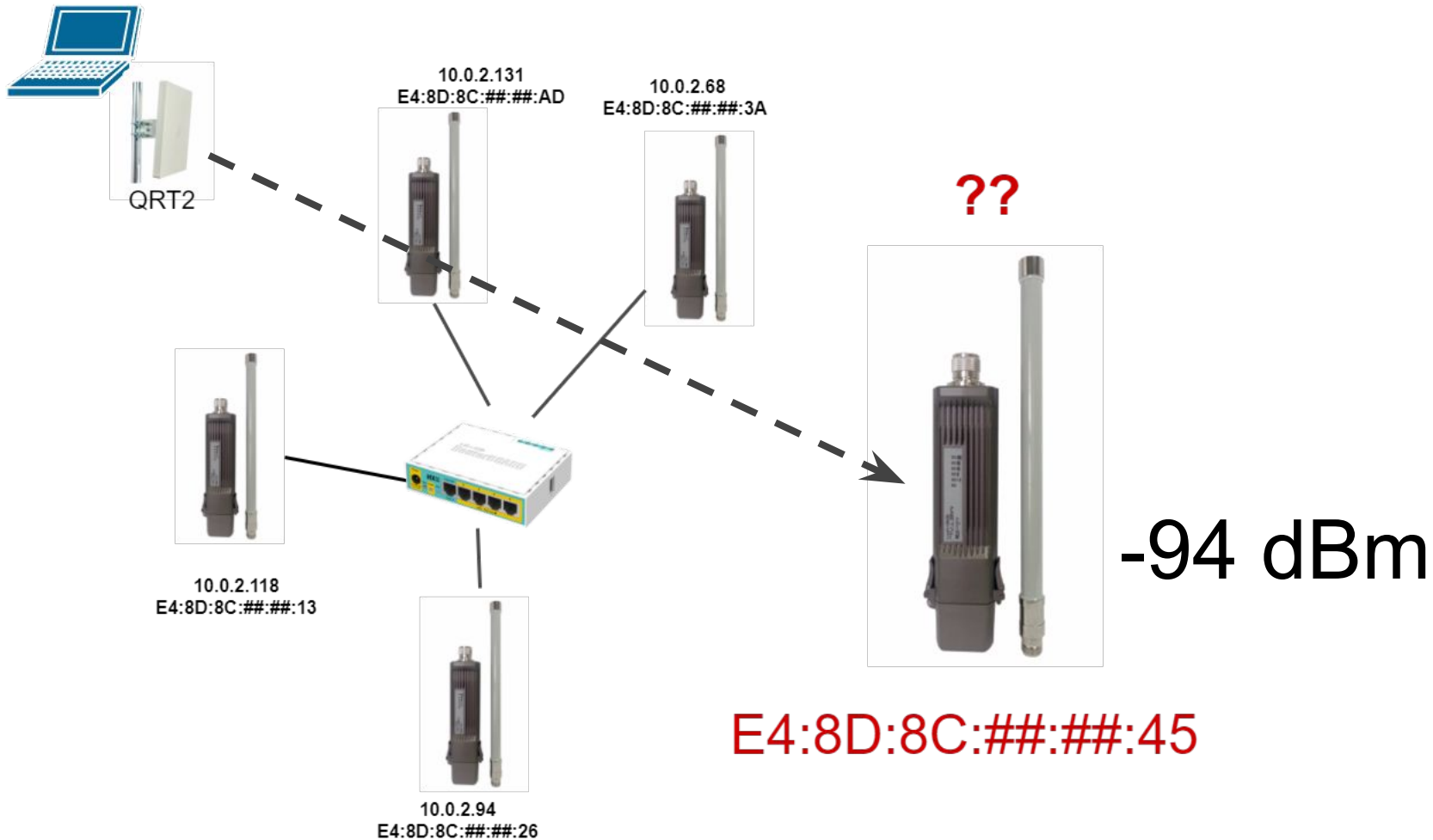
Close

Connect

New Window

	Address	SSID	Channel	Signal...	Noise ...	Signal To...	Radio Na...	Router...	
APRB	E4:8D:8C: :13	M a_WiFi_Free	2412/20/g	-78	-110	32	E48D8C...	6.36.4	
APRB	E4:8D:8C: :AD	M a_WiFi_Free	2412/20/g	-80	-110	30	E48D8C...	6.36.4	
APRB	E4:8D:8C: :26	M a_WiFi_Free	2412/20/g	-81	-110	29	E48D8C...	6.36.4	
AP	00:0E:8F: :8A		2412/20/gn	-84	-110	26			
APRB	E4:8D:8C: :3B	M a_WiFi_Free	2412/20/g	-88	-110	22	E48D8C...	6.36.4	
AP	10:FE:ED: :41		2437/20/gn	-91	-115	24			
AP	C4:A8:1D: :18		2422/20/gn	-92	-114	22			
APRB	E4:8D:8C: :45	M a_WiFi_Free	2412/20/g	-94	-110	16	E48D8C...	6.36.4	

8 items



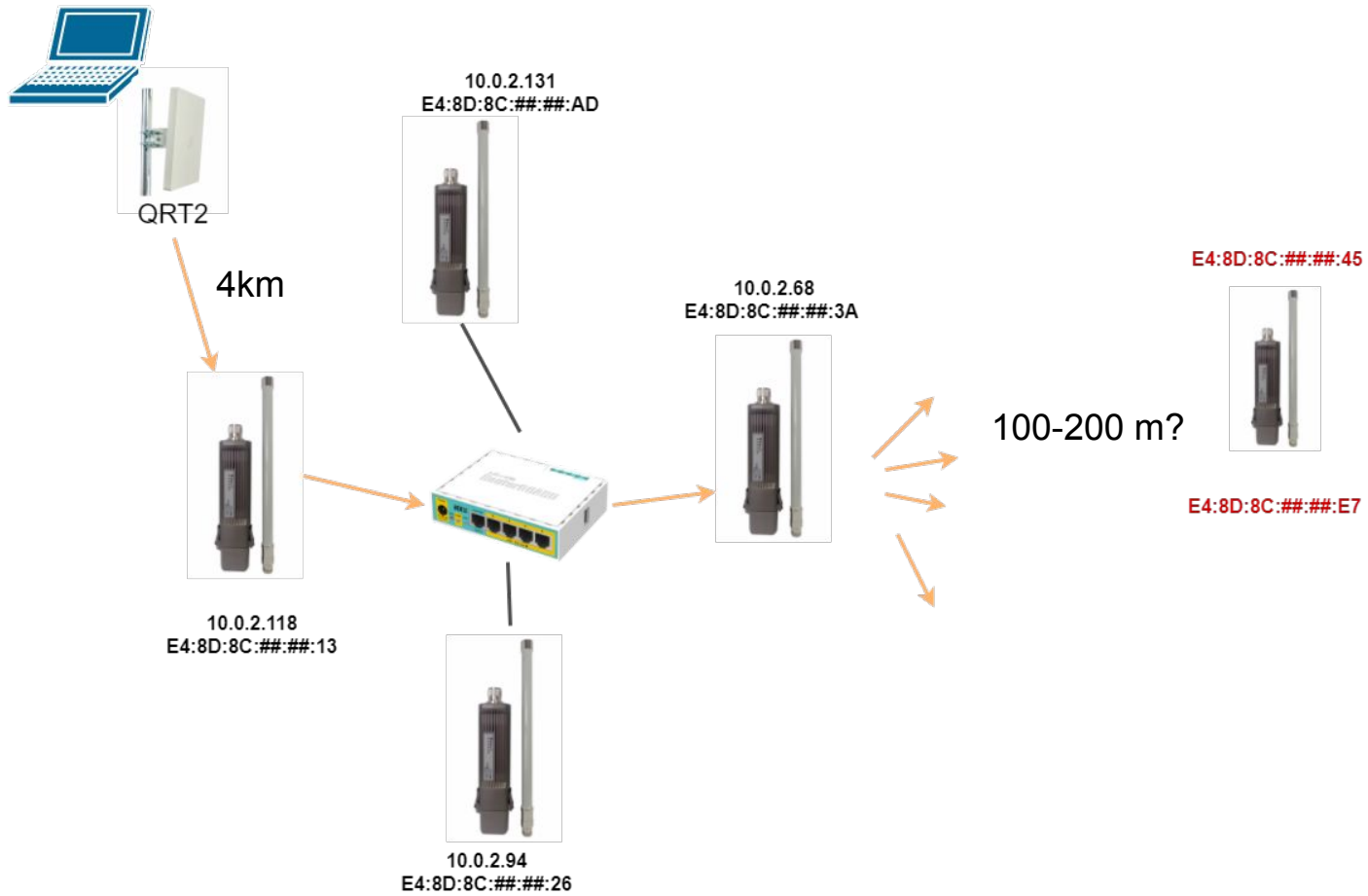
[Round 5]

Looking for the **missing**
RouterBoard access point



E4:8D:8C::#:#:45





Scanner (Running)

Interface: wlan1

Start

Stop

Close

Connect

New Window

	Address	SSID	Channel	Signal Stren...	Nois...	Sign...	Radio Name	Router...	
APRB	E4:8D:8C: :AD	M a_WiFi_Free	2412/20/g	-34	-106	72	E48D8C AD	6.36.4	
APRB	E4:8D:8C: :26	M a_WiFi_Free	2412/20/g	-41	-106	65	E48D8C 26	6.36.4	
APRB	E4:8D:8C: :3B	M a_WiFi_Free	2412/20/g	-48	-106	58	E48D8C 3B	6.36.4	
APRB	E4:8D:8C: :45	M a_WiFi_Free	2412/20/g	-57	-106	49	E48D8C 45	6.36.4	
APRB	E4:8D:8C: :31	M a_WiFi_Free	2412/20/g	-64	-106	42	E48D8C 31	6.36.4	
APRB	E4:8D:8C: :E7	M a_WiFi_Free	2412/20/g	-68	-106	38	E48D8C E7	6.36.4	
APRB	E4:8D:8C: :F4	M a_WiFi_Free	2412/20/g	-70	-106	36	E48D8C F4	6.36.4	
AP	00:0E:8F: :8A		2412/20/gn	-84	-106	22			
AP	10:FE:ED: :41		2437/20/gn	-90	-111	21			
AP	00:D2:AD: :AA		2422/20/gn	-91	-108	17			
AP	C4:A8:1D: :18		2422/20/gn	-92	-108	16			

11 items



QRT2

4km



10.0.2.118
E4:8D:8C:##:##:13

10.0.2.131
E4:8D:8C:##:##:AD



10.0.2.68
E4:8D:8C:##:##:3A



100-200 m?

E4:8D:8C:##:##:31



E4:8D:8C:##:##:45



E4:8D:8C:##:##:E7

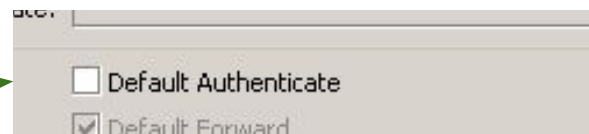
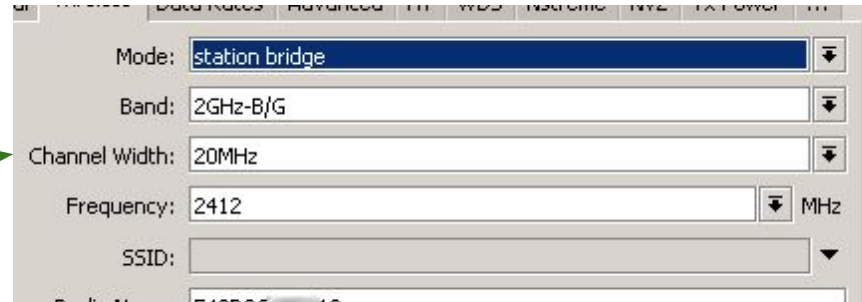
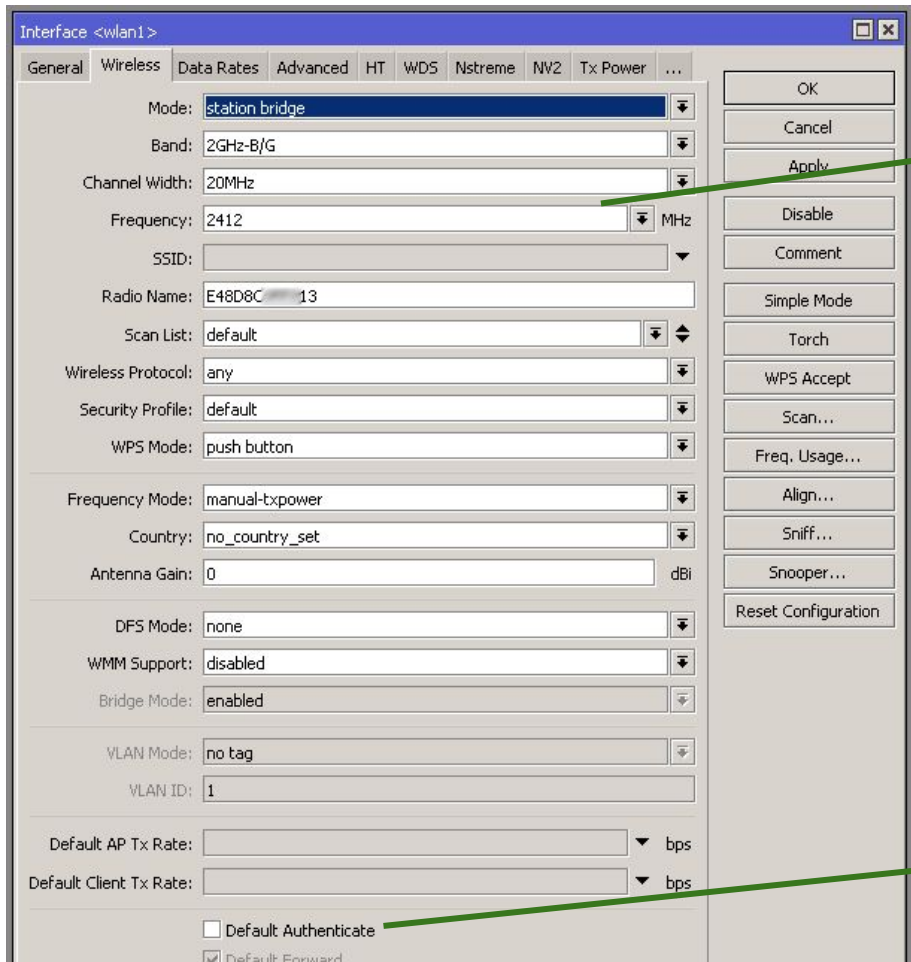


E4:8D:8C:##:##:F4



10.0.2.94
E4:8D:8C:##:##:26





Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles Channels

Reset

Radio Name	MAC Address	Interface	Uptime	AP	...	Last Activi...	Tx/Rx Signal
E48D8C:45	E4:8D:8C:45	wlan1	00:01:43	yes	no	5.010	-52/-43

1 item

Station Connect Rule <E4:8D:8C:45>

Interface: wlan1

MAC Address: E4:8D:8C:45

Connect

SSID: M...a_WiFi_Free

Area Prefix:

Signal Strength Range: -120..120

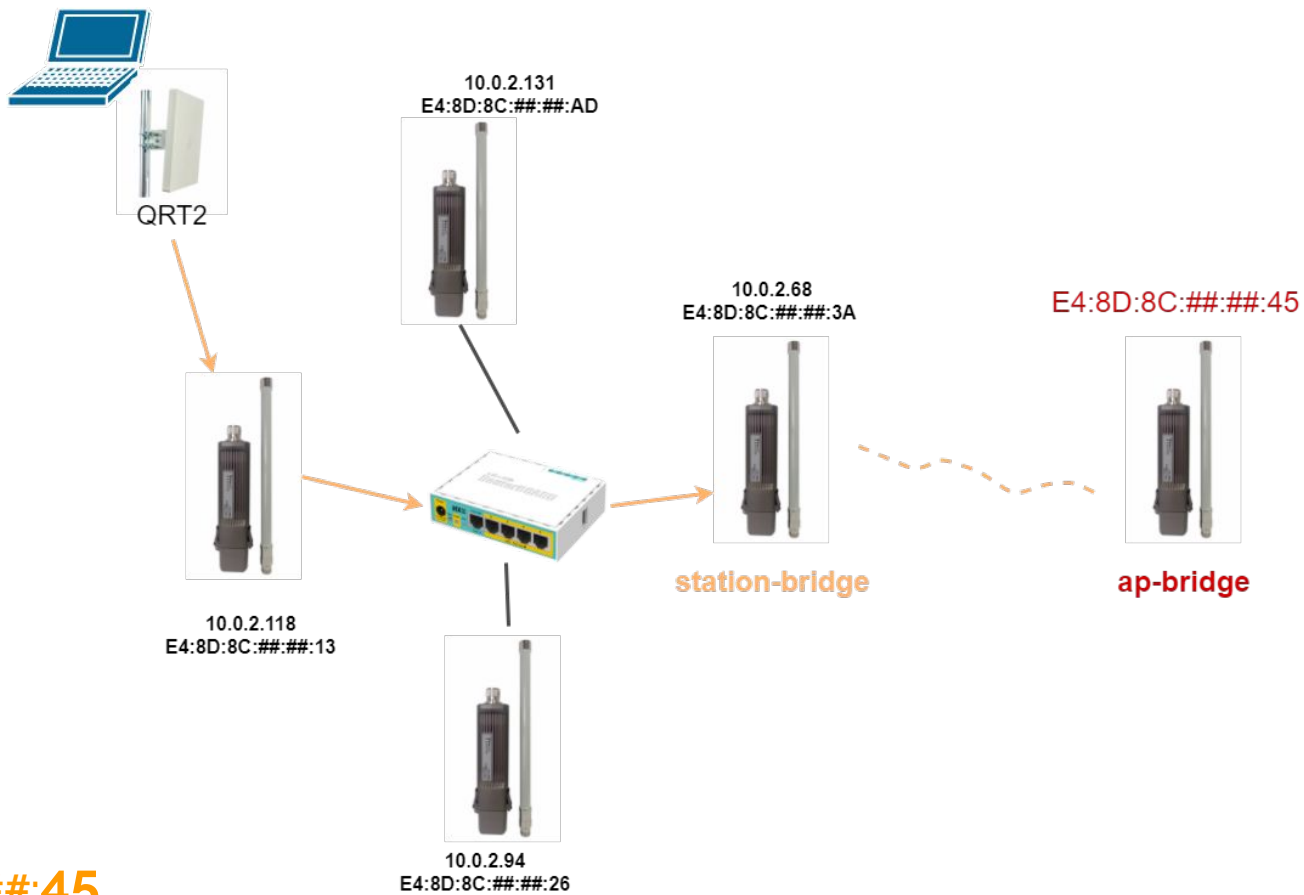
Wireless Protocol: any

Security Profile: default

enabled

OK Cancel Apply Disable Comment Copy Remove

E4:8D:8C:##:##:45



E4:8D:8C:##:##:45

Radio Name	MAC Address	Interface	Uptime	AP	...	Last
E48D8C 45	E4:8D:8C:###:45	wlan1	00:11:15	yes	no	

```
Terminal
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] >
[zabbix@MikroTik] > /to
Login: zabbix
Password:
Trying E4:8D:8C:###:4
Welcome back!
[zabbix@MikroTik] >
```

```
Terminal

[?] Gives the list of available commands
command [?] Gives help on the command and list of a
[Tab] Completes the command/word. If the input
a second [Tab] gives possible options

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

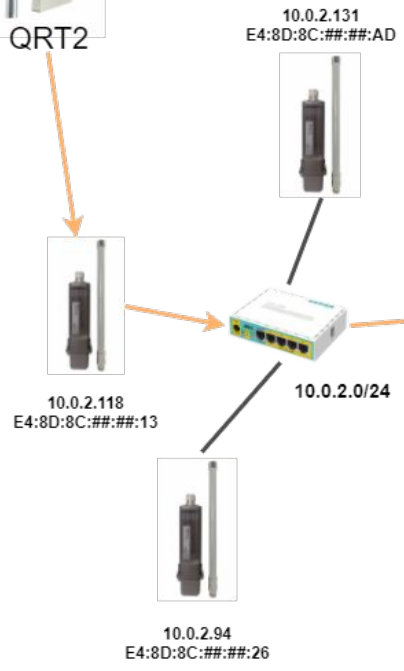
[zabbix@MikroTik] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 D 10.0.1.50/24 10.0.1.0 bridge
[zabbix@MikroTik] >
```

10.0.1.0/24

E4:8D:8C:###:45



QRT2



10.0.2.68
E4:8D:8C:##:##:3A



station-bridge



E4:8D:8C:##:##:44
10.0.1.54



ap-bridge

E4:8D:8C:##:##:30
10.0.1.78



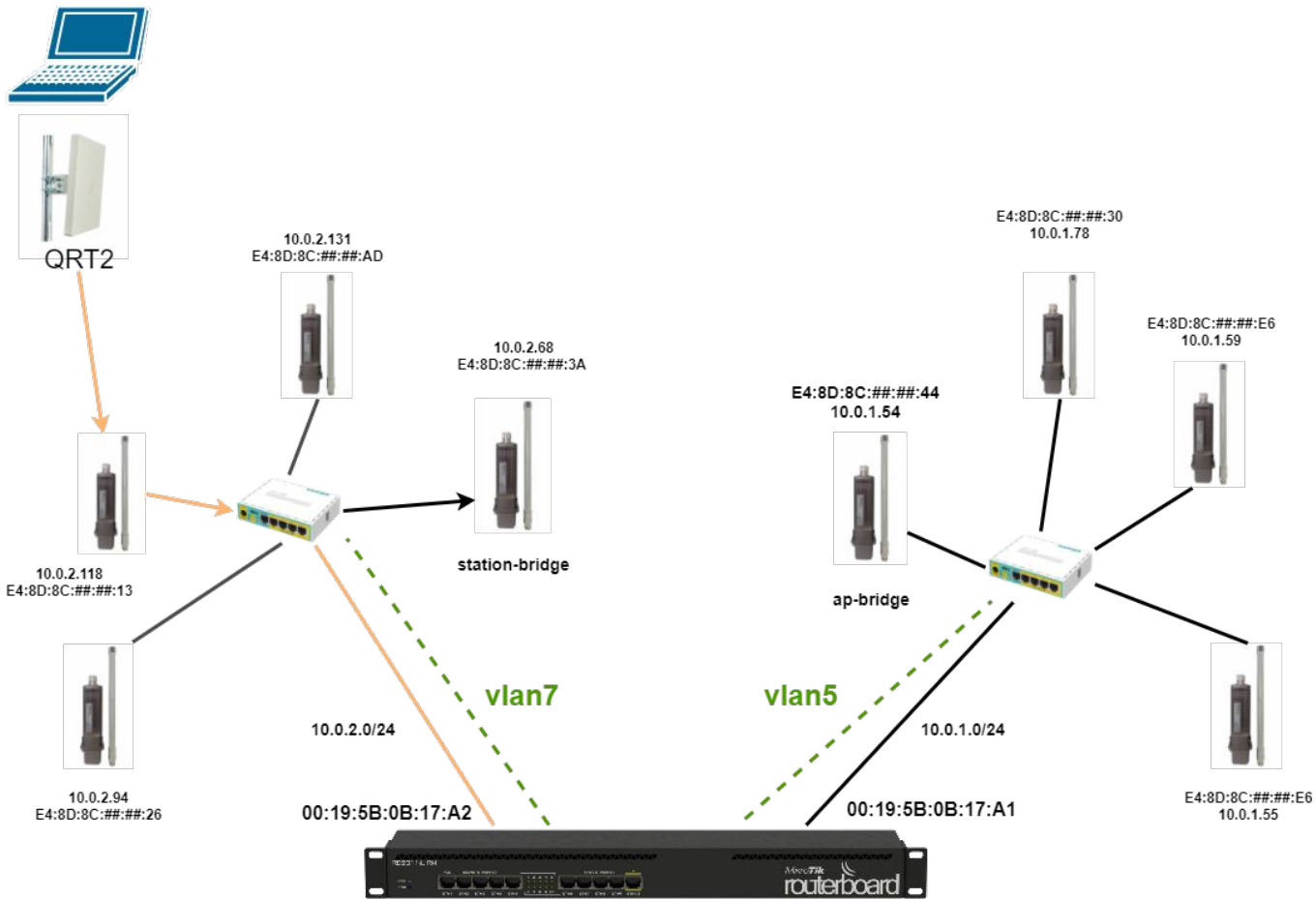
E4:8D:8C:##:##:E6
10.0.1.59



E4:8D:8C:##:##:E6
10.0.1.55



10.0.1.0/24



D-Link DIR-2011

Nikita Tarikin

Certified network engineer
MikroTik PRO, Russia 



Contact me

Web: tarikin.com

E-mail: nikita@tarikin.com

Facebook: fb.com/tarikin

Instagram: @tarikin

Telegram: t.me/tarikin

