The real story

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

Nikita Tarikin

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%

Nikita Tarikin

Contact me

Web: tarikin.com

E-mail: nikita@tarikin.com

Facebook: fb.com/tarikin

Instagram: @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 ...

– – –

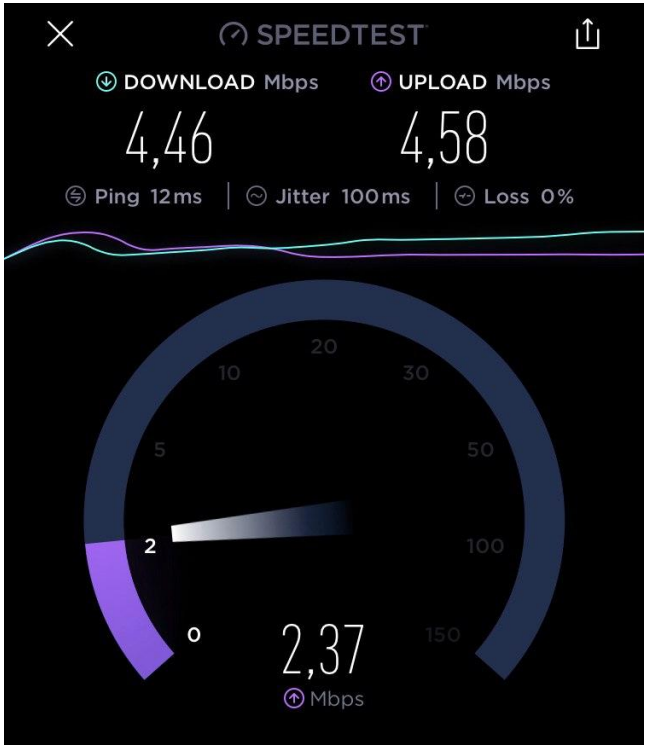
Reserved a private table in restaurant:

- 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..

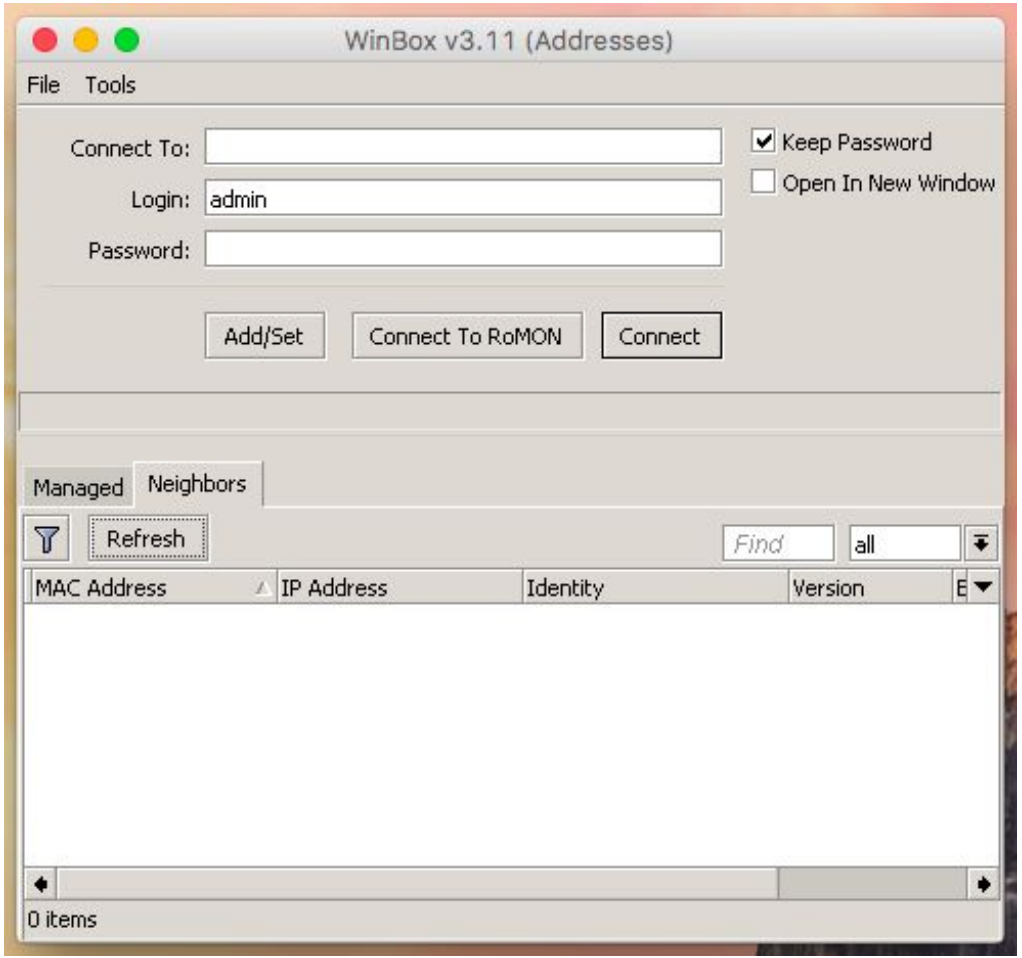
RouterBoard ?

```
arp -a
```

gw: 10.0.2.1

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

D-Link.



[Round 2]

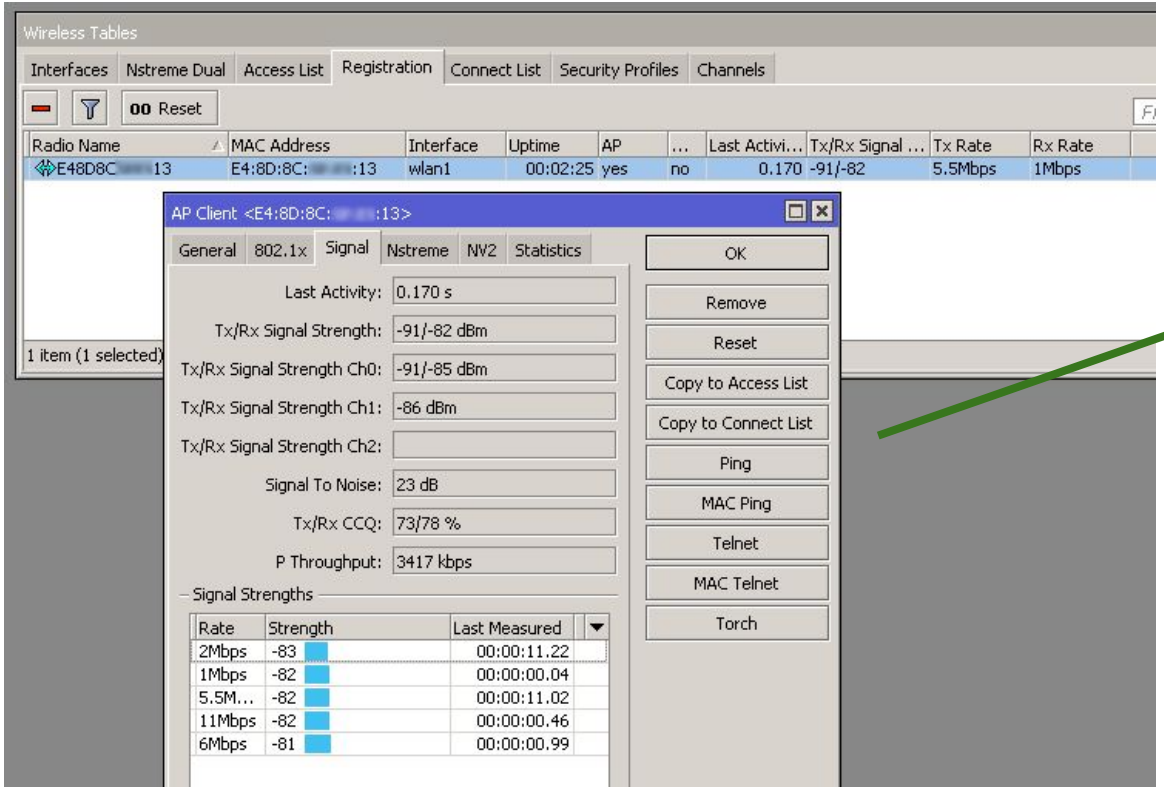
Aiming the target

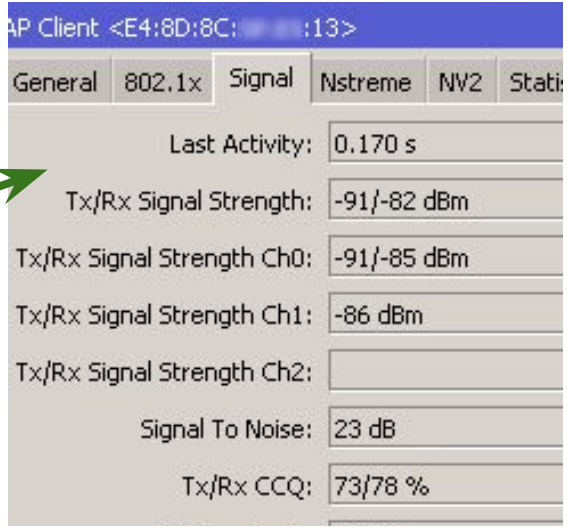
Always on WiFi enabled: false

Always on WiFi enabled: connecting ...

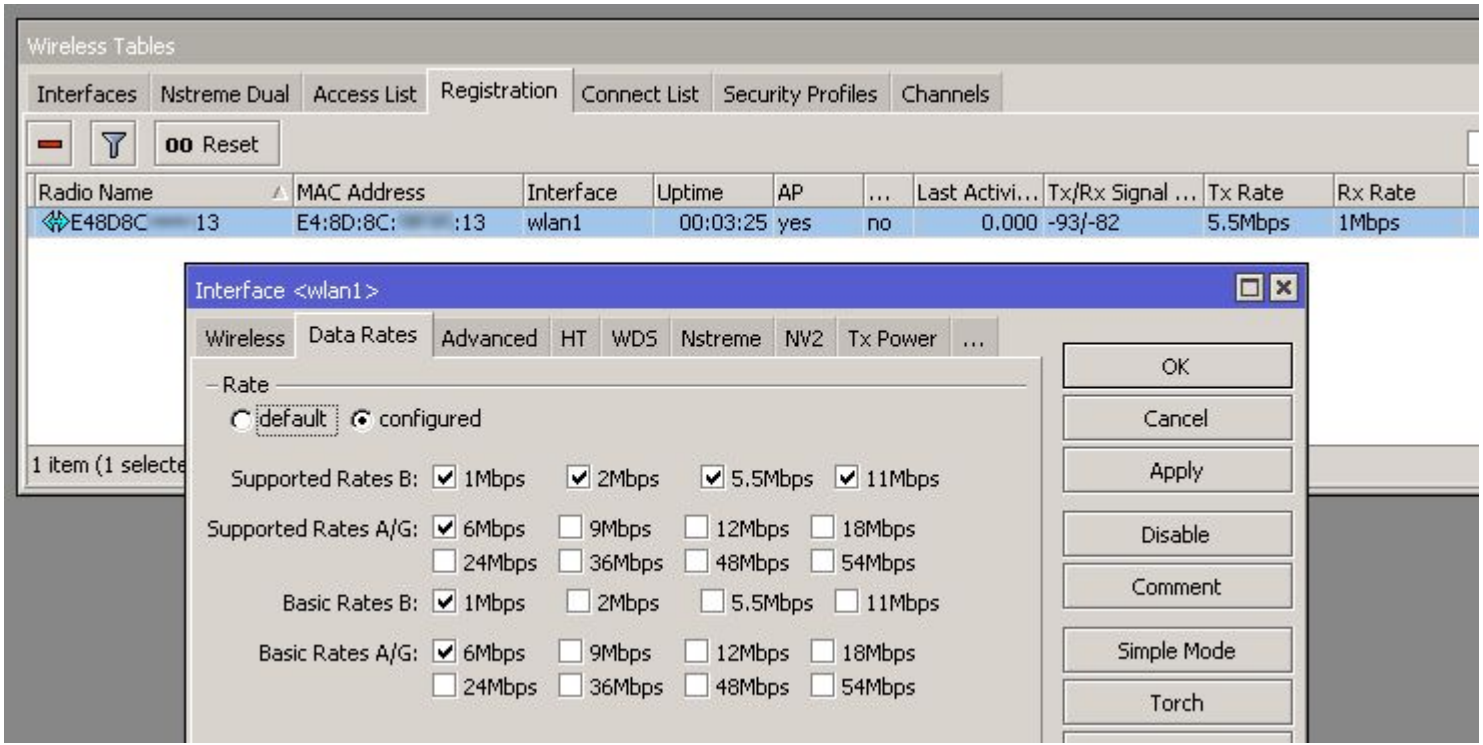
MikroTik SXT Lite2. I always keep it in my backpack.

Always on WiFi enabled: CONNECTED!



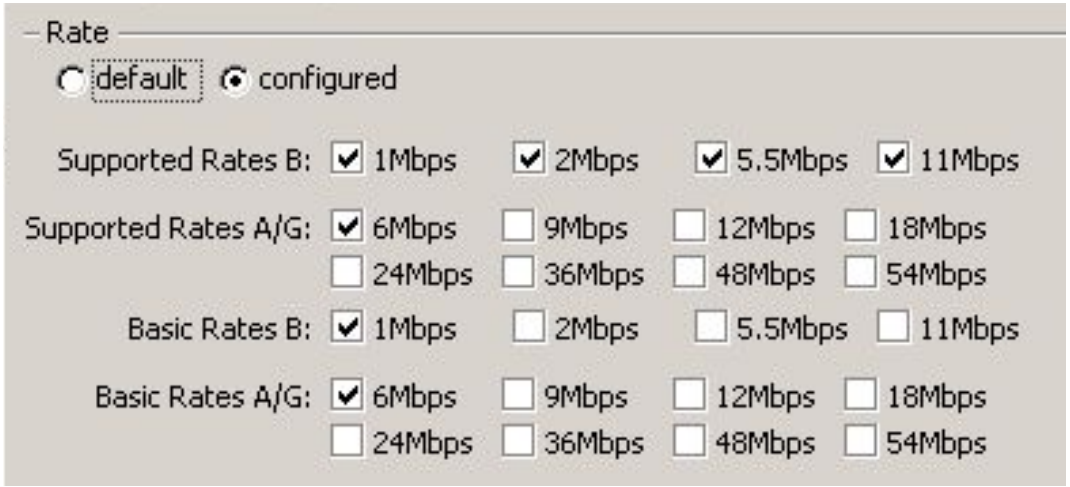


Always on WiFi enabled: CONNECTED!



Always on WiFi enabled: CONNECTED!

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

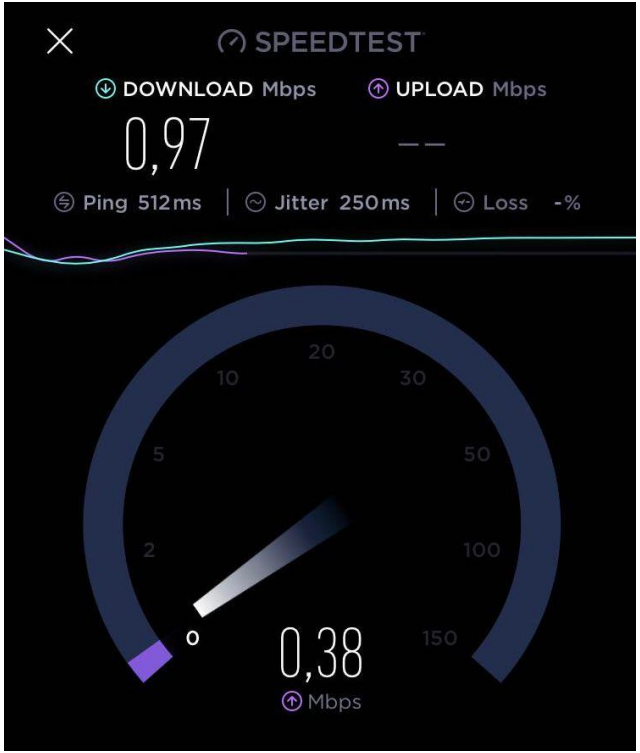


Always on WiFi enabled: TRUE!

– – –

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

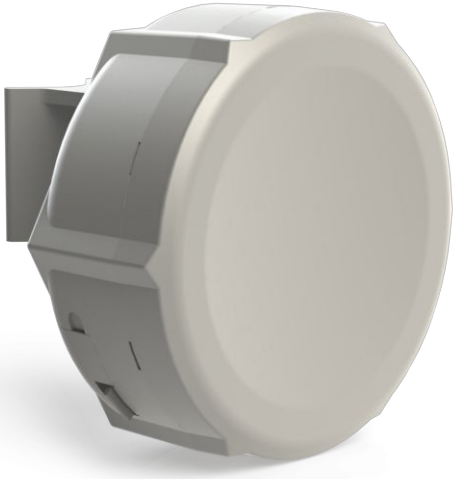
[Round 3]

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!

VS

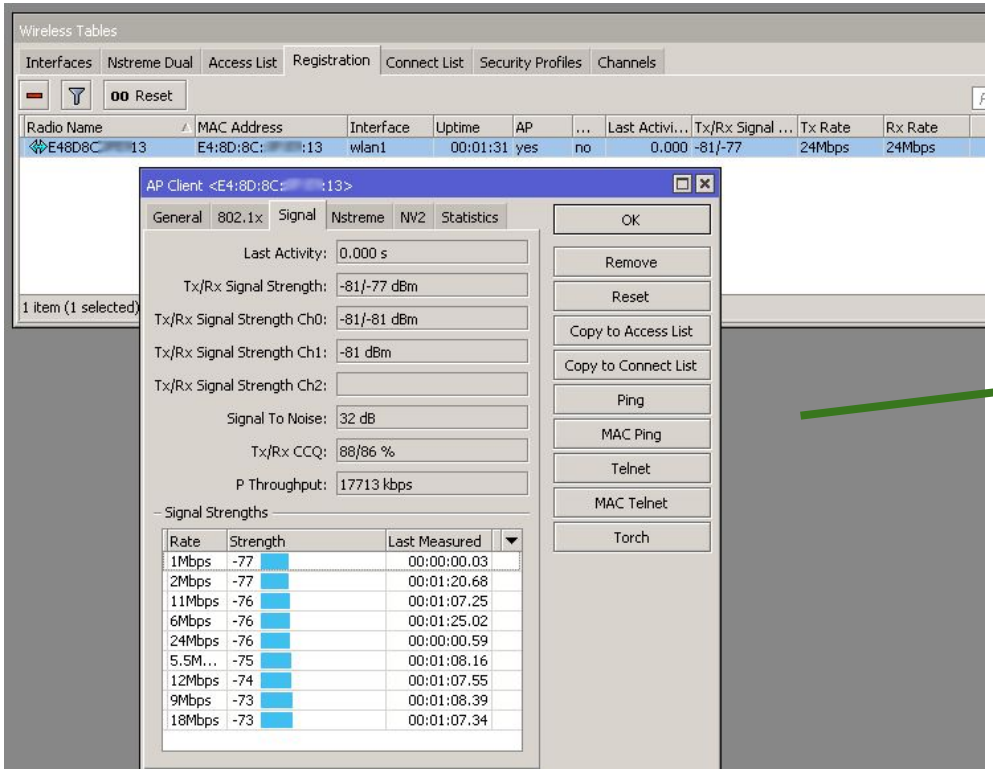
SXT Lite2

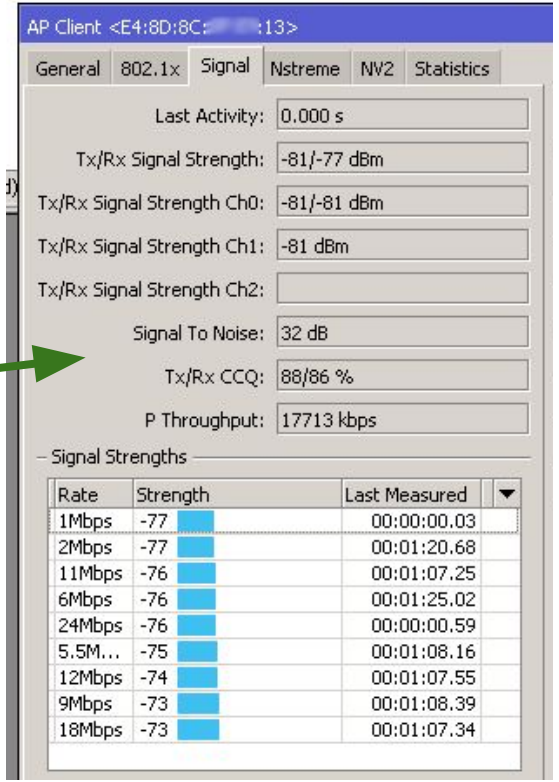
Tx-power:	27 dBm (500mW)
Antenna gain:	10 dBi
Beam:	60 degree

QRT 2

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

Always on WiFi enabled: 2 Mbit/s





4.5 Mbit/sec

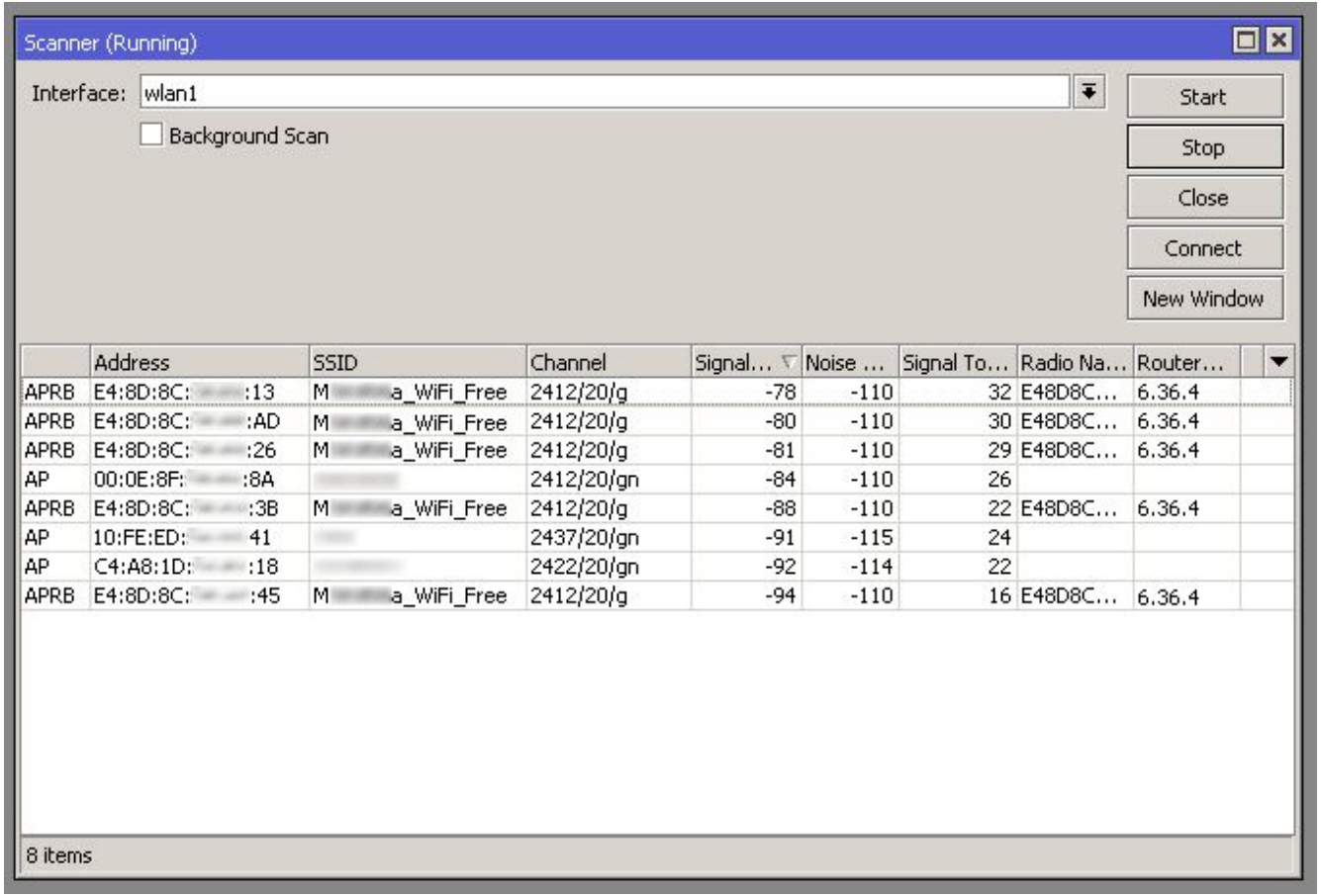
Speedtest:

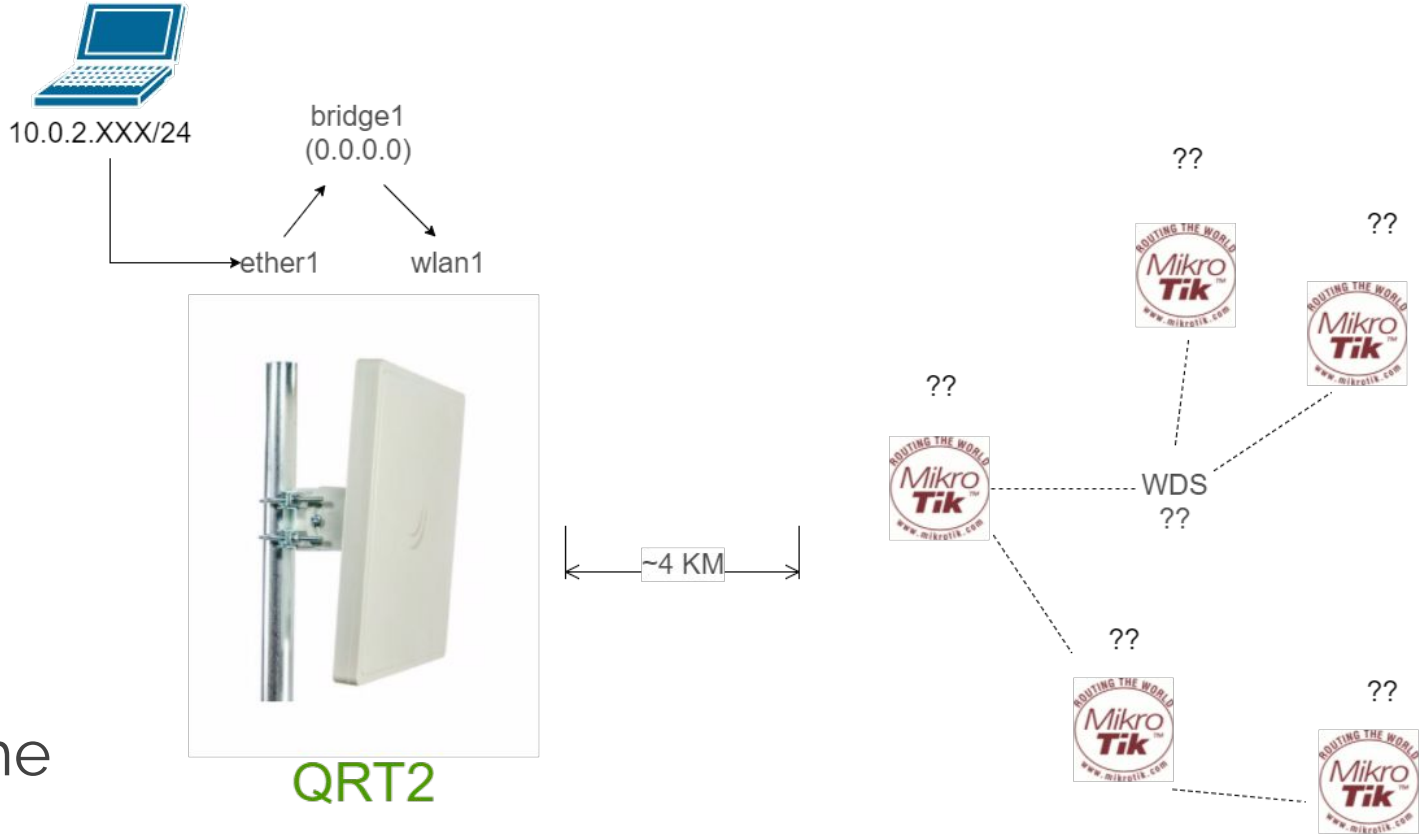
Download: 4.46Mbit/sec
Upload: 4.58Mbit/sec
Ping: 12ms
Jitter: 100ms

[Round 4]

Audit

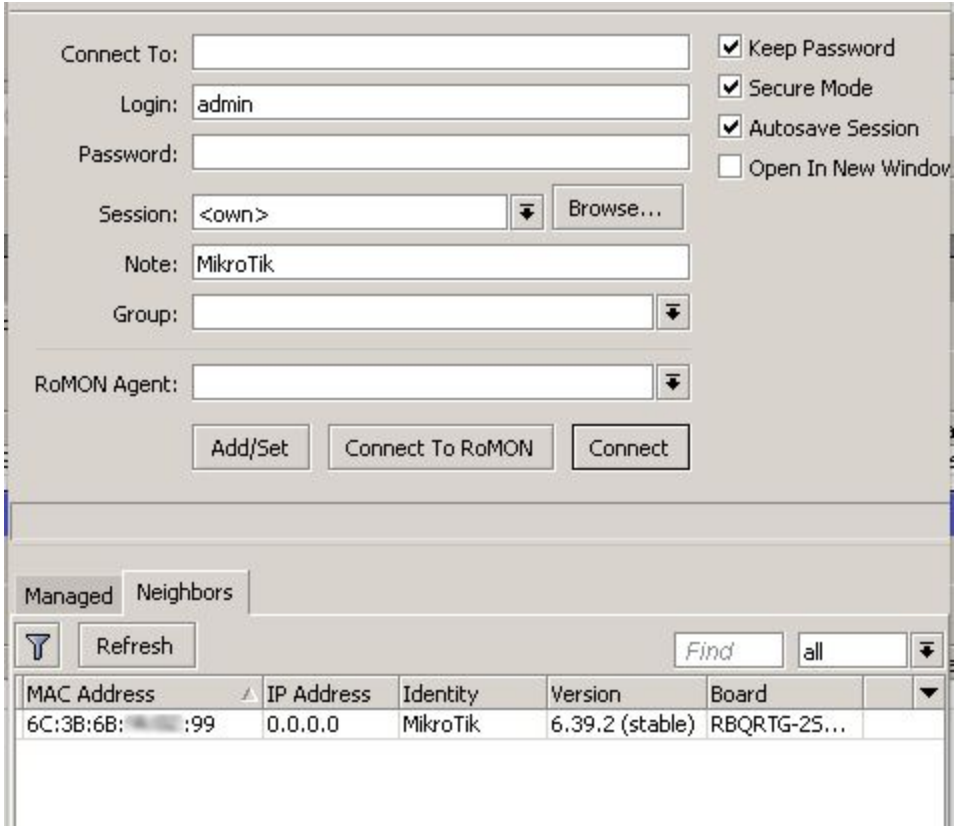
Let's see what's under the hood ...





Under the hood ...

Under the hood ...



File Edit View Insert Format Data

100% £ % .0

fx 10.0.2.118

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

QRT2

~4 KM

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

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

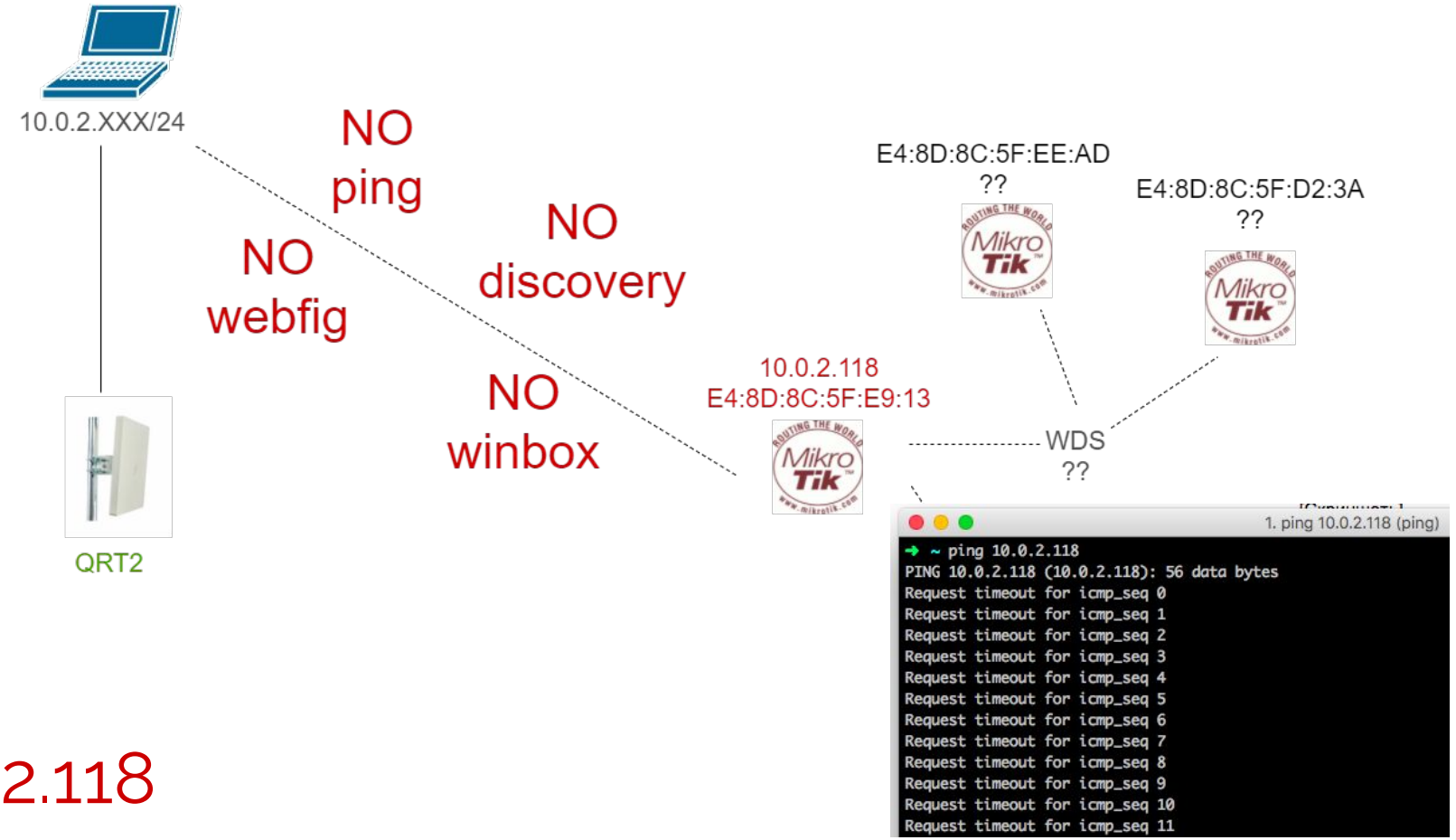
E4:8D:8C:##:##:3A
??

WDS
??

??

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

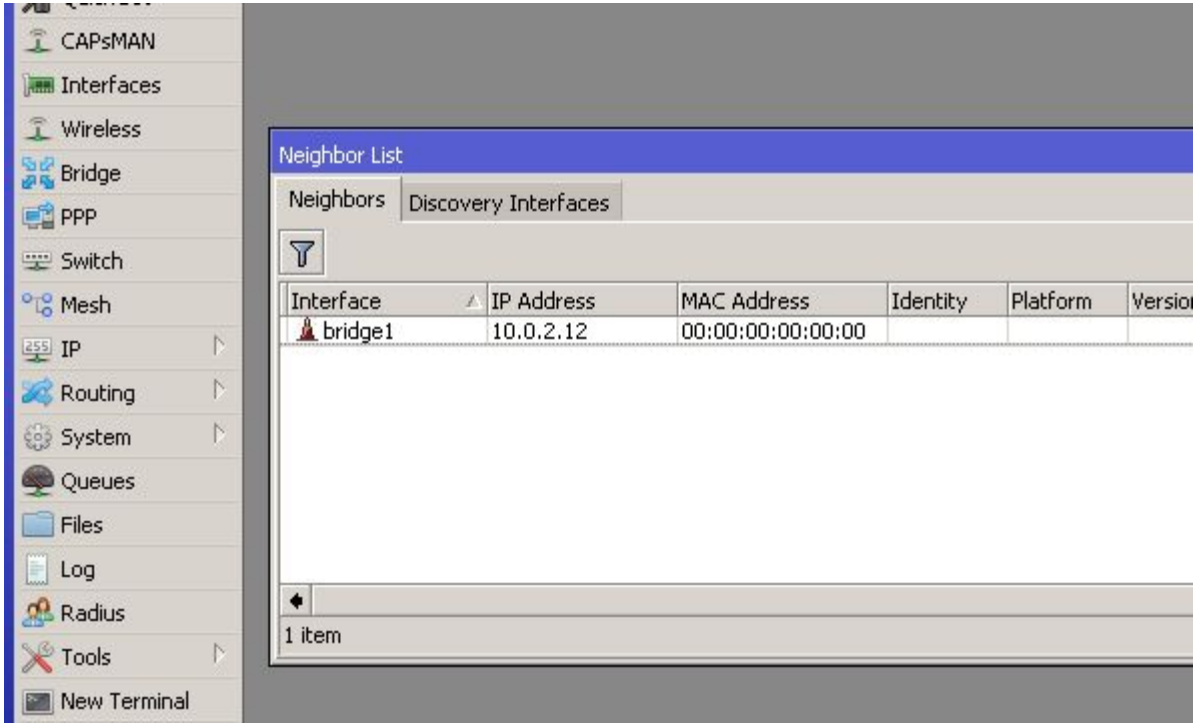
Nikita Tarikin


10.0.2.XXX/24
NO ping
NO webfig
NO discovery
NO winbox
E4:8D:8C:5F:EE:AD
??
E4:8D:8C:5F:D2:3A
??
10.0.2.118
E4:8D:8C:5F:E9:13
WDS
??
QRT2
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

10.0.2.118

QRT 2

NO DISCOVERY



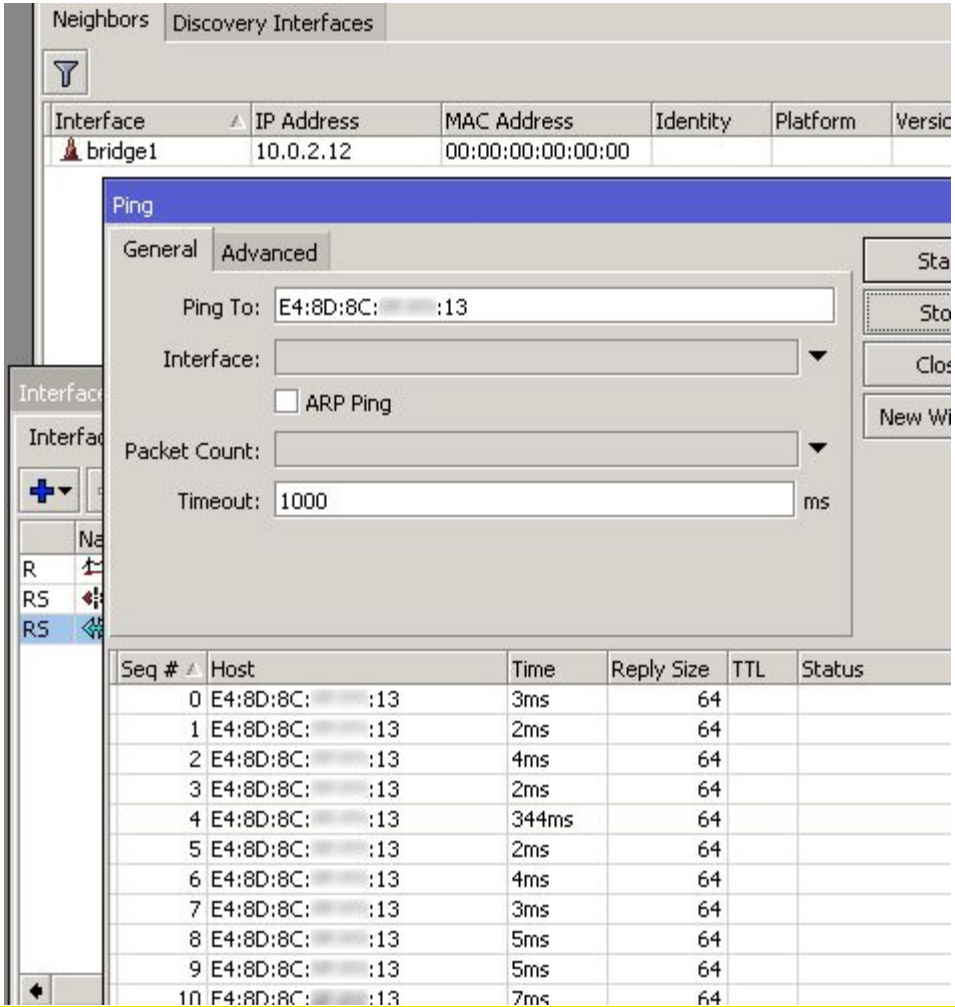
10.0.2.118

RouterOS MAC PING

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

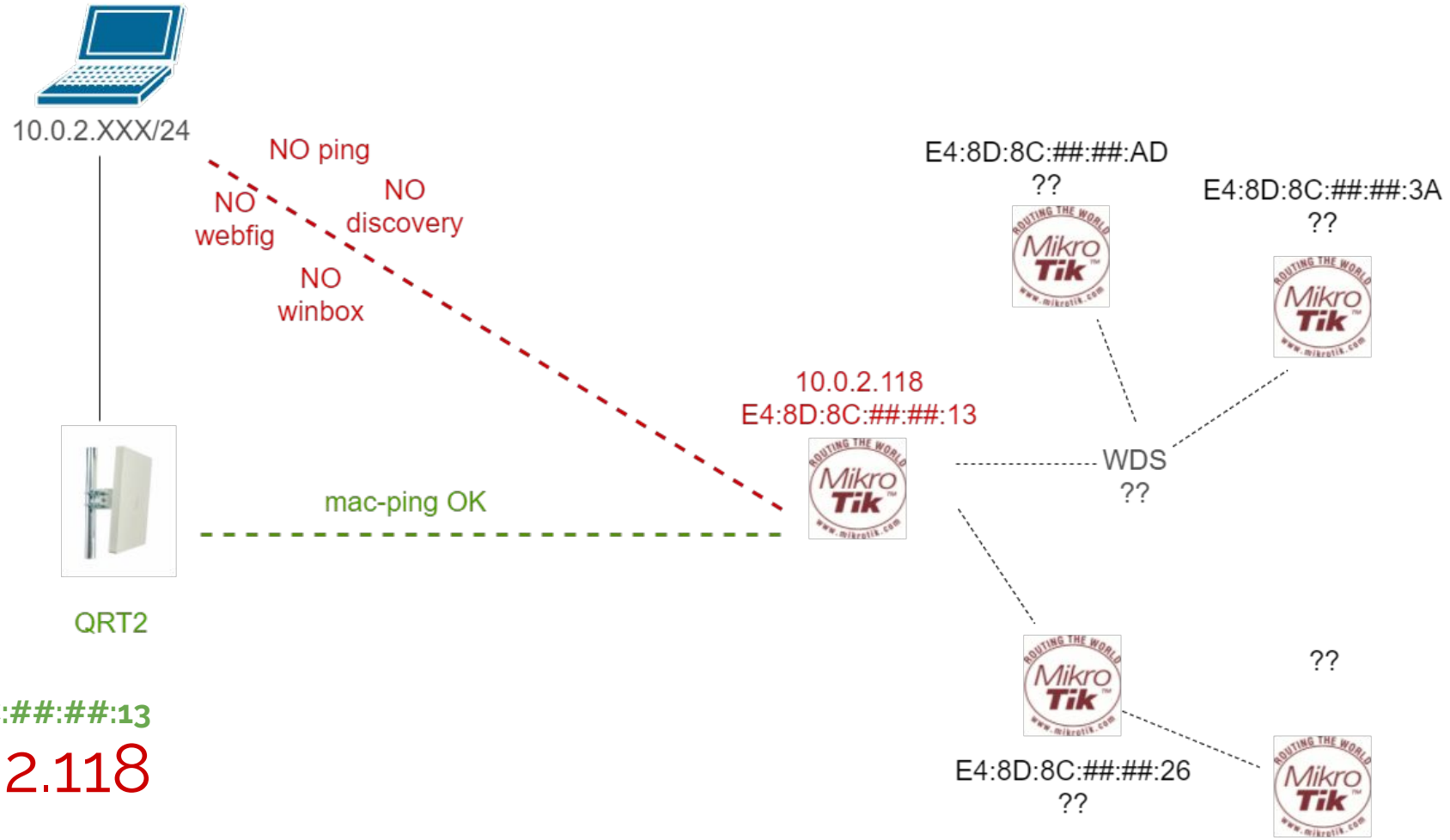
10.0.2.118

Nikita Tarikin



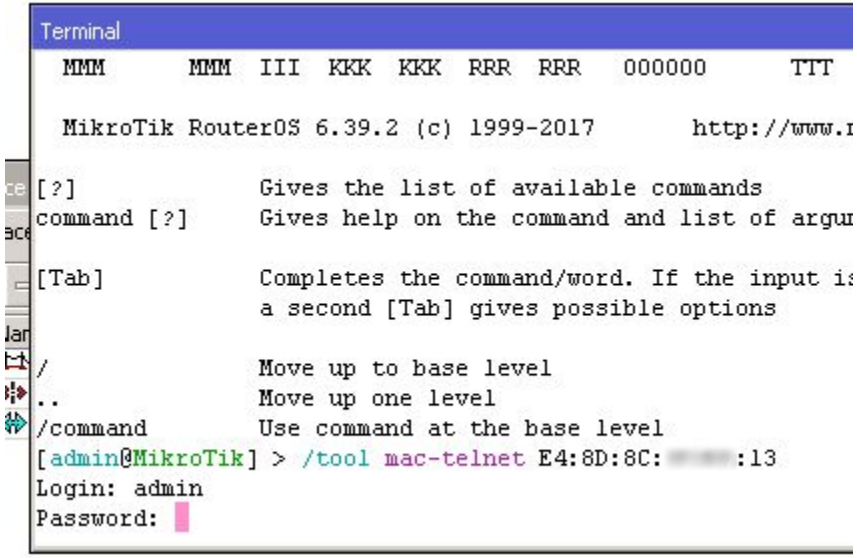
E4:8D:8C:##:##:13

10.0.2.118



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

10.0.2.118



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

10.0.2.118

User: admin

Password: Admin@123

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

10.0.2.118

Terminal

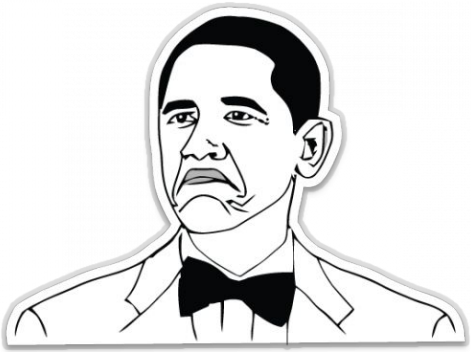
```
  MMM      MMM  III  KKK  KKK  RRR  RRR   000000      TTT

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

[?]             Gives the list of avai
command [?]     Gives help on the comm

[Tab]           Completes the command/
                a second [Tab] gives p

/               Move up to base level
..              Move up one level
/command        Use command at the base
[admin@MikroTik] > /tool mac-telnet E4-
Login: admin
Password:
```

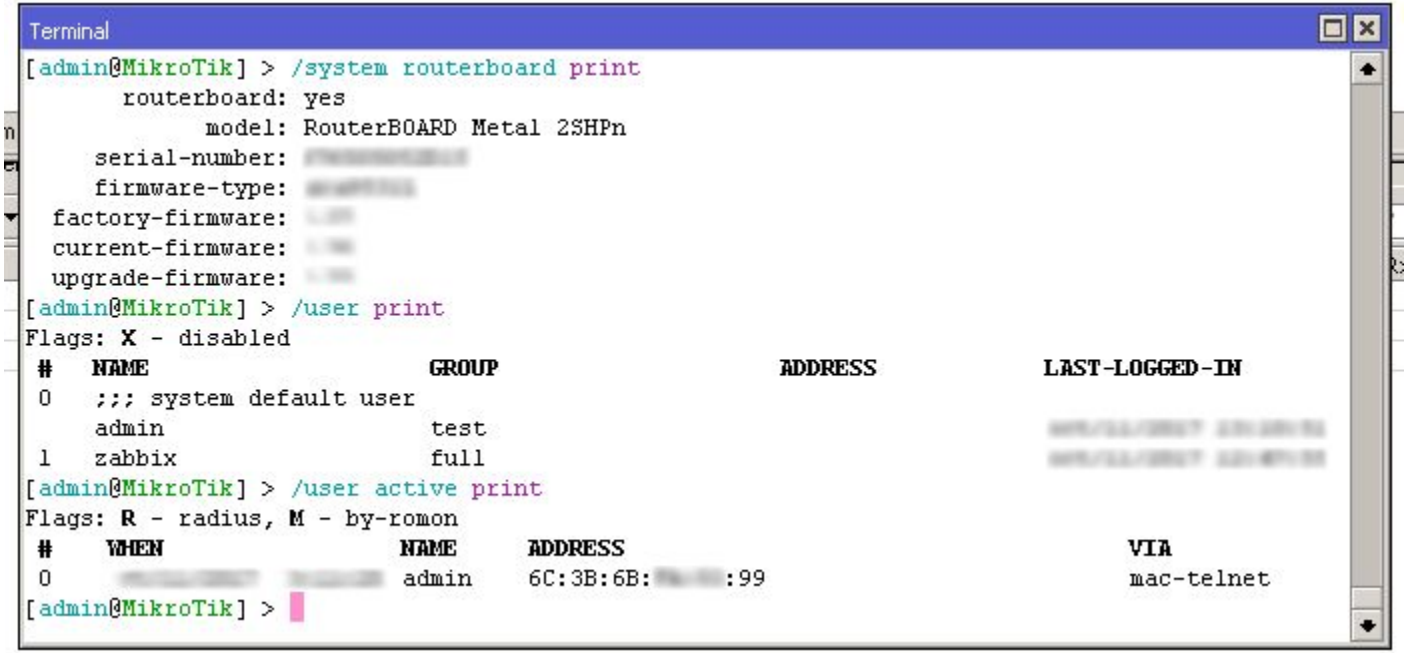
Terminal

```
  MikroTik RouterOS 6.36.4 (c) 1999-2016       htt

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

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

/               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

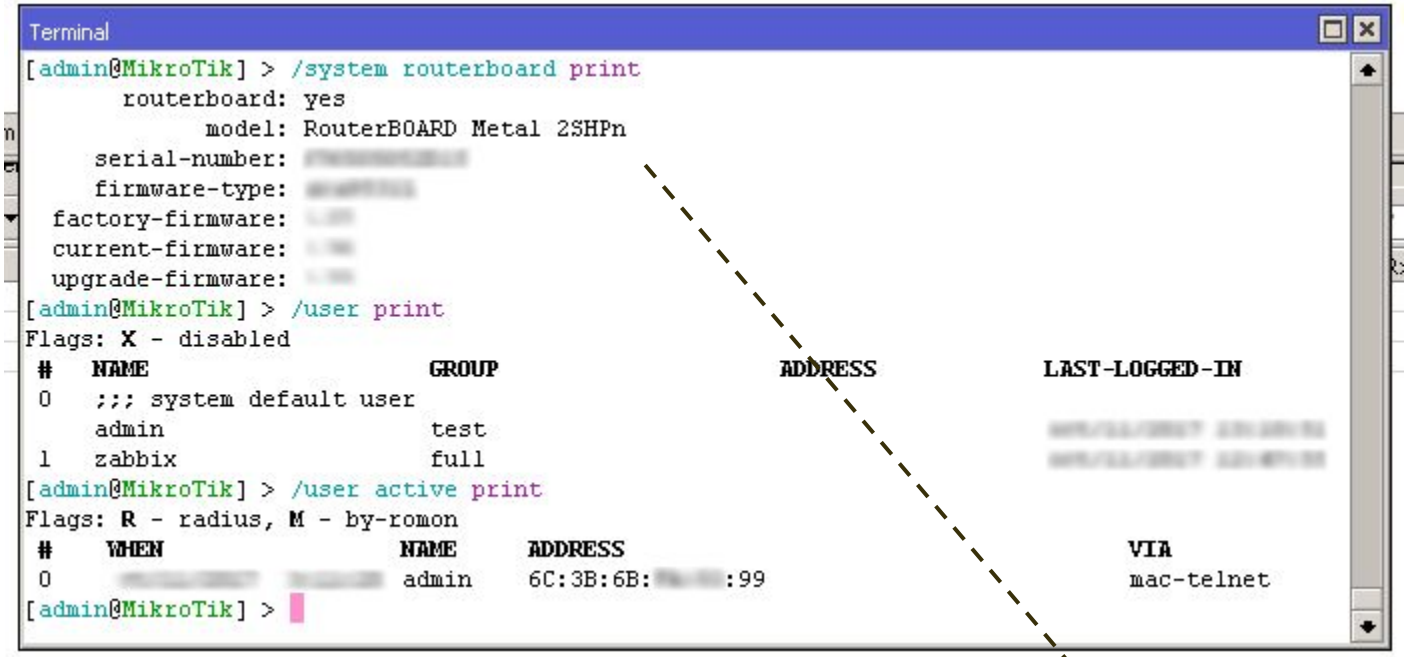
10.0.2.118





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

10.0.2.118



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

10.0.2.118

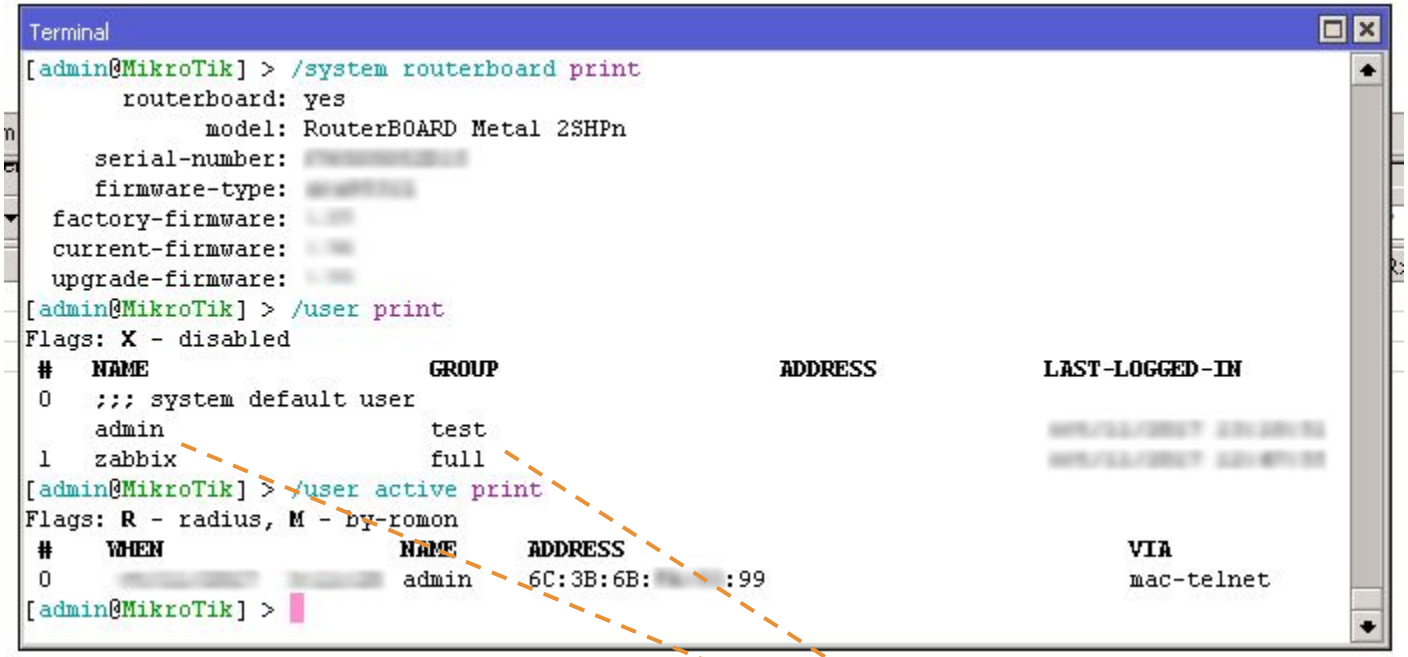
RouterBoard
Metal 2SHPn

RouterBoard
RBMetal2SHPn

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

10.0.2.118

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

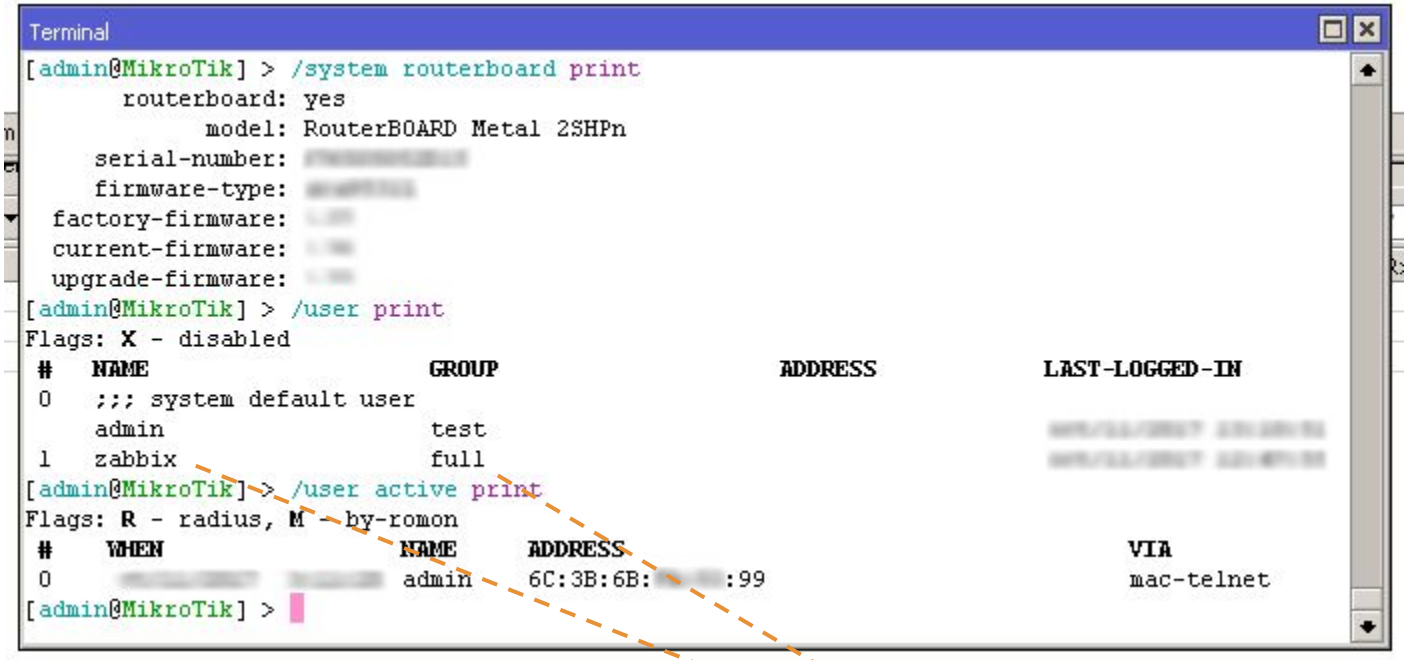


E4:8D:8C:##:##:13

10.0.2.118

User: admin

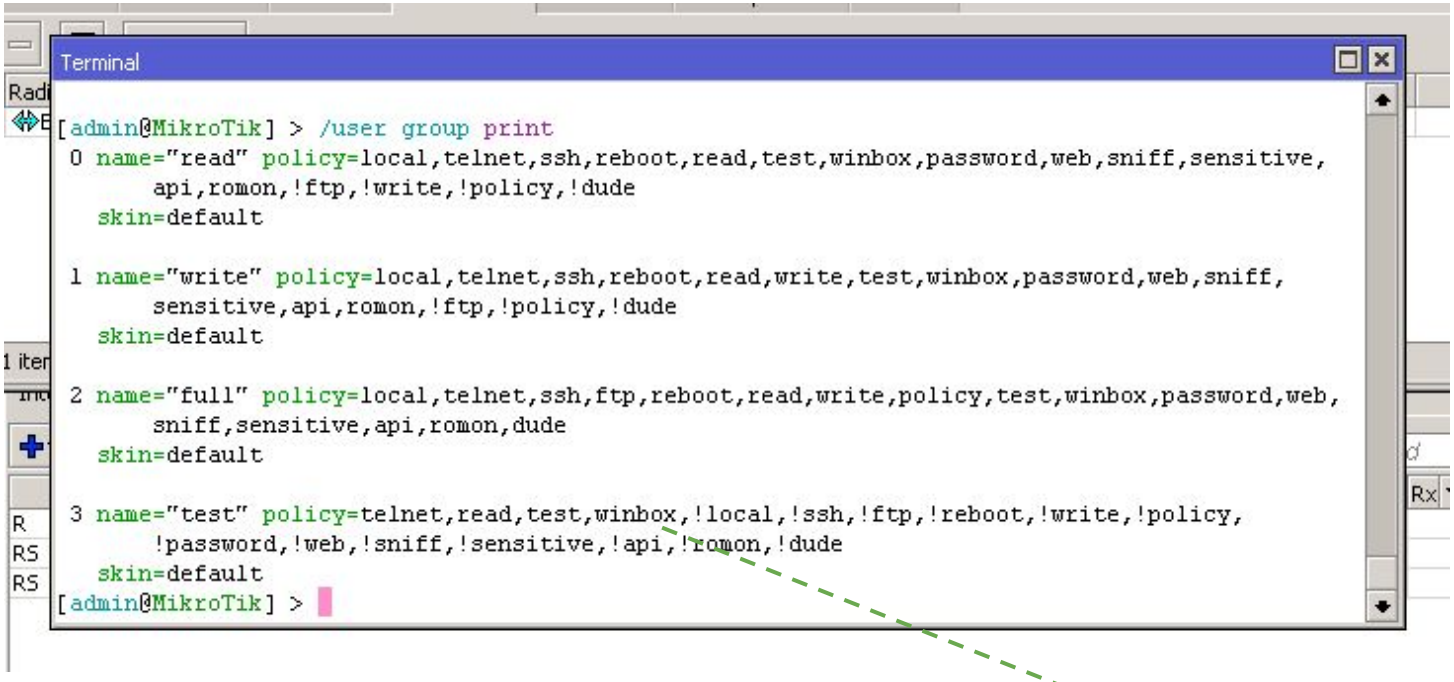
Group: **test ??**



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

10.0.2.118

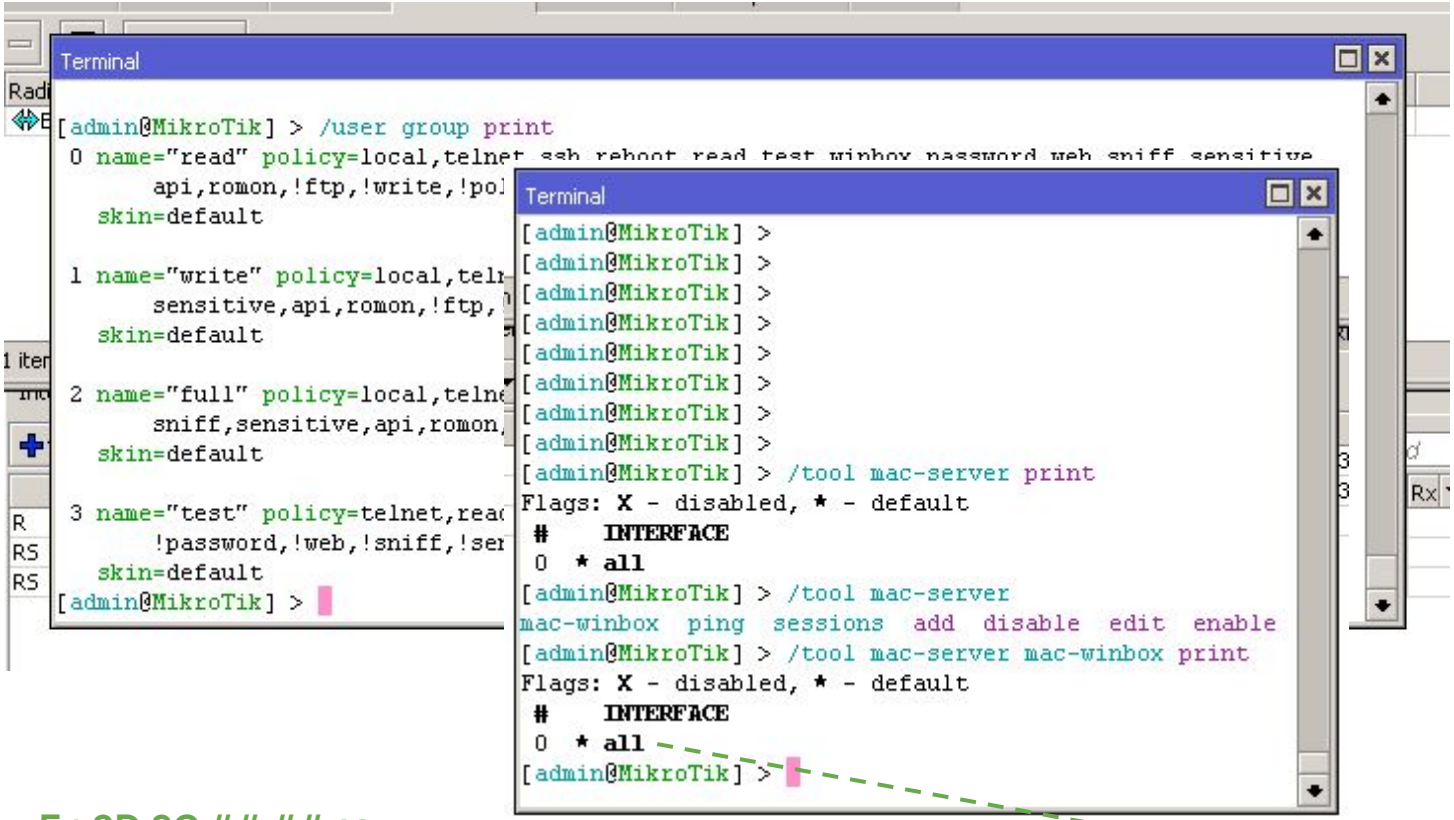
User: zabbix
Group: full



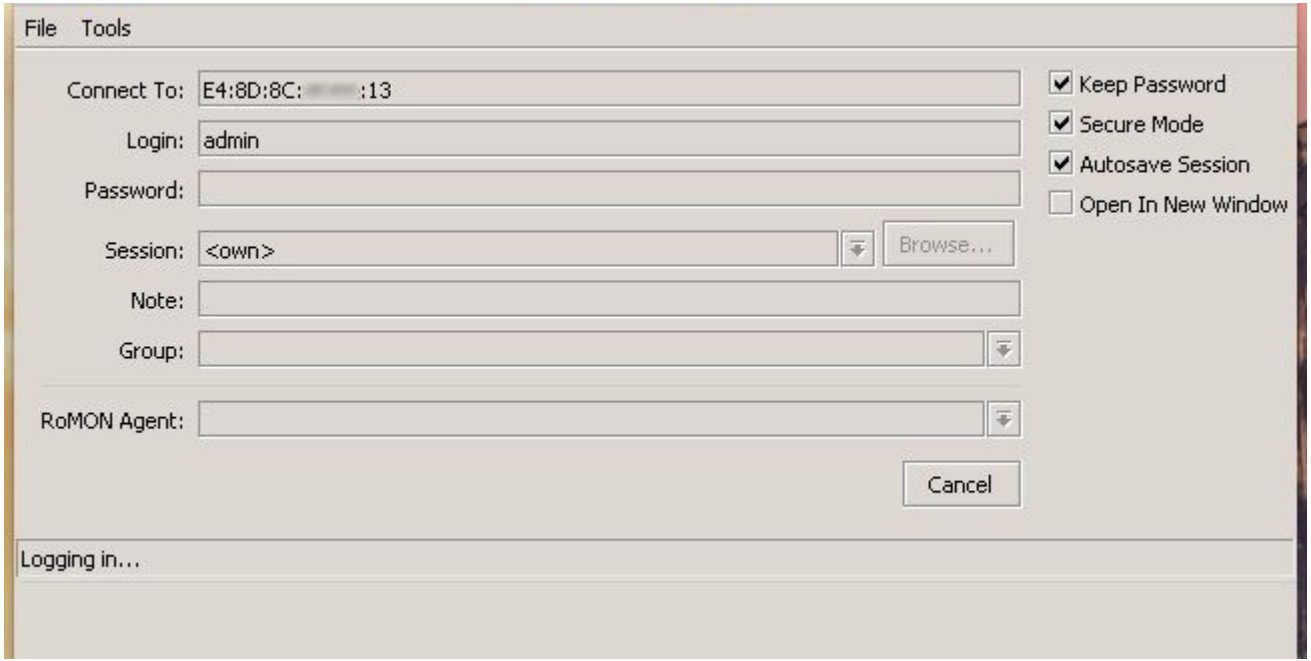
E4:8D:8C:##:##:13

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,!pol
skin=default
1 name="write" policy=local,teln
sensitive,api,romon,!ftp,
skin=default
2 name="full" policy=local,telne
sniff,sensitive,api,romon,
skin=default
3 name="test" policy=telnet,read
!password,!web,!sniff,!ser
skin=default
[admin@MikroTik] >
Terminal
[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

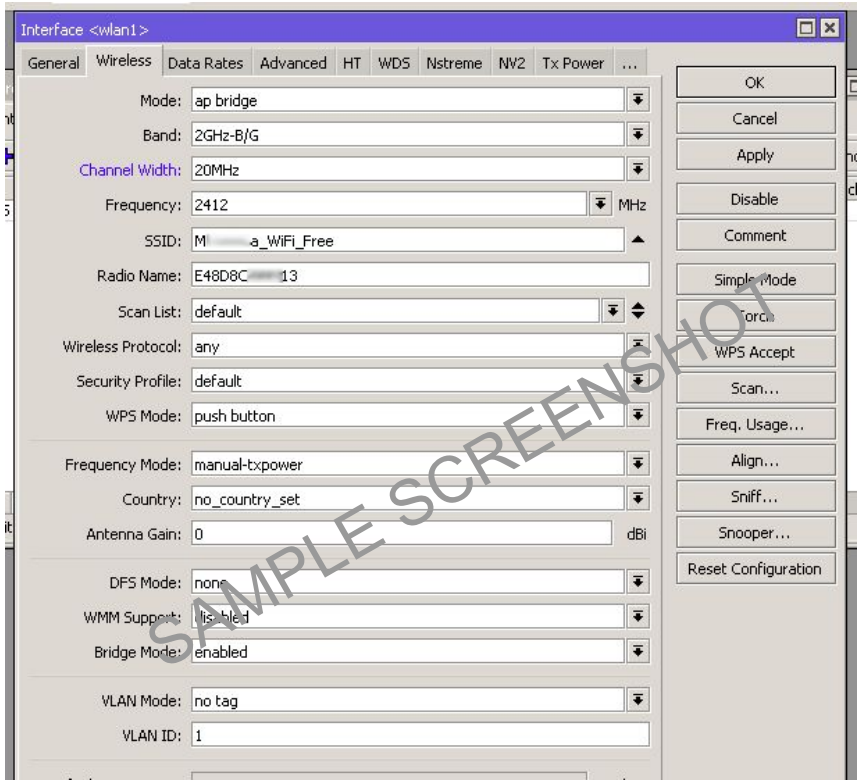
Continue to Winbox

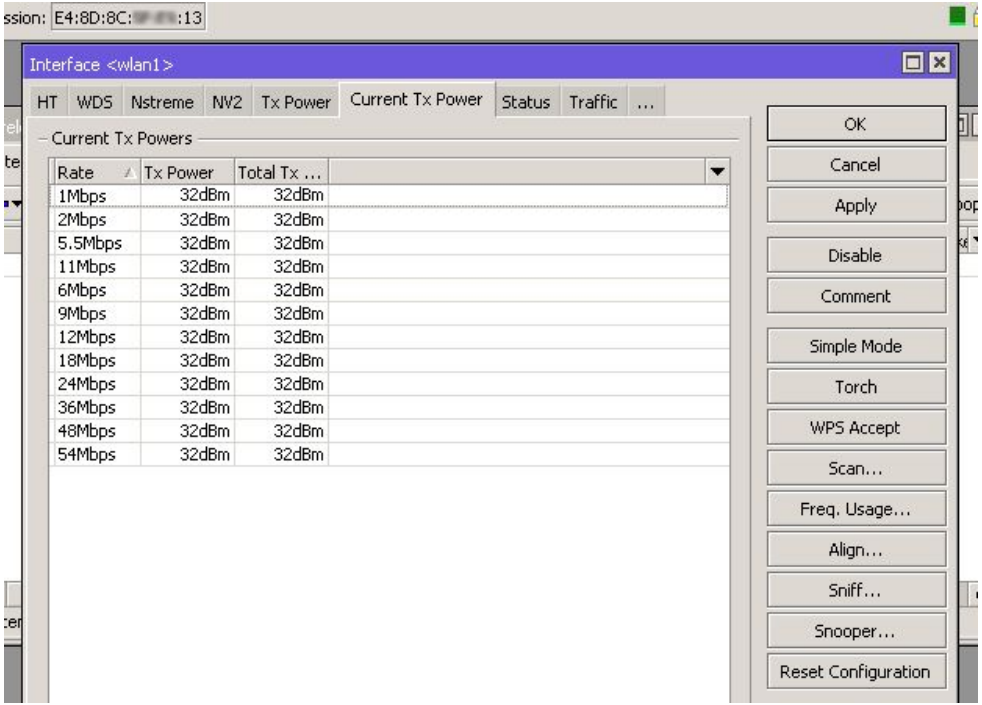


E4:8D:8C:##:##:13

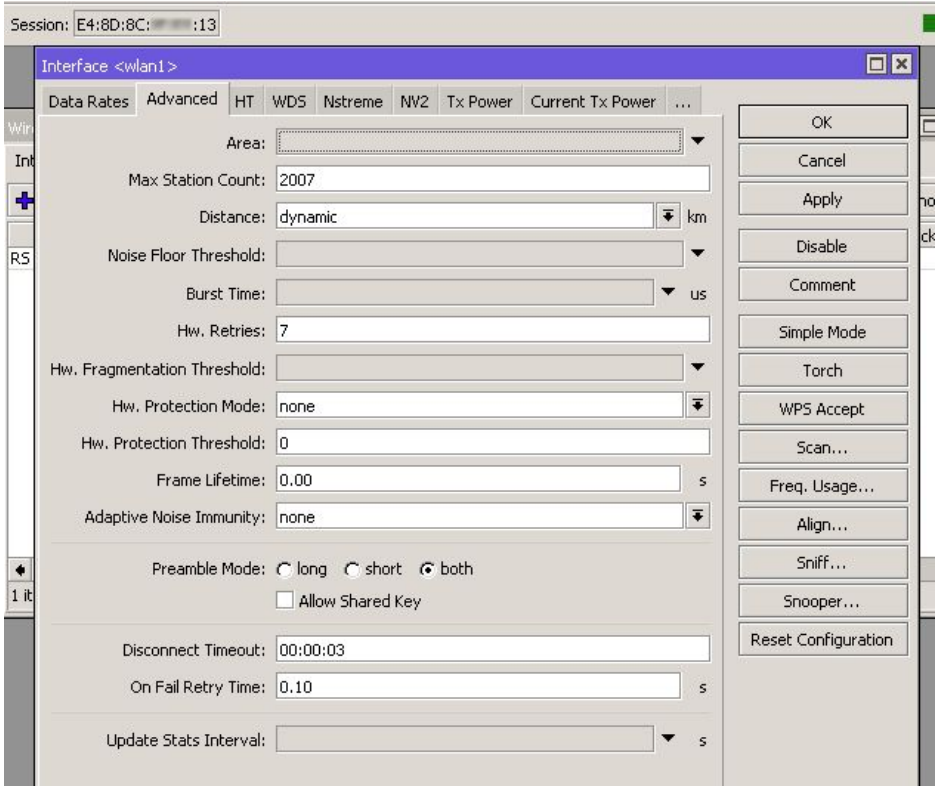
10.0.2.118

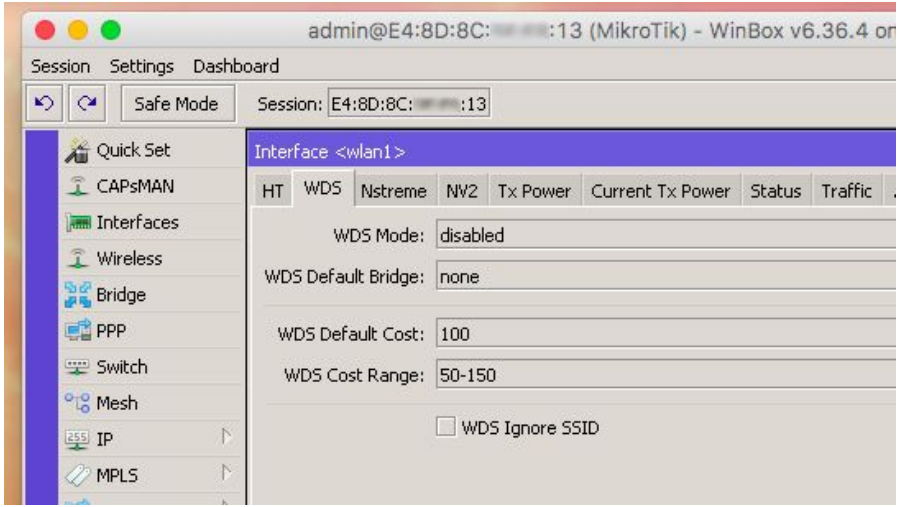
Always on WiFi enabled: … but too slow!



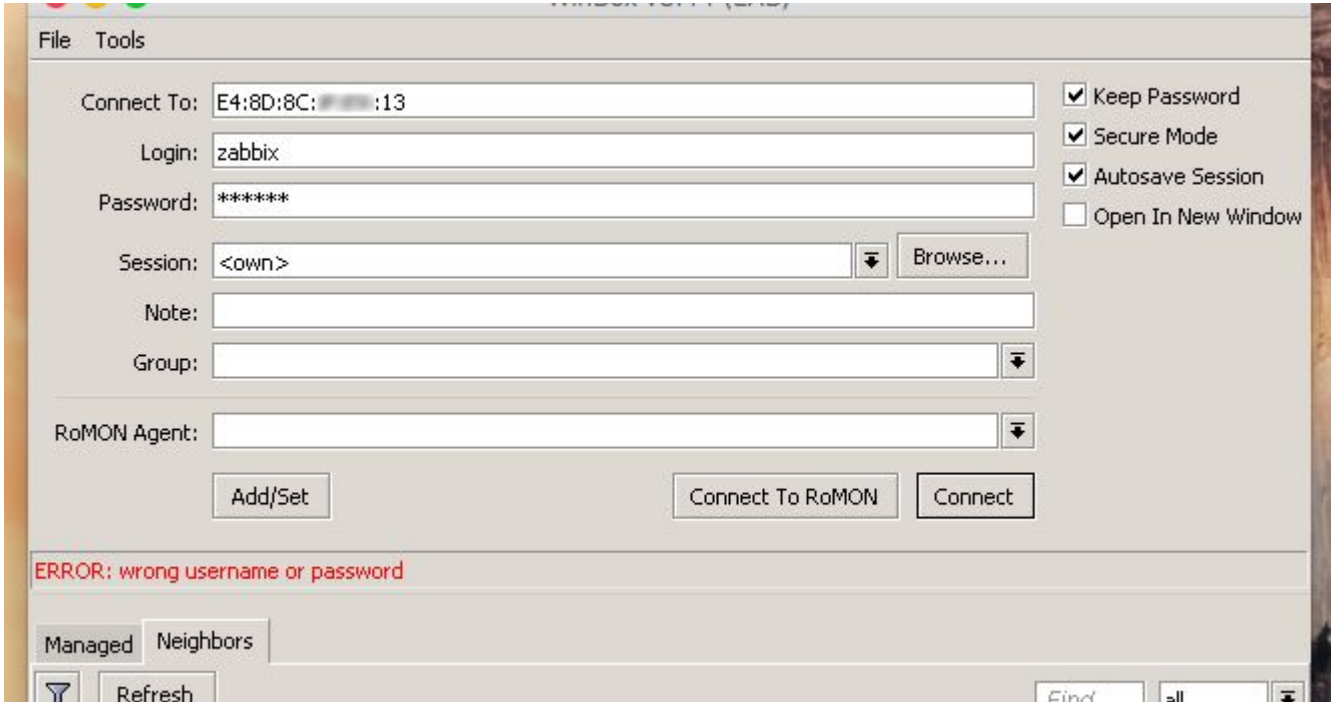


Always on WiFi enabled: … but too slow!



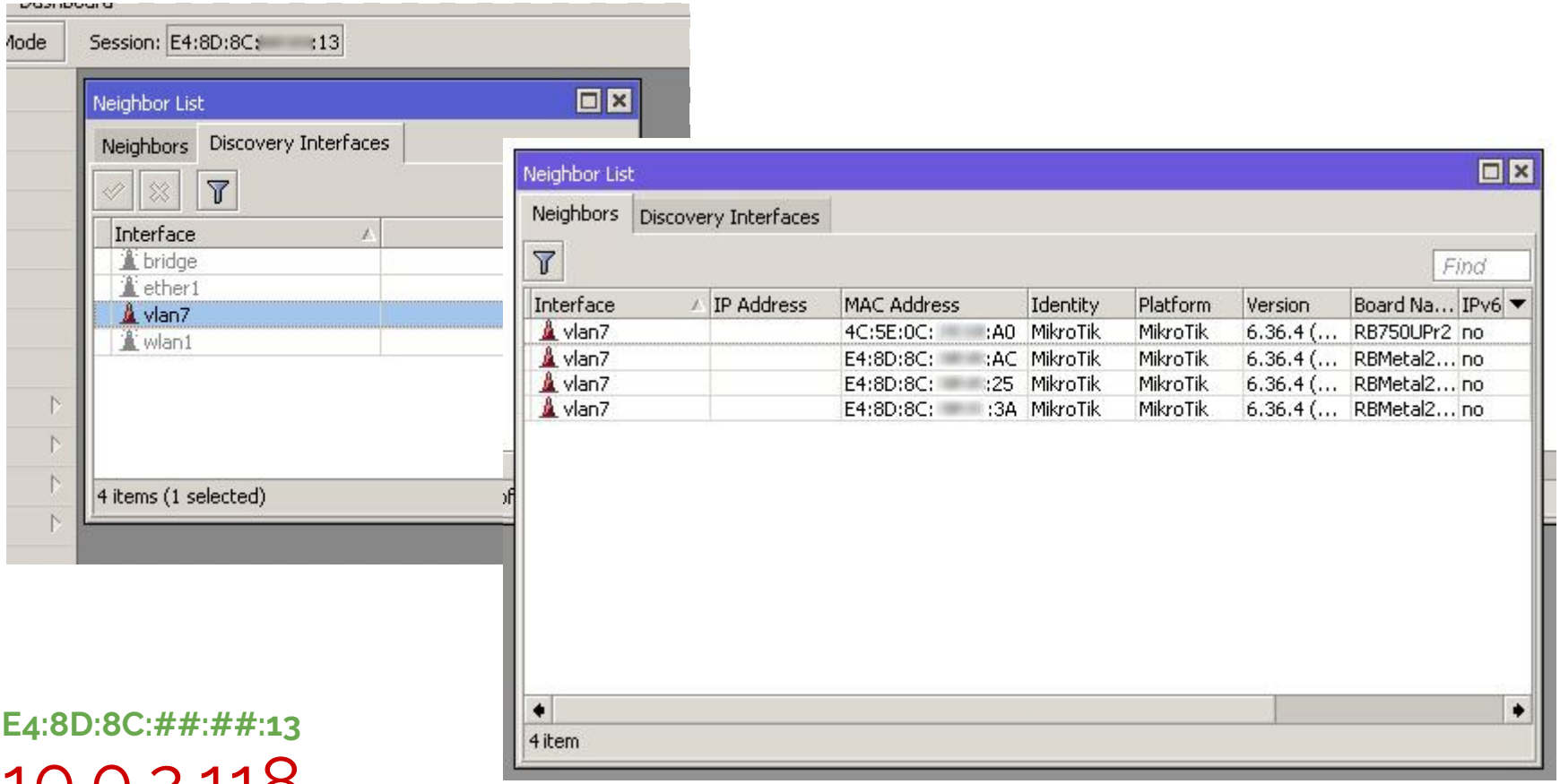


WDS: disabled



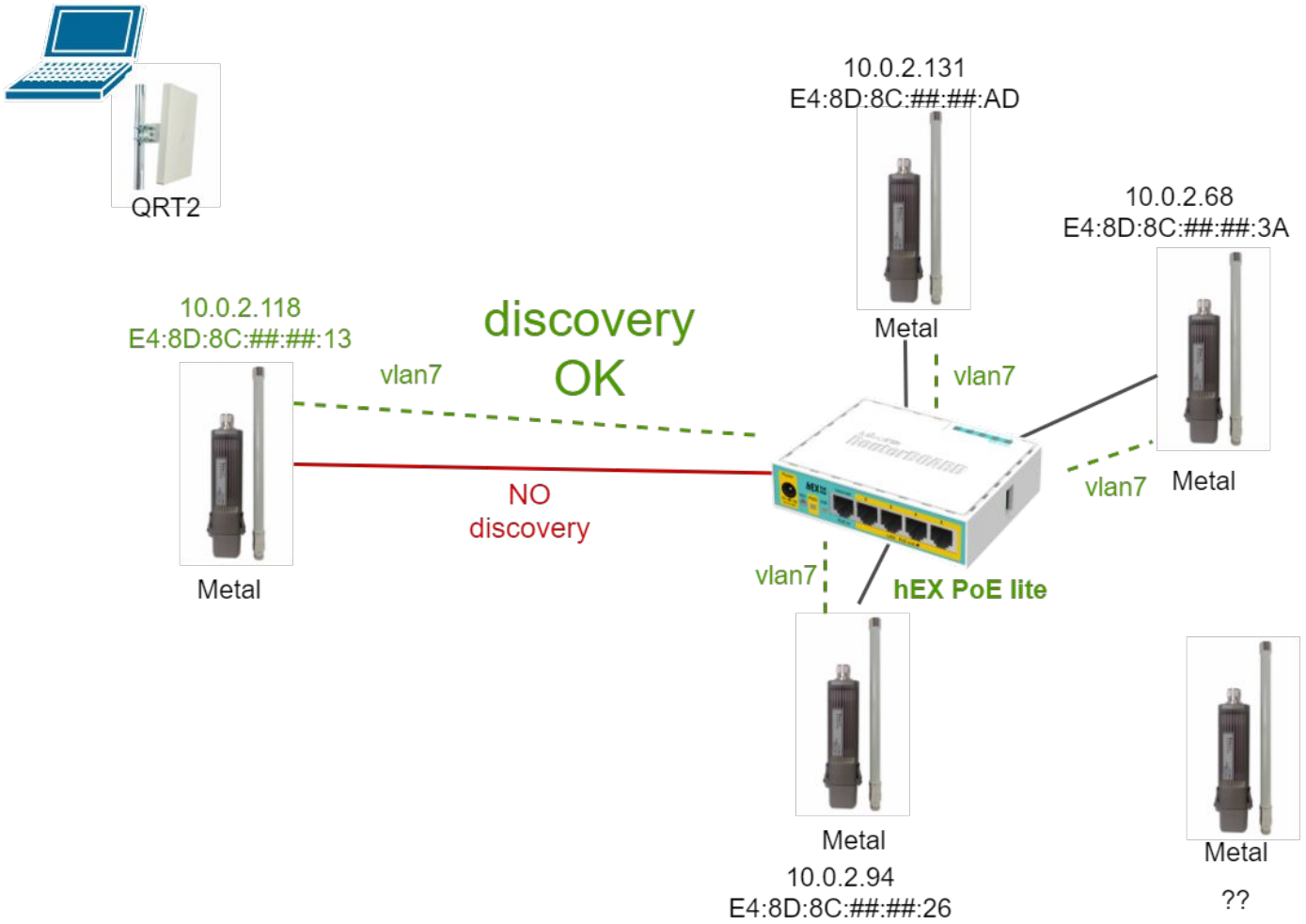
E4:8D:8C:##:##:13

10.0.2.118



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

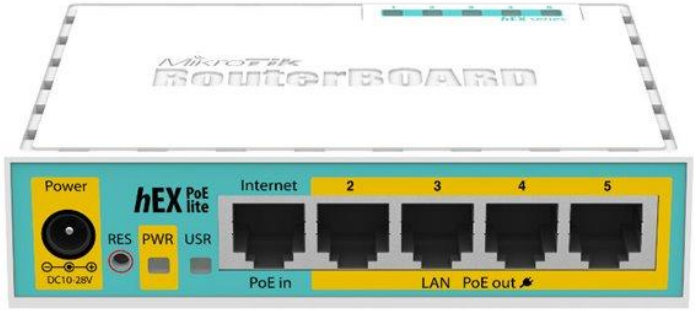
10.0.2.118



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

10.0.2.118

RouterBoard
RB750UPr2

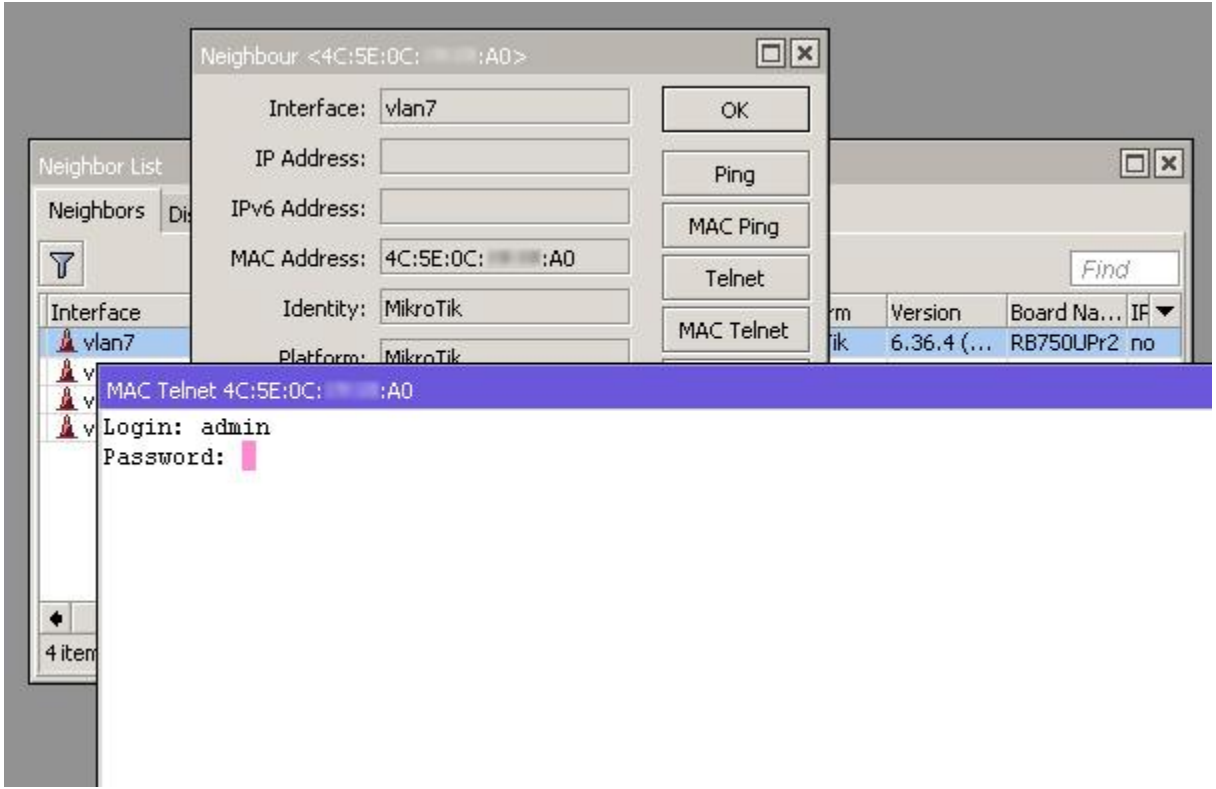


CPU:	650MHz
RAM:	64MB
PoE-out:	2-5 ports (2A max total)
PoE-in:	ether1

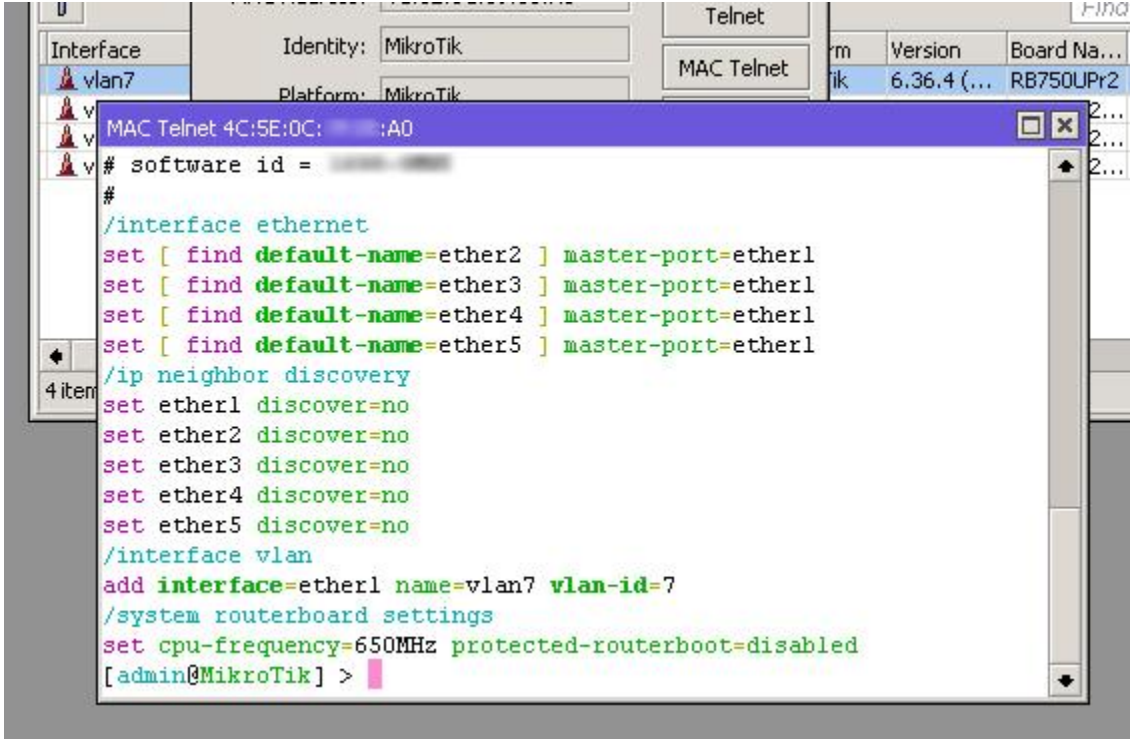
Trying to ~~hack~~ hug the hEX PoE lite

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

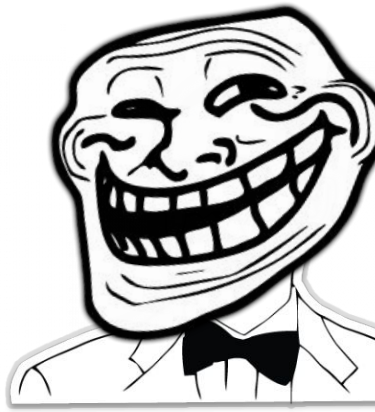
Nikita Tarikin

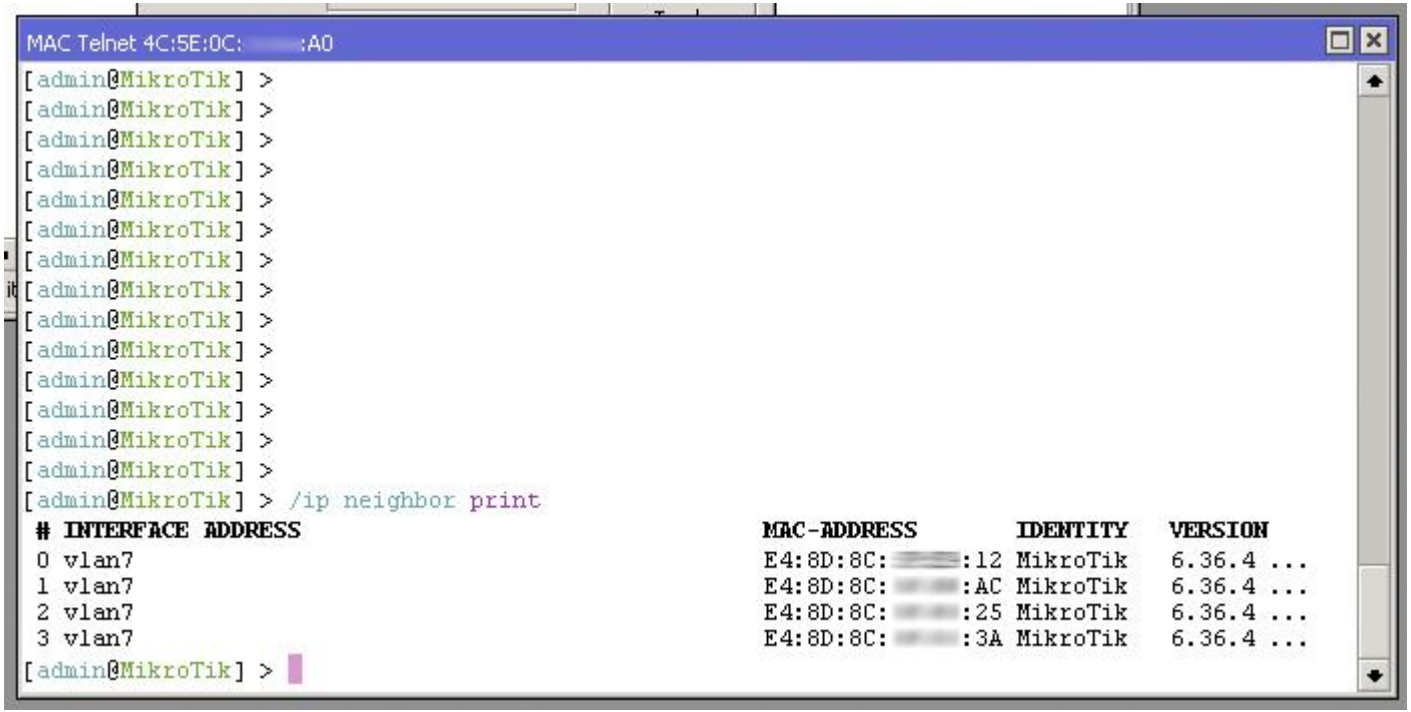

Neighbour <4C:5E:0C:[redacted]:A0>
Interface: vlan7
IP Address:
IPv6 Address:
MAC Address: 4C:5E:0C:[redacted]:A0
Identity: MikroTik
Platform: MikroTik
OK
Ping
MAC Ping
Telnet
MAC Telnet
Neighbor List
Neighbors
Find
Interface
Version
Board Na...
vlan7
6.36.4 (...
RB750UPr2
no
MAC Telnet 4C:5E:0C:[redacted]:A0
Login: admin
Password:

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

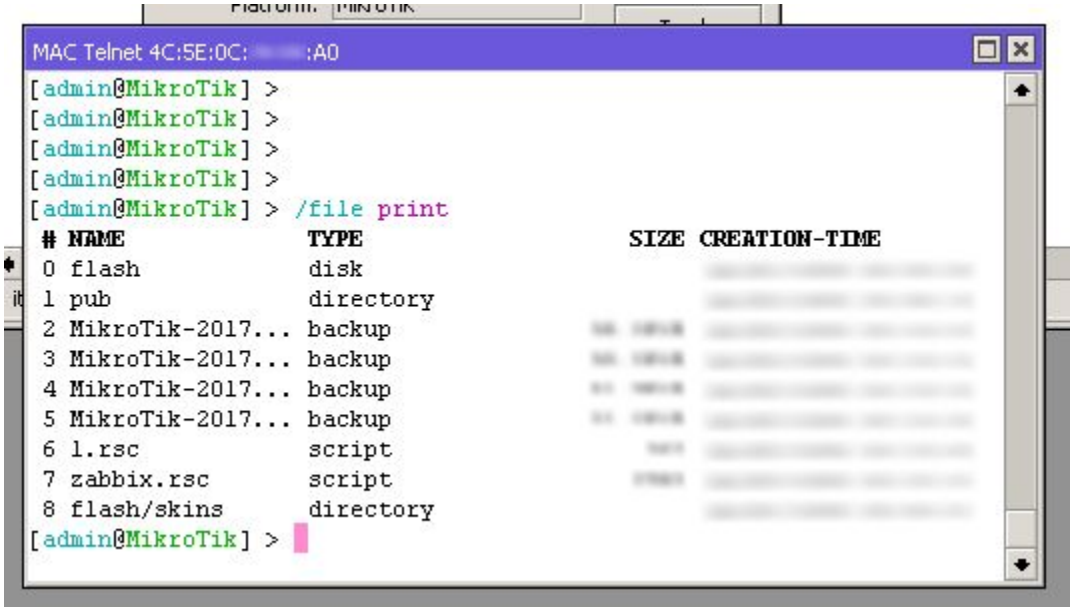

Telnet
Identity: MikroTik
MAC Telnet
Interface
Version
Board Na...
vlan7
6.36.4 (...
RB750UPr2
MAC Telnet 4C:5E:0C:[redacted]:A0
software id = [redacted]
#
/interface ethernet
set [find default-name=ether2] master-port=ether1
set [find default-name=ether3] master-port=ether1
set [find default-name=ether4] 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:##:##:A0

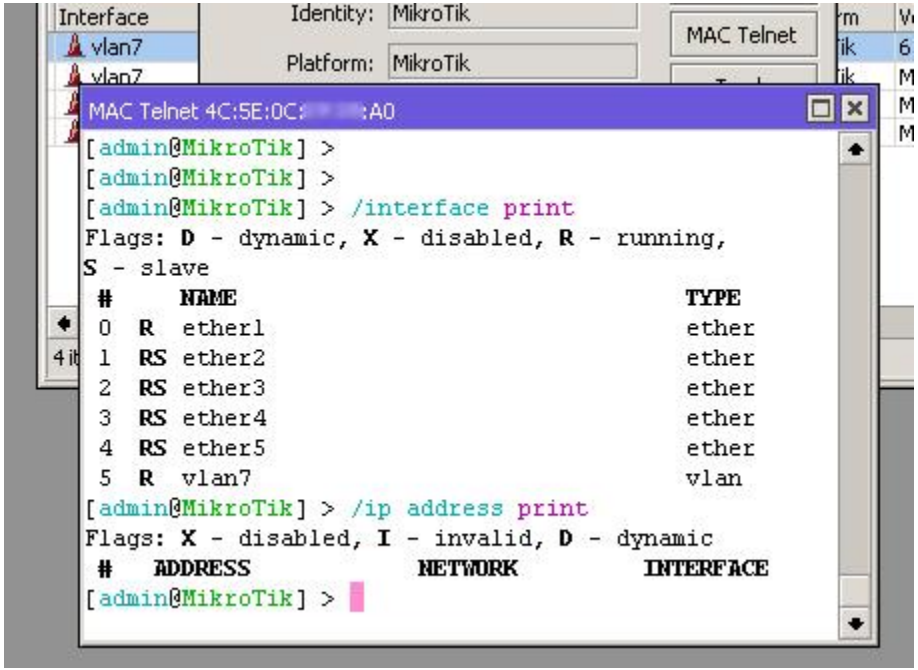



MAC Telnet 4C:5E:0C: :A0
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] >
[admin@MikroTik] > /ip neighbor print
INTERFACE ADDRESS MAC-ADDRESS IDENTITY VERSION
0 vlan7 E4:8D:8C: :12 MikroTik 6.36.4 ...
1 vlan7 E4:8D:8C: :AC MikroTik 6.36.4 ...
2 vlan7 E4:8D:8C: :25 MikroTik 6.36.4 ...
3 vlan7 E4:8D:8C: :3A MikroTik 6.36.4 ...
[admin@MikroTik] >

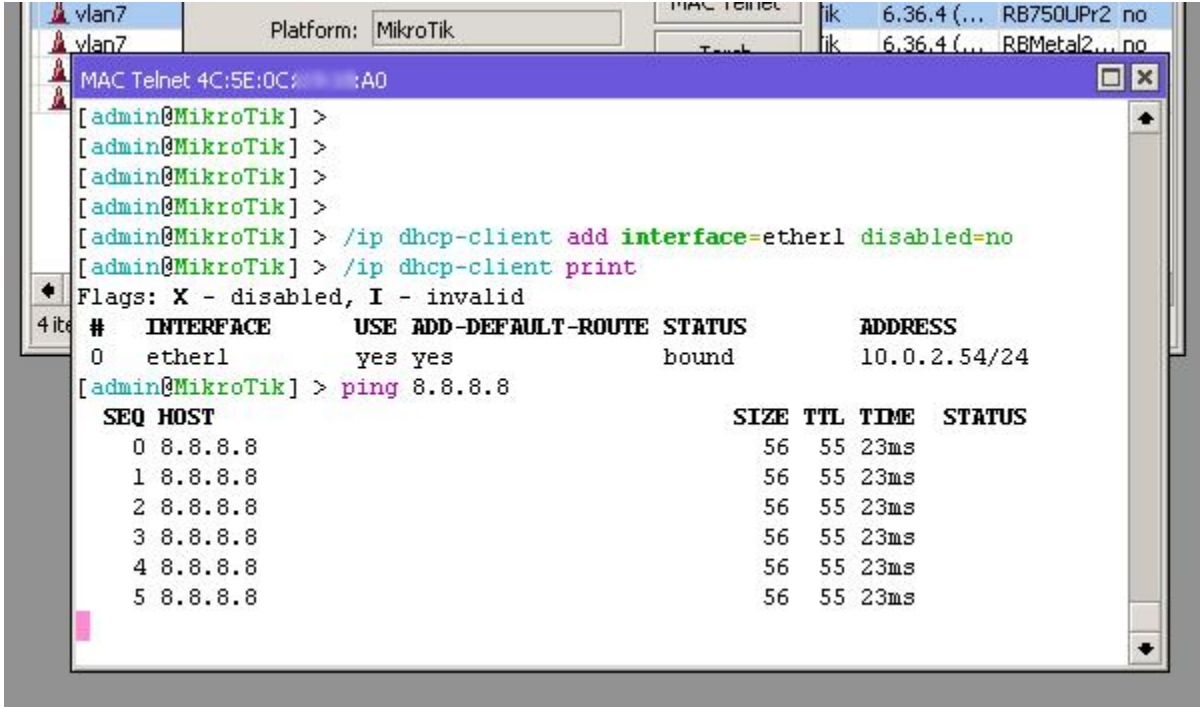
4C:E5:0C:##:##:A0


MAC Telnet 4C:5E:0C:[redacted]:A0
[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
3 MikroTik-2017... backup
4 MikroTik-2017... backup
5 MikroTik-2017... backup
6 l.rsc script
7 zabbix.rsc script
8 flash/skins directory
[admin@MikroTik] >

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


Interface
vlan7
Identity: MikroTik
Platform: MikroTik
MAC Telnet
MAC Telnet 4C:5E:0C:[redacted]:A0
[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] >

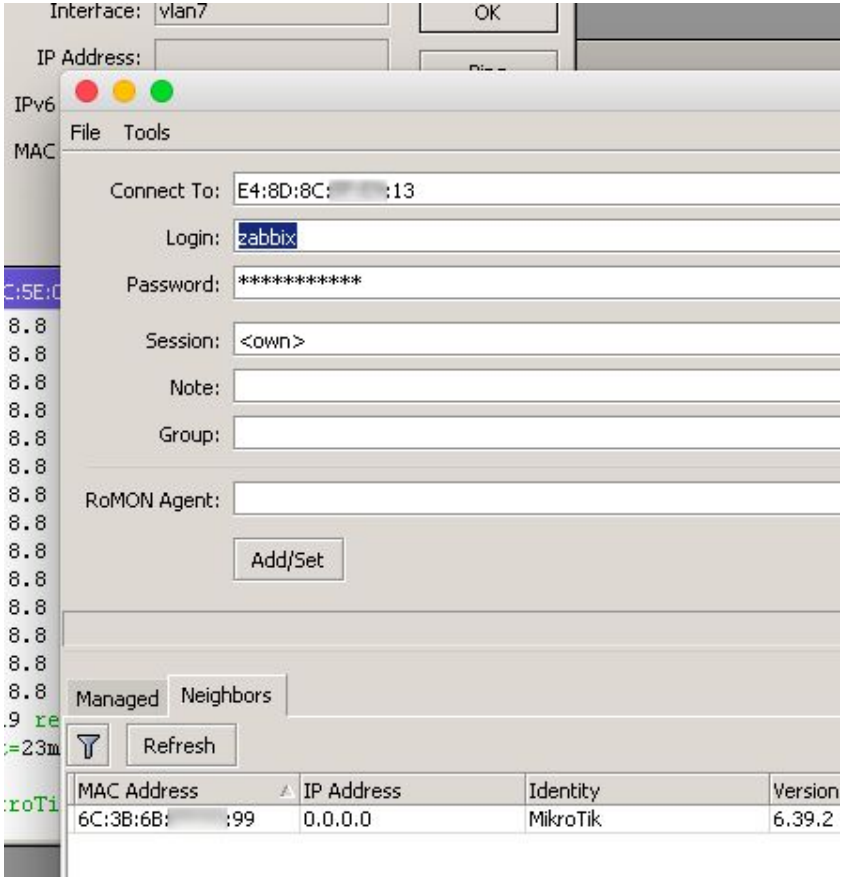
4C:E5:0C:##:##:A0


vlan7
vlan7
Platform: MikroTik
6.36.4 (...
RB750UPr2
no
6.36.4 (...
RBMetal2...
no
MAC Telnet 4C:5E:0C:
:A0
[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

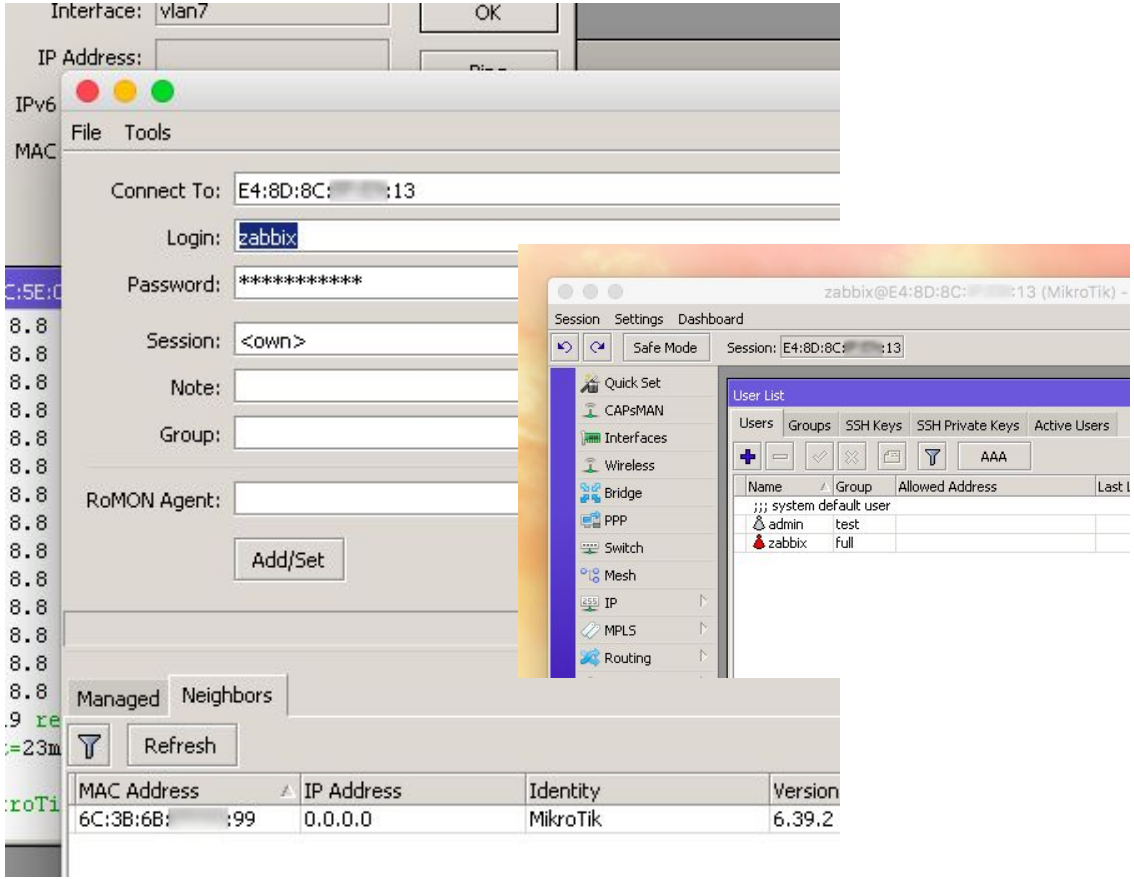
4C:E5:0C:##:##:A0

You have new mail...

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

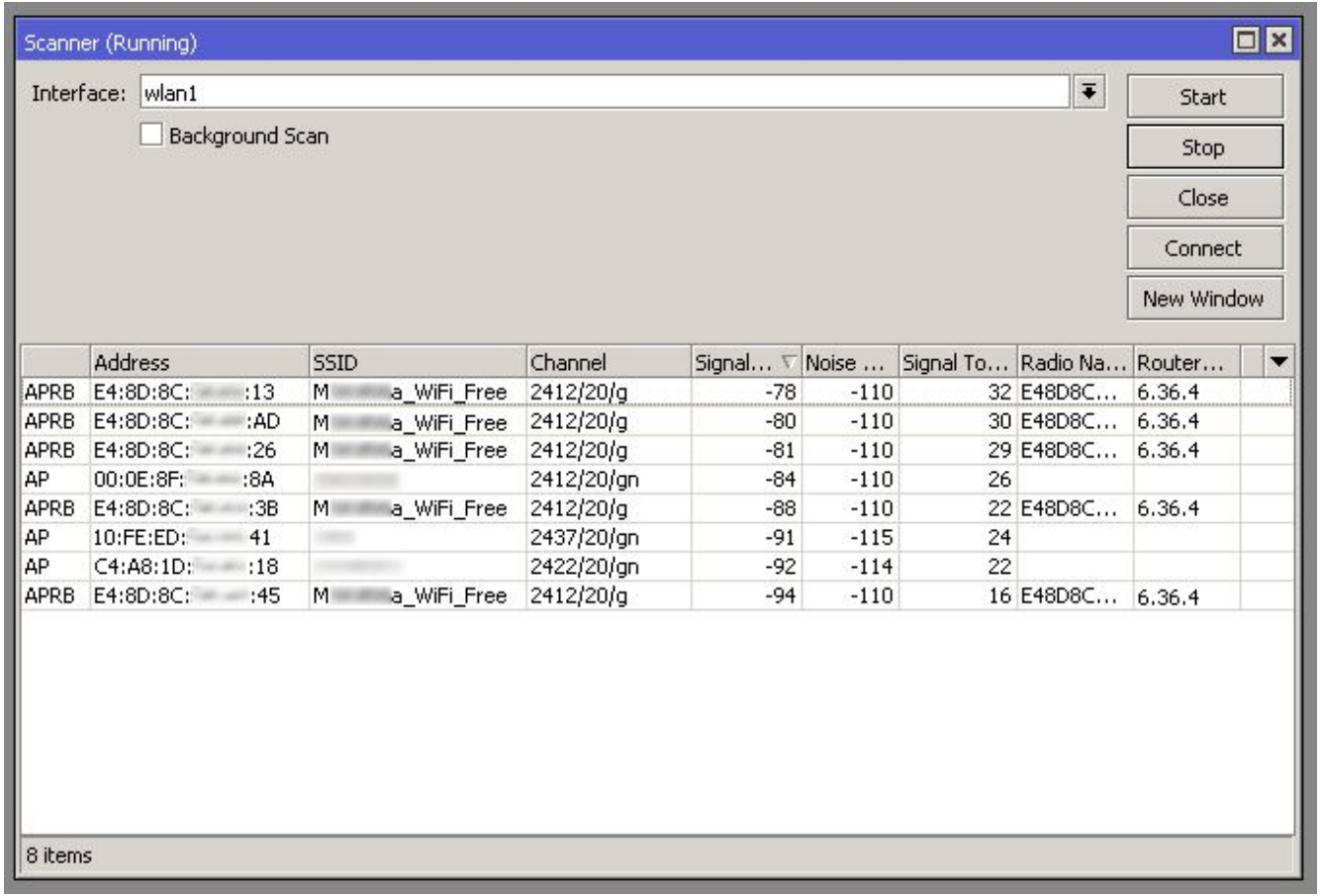

Interface: vlan7
OK
IP Address:
IPv6
MAC
File Tools
Connect To: E4:8D:8C:##:13
Login: zabbix
Password: ********
Session: <own>
Note:
Group:
RoMON Agent:
Add/Set
Managed
Neighbors
Refresh
MAC Address
IP Address
Identity
Version
6C:3B:6B:##:99
0.0.0.0
MikroTik
6.39.2

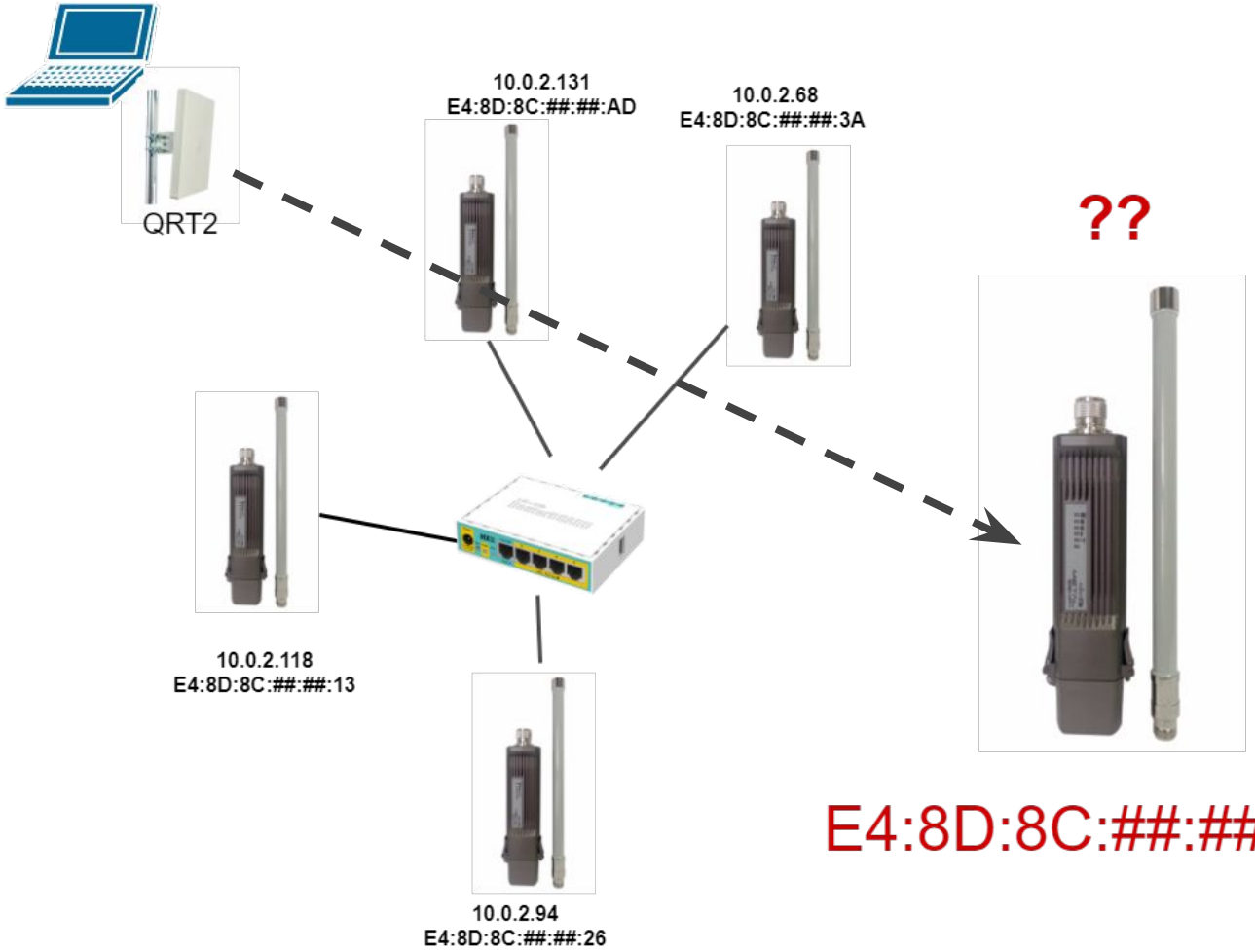
E4:8D:8C:##:##:13


Interface: vlan7
OK
IP Address:
IPv6
MAC
File Tools
Connect To: E4:8D:8C:[redacted]:13
Login: zabbix
Password: ••••••••••••
Session: <own>
Note:
Group:
RoMON Agent:
Add/Set
zabbix@E4:8D:8C:[redacted]:13 (MikroTik)
Session Settings Dashboard
Safe Mode
Session: E4:8D:8C:[redacted]:13
Quick Set
CAPsMAN
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
;;; system default user
admin test
zabbix full
Managed Neighbors
Refresh
MAC Address IP Address Identity Version
6C:3B:6B:[redacted]:99 0.0.0.0 MikroTik 6.39.2

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

QRT2 wireless scanner (Running)



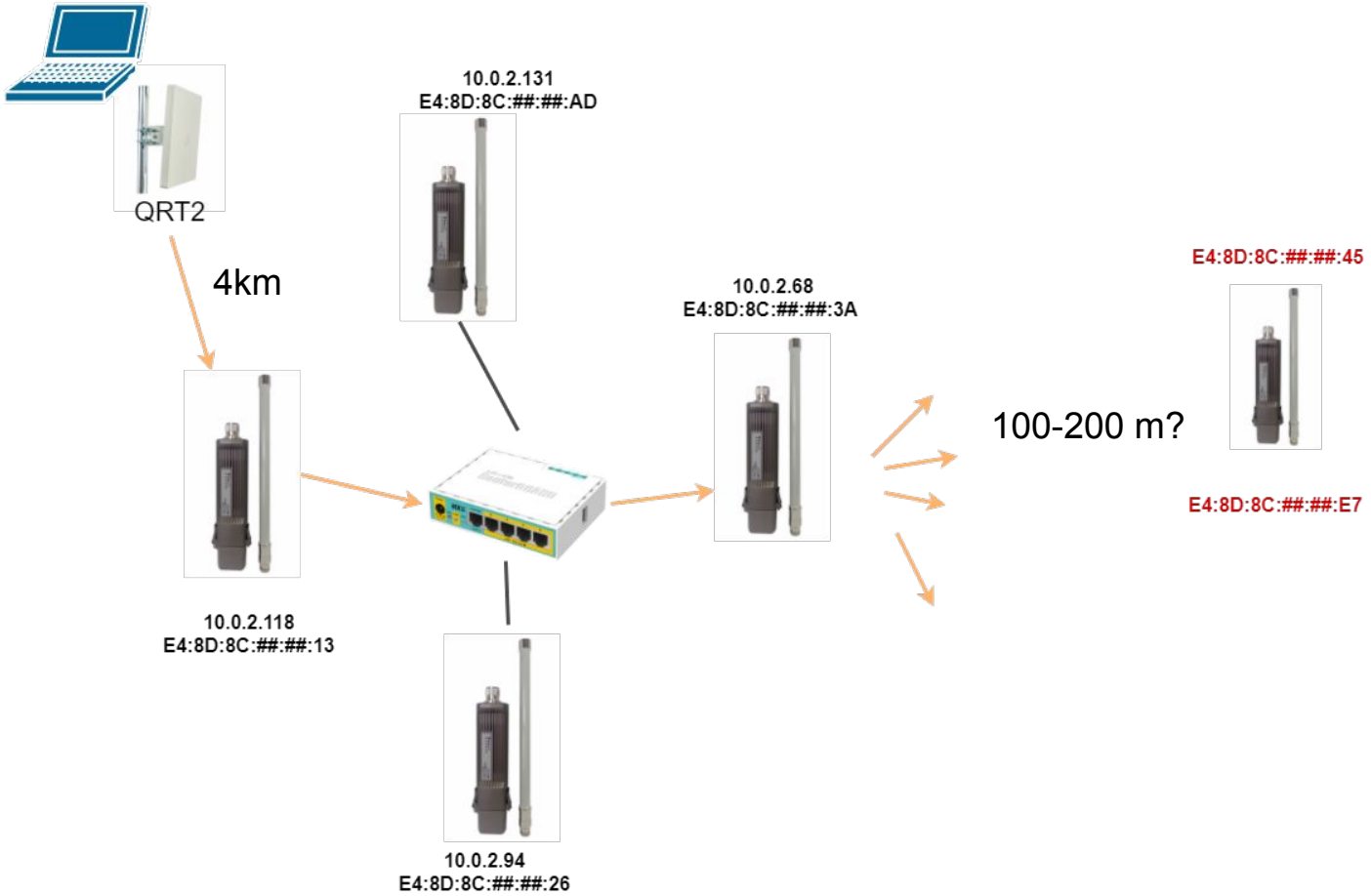

QRT2
10.0.2.131
E4:8D:8C:##:##:AD
10.0.2.68
E4:8D:8C:##:##:3A
??
10.0.2.118
E4:8D:8C:##:##:13
10.0.2.94
E4:8D:8C:##:##:26
-94 dBm
E4:8D:8C:##:##:45

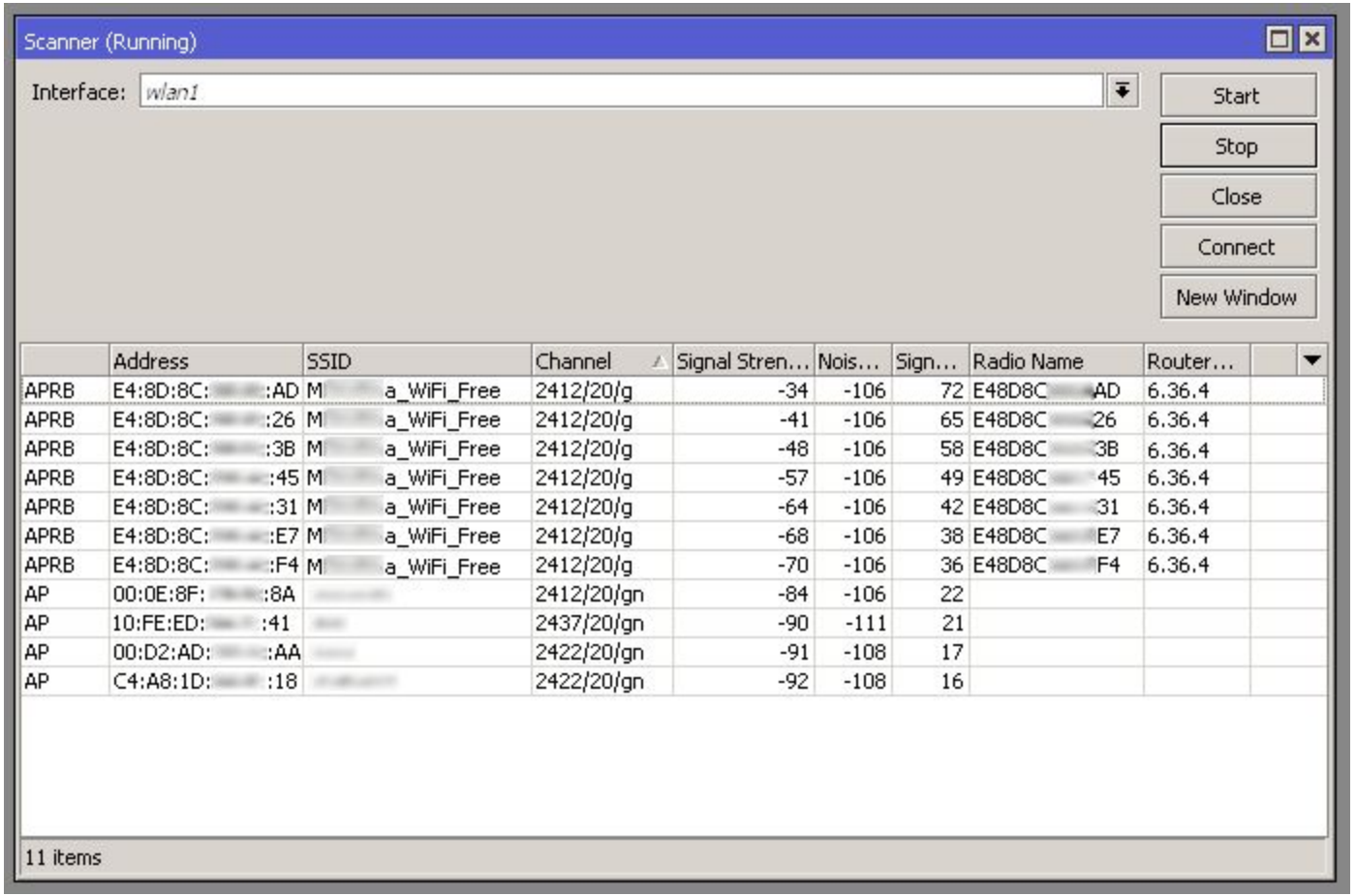
[Round 5]

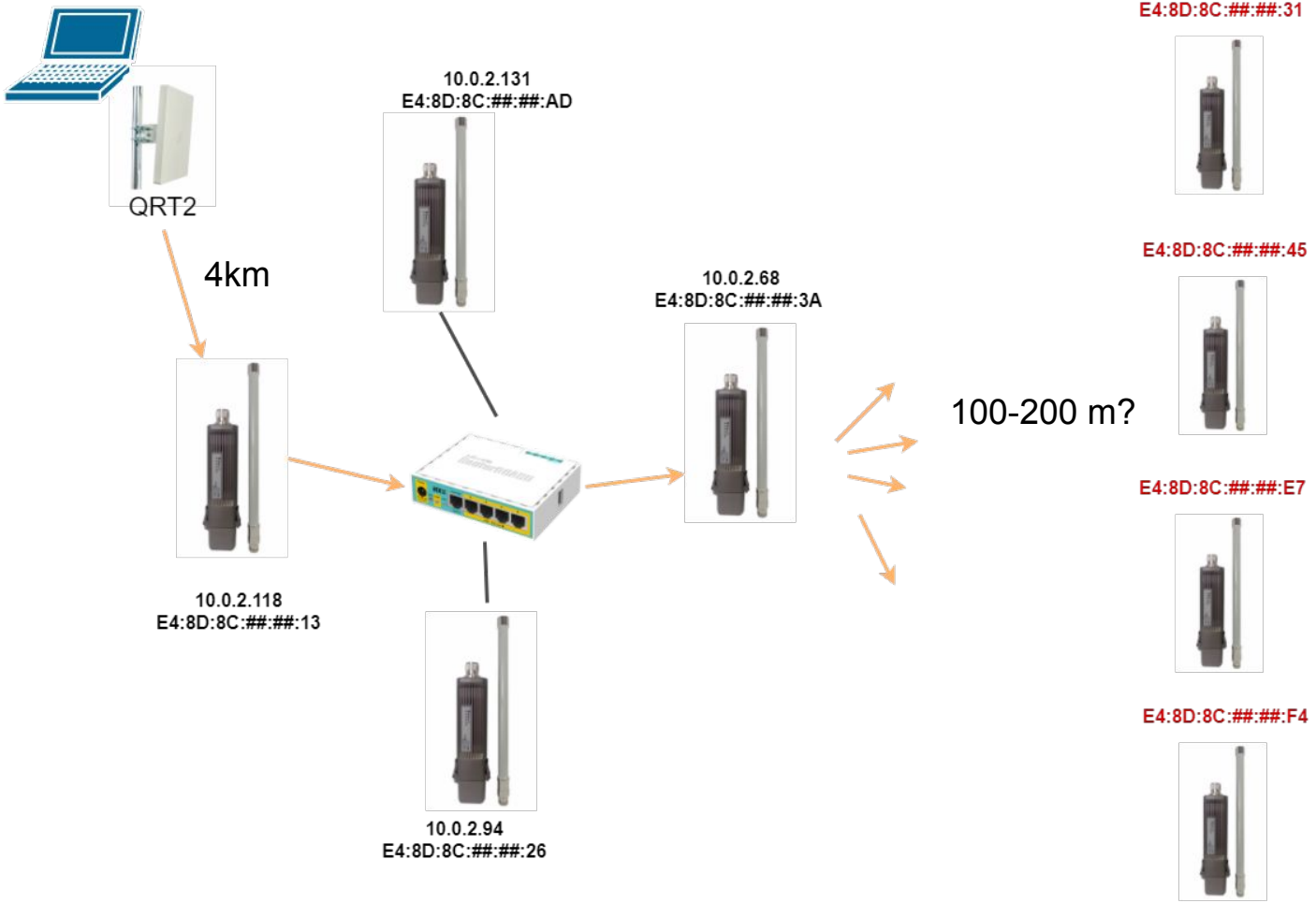
Looking for the missing
RouterBoard access point

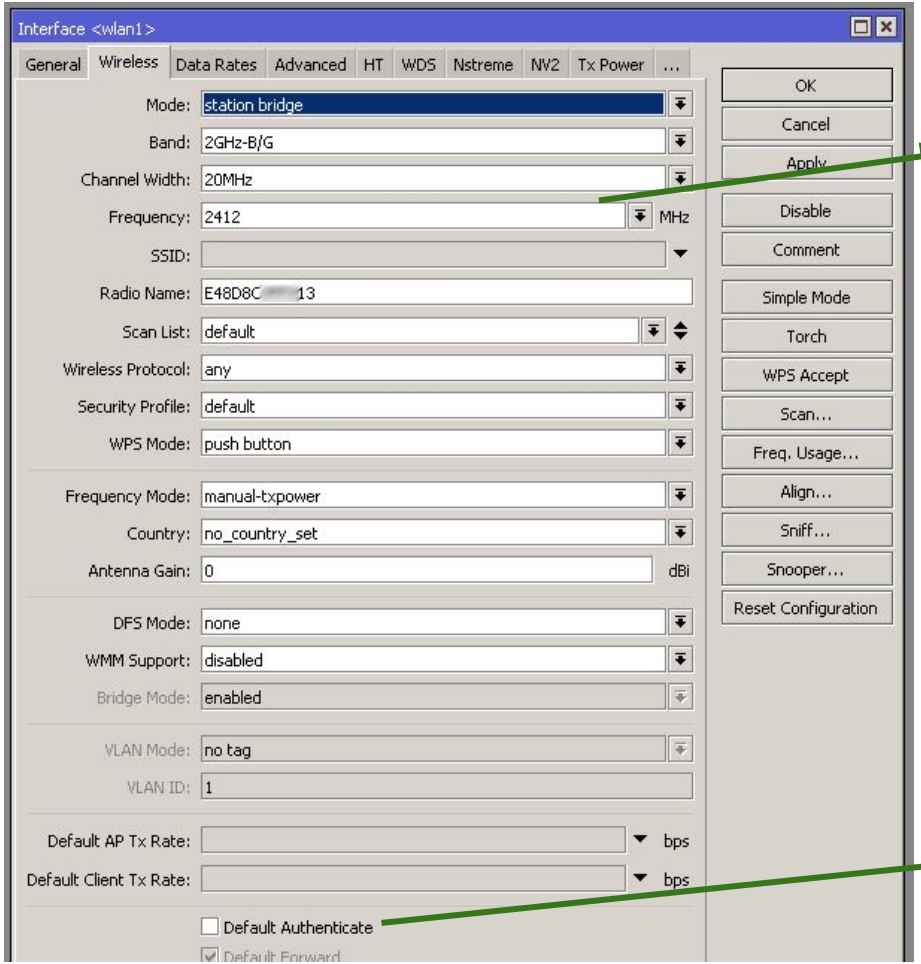
E4:8D:8C:##:##:45

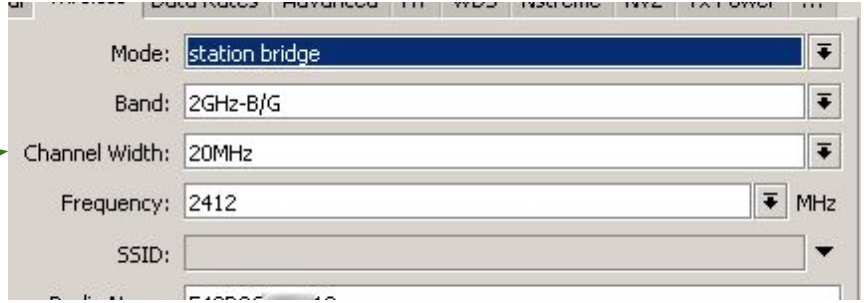
Nikita Tarikin

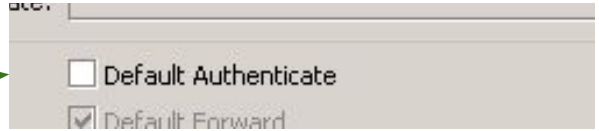

QRT2
4km
10.0.2.131
E4:8D:8C:##:##:AD
10.0.2.68
E4:8D:8C:##:##:3A
E4:8D:8C:##:##:45
100-200 m?
E4:8D:8C:##:##:E7
10.0.2.118
E4:8D:8C:##:##:13
10.0.2.94
E4:8D:8C:##:##:26

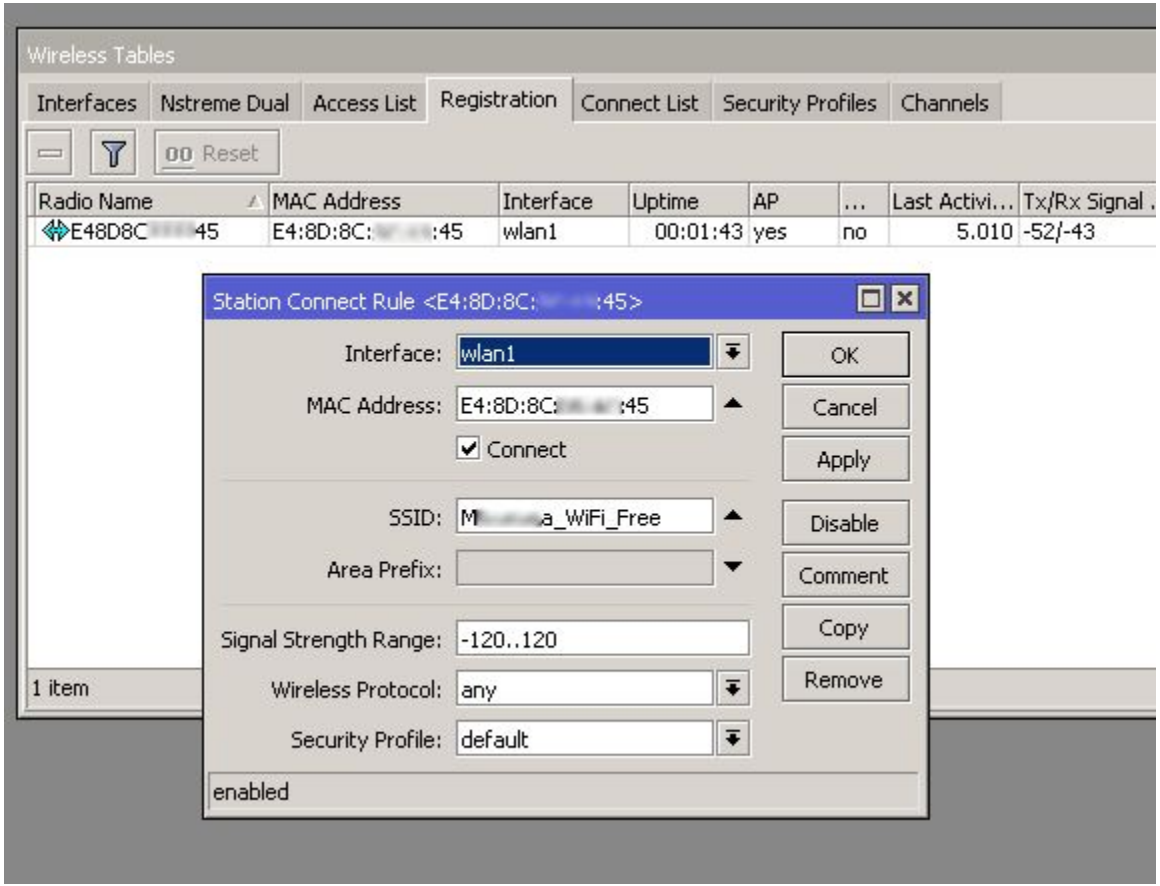

Scanner (Running)
Interface: wlan1
Start
Stop
Close
Connect
New Window
Address
SSID
Channel
Signal Stren...
Nois...
Sign...
Radio Name
Router...
APRB E4:8D:8C:[redacted]:AD M[redacted]a_WiFi_Free 2412/20/g -34 -106 72 E48D8C[redacted]AD 6.36.4
APRB E4:8D:8C:[redacted]:26 M[redacted]a_WiFi_Free 2412/20/g -41 -106 65 E48D8C[redacted]26 6.36.4
APRB E4:8D:8C:[redacted]:3B M[redacted]a_WiFi_Free 2412/20/g -48 -106 58 E48D8C[redacted]3B 6.36.4
APRB E4:8D:8C:[redacted]:45 M[redacted]a_WiFi_Free 2412/20/g -57 -106 49 E48D8C[redacted]45 6.36.4
APRB E4:8D:8C:[redacted]:31 M[redacted]a_WiFi_Free 2412/20/g -64 -106 42 E48D8C[redacted]31 6.36.4
APRB E4:8D:8C:[redacted]:E7 M[redacted]a_WiFi_Free 2412/20/g -68 -106 38 E48D8C[redacted]E7 6.36.4
APRB E4:8D:8C:[redacted]:F4 M[redacted]a_WiFi_Free 2412/20/g -70 -106 36 E48D8C[redacted]F4 6.36.4
AP 00:0E:8F:[redacted]:8A [redacted] 2412/20/gn -84 -106 22
AP 10:FE:ED:[redacted]:41 [redacted] 2437/20/gn -90 -111 21
AP 00:D2:AD:[redacted]:AA [redacted] 2422/20/gn -91 -108 17
AP C4:A8:1D:[redacted]:18 [redacted] 2422/20/gn -92 -108 16
11 items


QRT2
4km
10.0.2.131
E4:8D:8C:##:##:AD
10.0.2.68
E4:8D:8C:##:##:3A
10.0.2.118
E4:8D:8C:##:##:13
10.0.2.94
E4:8D:8C:##:##:26
100-200 m?
E4:8D:8C:##:##:31
E4:8D:8C:##:##:45
E4:8D:8C:##:##:E7
E4:8D:8C:##:##:F4

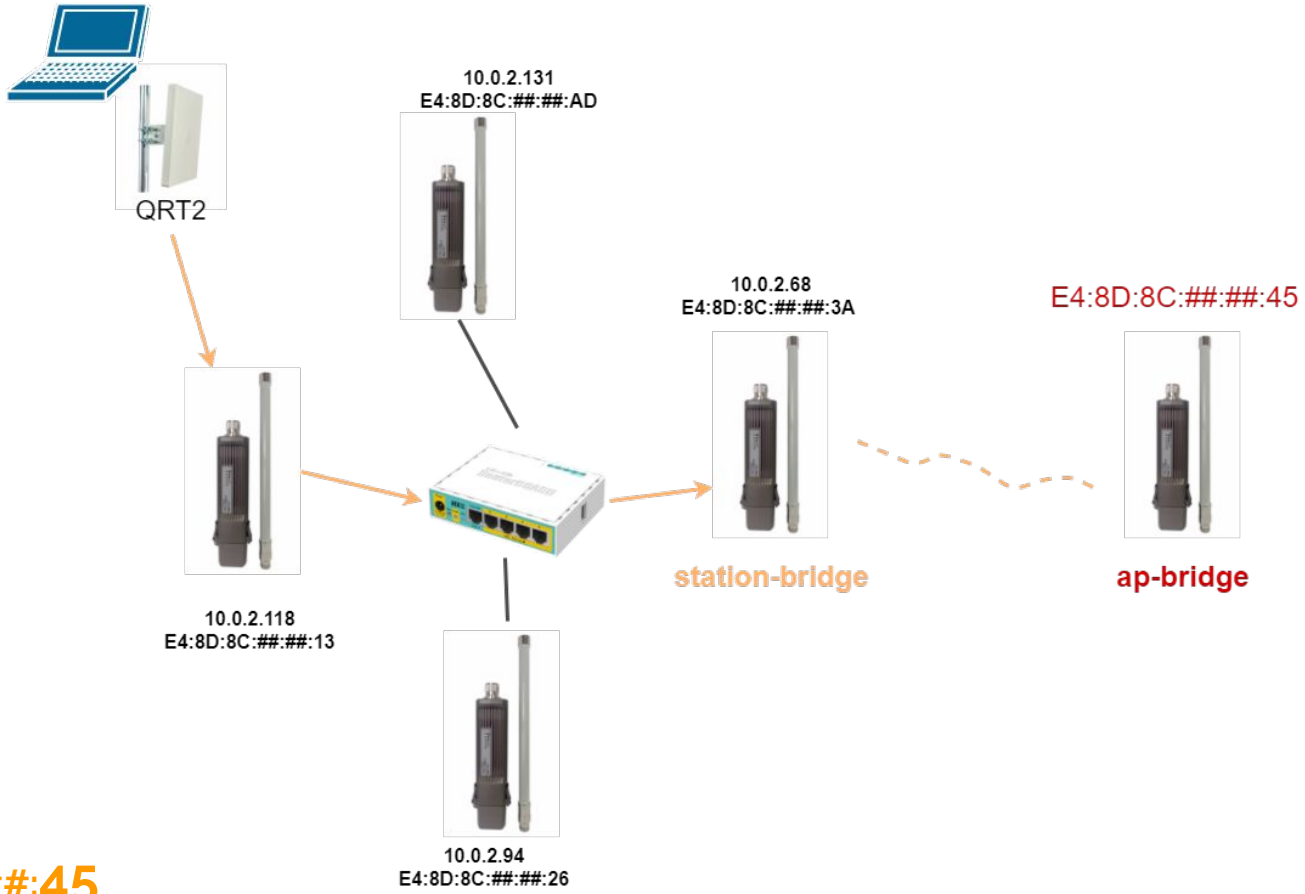

Interface <wlan1>
General
Wireless
Data Rates
Advanced
HT
WDS
Nstreme
NV2
Tx Power
...
Mode: station bridge
Band: 2GHz-B/G
Channel Width: 20MHz
Frequency: 2412 MHz
SSID:
Radio Name: E48D8C 13
Scan List: default
Wireless Protocol: any
Security Profile: default
WPS Mode: push button
Frequency Mode: manual-txpower
Country: no_country_set
Antenna Gain: 0 dBi
DFS Mode: none
WMM Support: disabled
Bridge Mode: enabled
VLAN Mode: no tag
VLAN ID: 1
Default AP Tx Rate: bps
Default Client Tx Rate: bps
Default Authenticate
Default Forward
OK
Cancel
Apply
Disable
Comment
Simple Mode
Torch
WPS Accept
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...
Reset Configuration


Mode: station bridge
Band: 2GHz-B/G
Channel Width: 20MHz
Frequency: 2412 MHz
SSID:

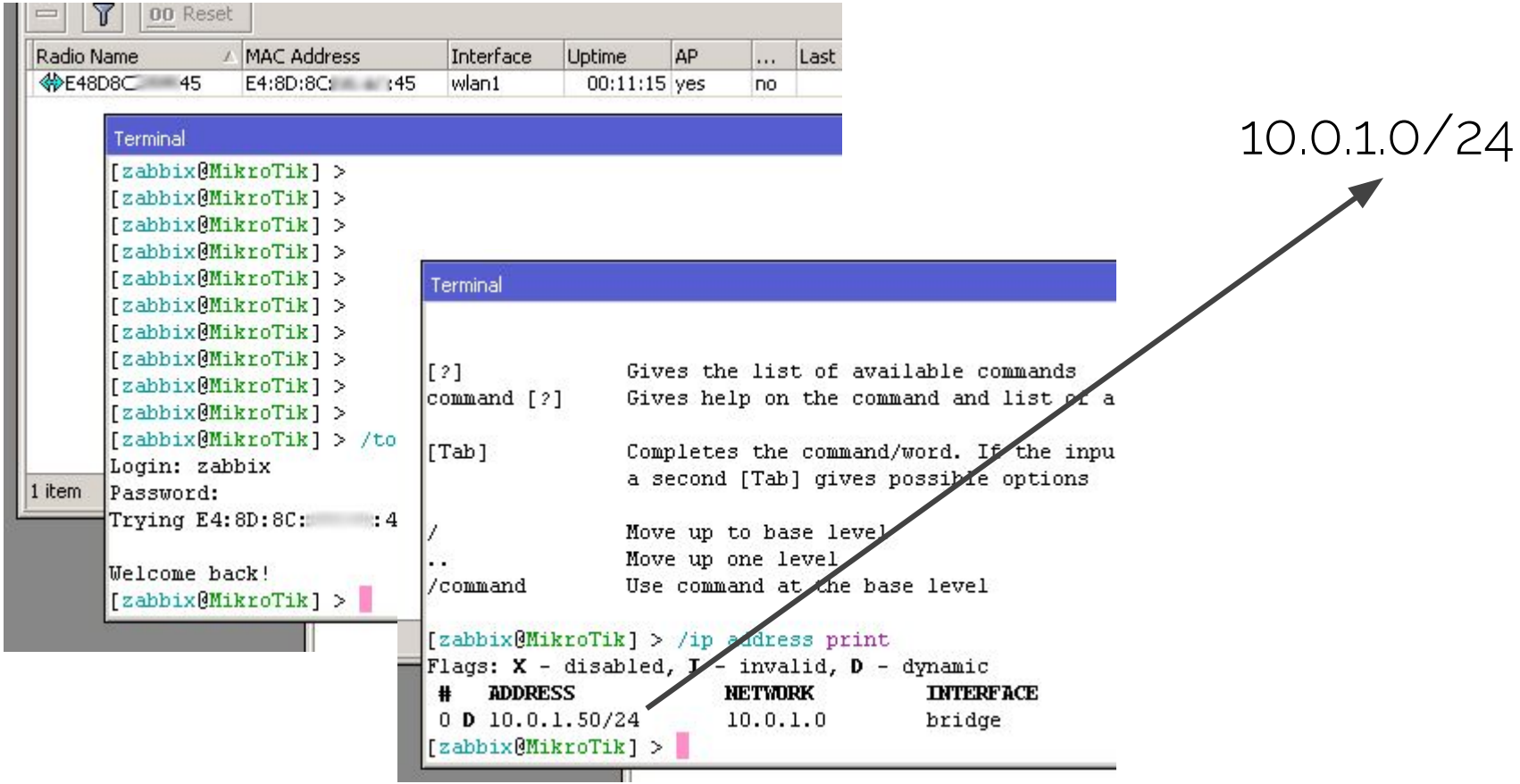

Default Authenticate
Default Forward


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

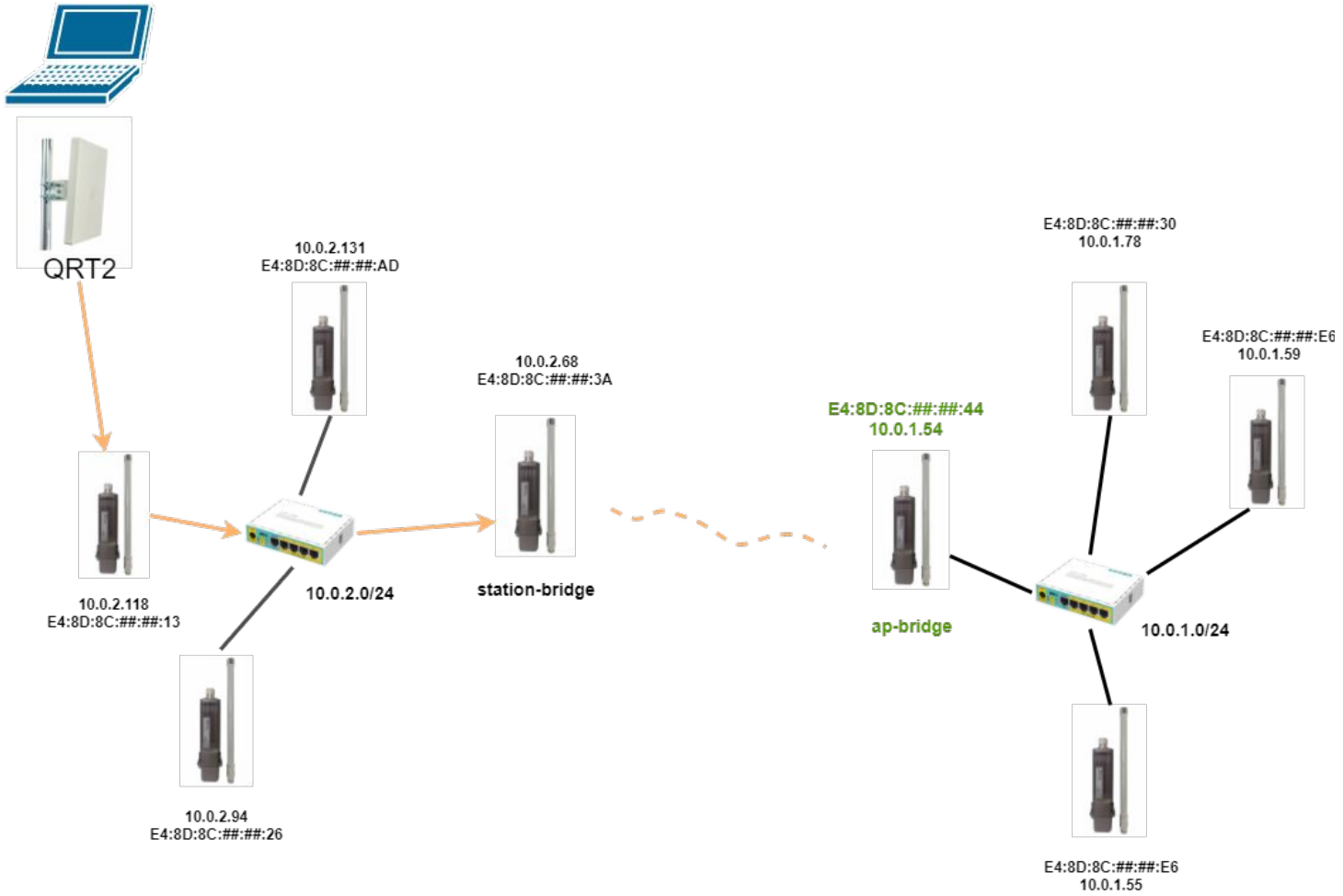
E4:8D:8C:##:##:45

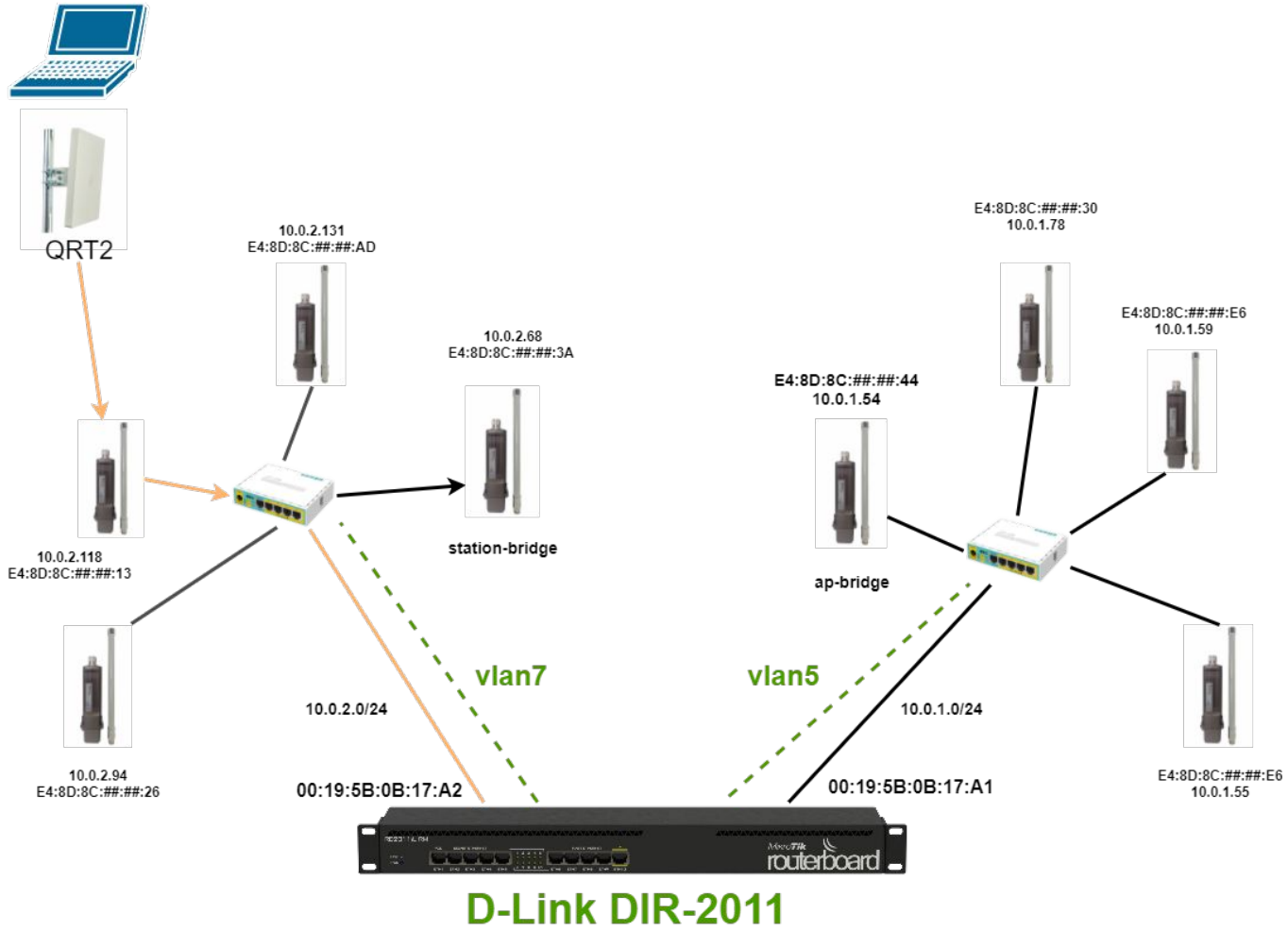

QRT2
10.0.2.131
E4:8D:8C:##:##:AD
10.0.2.68
E4:8D:8C:##:##:3A
E4:8D:8C:##:##:45
10.0.2.118
E4:8D:8C:##:##:13
station-bridge
ap-bridge
10.0.2.94
E4:8D:8C:##:##:26

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


00 Reset
Radio Name
MAC Address
Interface
Uptime
AP
...
Last
E48D8C 45
E4:8D:8C: :45
wlan1
00:11:15
yes
no
1 item
Terminal
[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 inpu
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
10.0.2.131
E4:8D:8C:##:##:AD
10.0.2.68
E4:8D:8C:##:##:3A
E4:8D:8C:##:##:44
10.0.1.54
E4:8D:8C:##:##:30
10.0.1.78
E4:8D:8C:##:##:E6
10.0.1.59
10.0.2.118
E4:8D:8C:##:##:13
10.0.2.0/24
station-bridge
ap-bridge
10.0.1.0/24
10.0.2.94
E4:8D:8C:##:##:26
E4:8D:8C:##:##:E6
10.0.1.55



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