

RouterBOARD Wireless Hacks

Jesse Liu edit Master subtitle style
Convergingstream

MikroTik Distributor

For purchases of Hardware or MikroTik RouterOS please contact our Official Distributors:

Contents:

North America

Canada
Costa Rica
Mexico
USA

South America

Argentina
Bolivia
Brazil
Chile
Colombia
Ecuador
Paraguay
Peru
Uruguay
Venezuela

Africa

Cameroon
Egypt
Gabon
Kenya
Nigeria
South Africa
Tanzania

Asia

Afghanistan
Bangladesh
China
India
Indonesia

Asia

EDCwifi

Shenzhen, China
RouterBOARD
components, training
Tel: 86-755-82642594
[Write e-mail](#)



CDNAT

Chengdu, China
RouterBOARD
components
Tel: 86-28-87777784
[Write e-mail](#)



ConvergingStream Technologies

Beijing, China
RouterBOARD
components
Tel: 010 6894 8781
[Write e-mail](#)



XBase

Changsha, China
RouterBOARD
components
Tel: +86-4006770099
[Write e-mail](#)



北京恒通安信科技有限公司

MikroTik certified Integrator

Uniterm Direct
www.dbg.co.za

Uniterm in South Africa offer cases, antennas and preassembled kits based on RouterOS and RouterBOARD



Discomp
www.discomp.eu

Discomp make a variety of CPE/AP solutions, including this outdoor client, the "MaxLink MaxStation Mikron", with 19dBi antenna.



ConvergingStream
www.cstinc.com.cn

Convergingstream from China builds products based on RouterOS preinstalled in high power multicore x86 rackmountable systems, ranging from Intel Celeron powered (MT-500L), up to multicore Xeon devices (MT-800+)



Hana Wireless
www.hanawireless.com

Hana Wireless from the USA make a variety of CPE/AP solutions based on MikroTik RouterBOARD



Xagyl
www.xagyl.com

Xagyl Communications, Canada's premier Mikrotik integrator, distributes a variety of products based on the proven RouterBOARD platform; including several versions of Outdoor Access Points, Customer Premise Equipment, Routers and Antennas.



MikroTik Application Examples

- Wireless Access Point
- Wireless Bridge
- Router
- Firewall
- VPN Concentrators
- Bandwidth Management
- Link Load Balancing
- Hotspot Gateway
- User Manager
- Network Monitor

Agenda

- Hack 1. Wireless client isolate
- Hack 2. Frequency Selection
- Hack 3. Access list and Security profile
- Hack 4. Wireless client bandwidth control
- Hack 5. Virtual AP and VLAN
- Hack 6. Wireless Distribution System
- Hack 7. Turbo mode (up to 108Mbps)
- Hack 8. 802.11n (up to 300Mbps)
- Hack 9. Dual radio Point-to-Point mode

Hack 1. Wireless client isolate

Interface <wlan1>

General Wireless Data Rates Advanced WDS Nstreme ...

Mode: ap bridge

Band: 2.4GHz-B/G

Frequency: 2412 MHz

SSID: EASPIS

Radio Name: 000C42631D22

Scan List:

Security Profile: profile1

Frequency Mode: manual bpower

Country: china

Antenna Mode: antenna a

Antenna Gain: 0 dBi

DFS Mode: none

Proprietary Extensions: post-2.9.25

WMM Support: disabled

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK Cancel Apply Disable Comment Torch Scan... Freq. Usage... Align... Sniff... Snooper... Reset Configuration Simple Mode

disabled running slave running ap

New AP Access Rule

MAC Address: 90:4C:E5:E1:4A:73

Interface: wlan1

Signal Strength Range: -120..120

AP Tx Limit:

Client Tx Limit:

Authentication

Forwarding

Private Key: none 0x:

Private Pre Shared Key:

Management Protection Key:

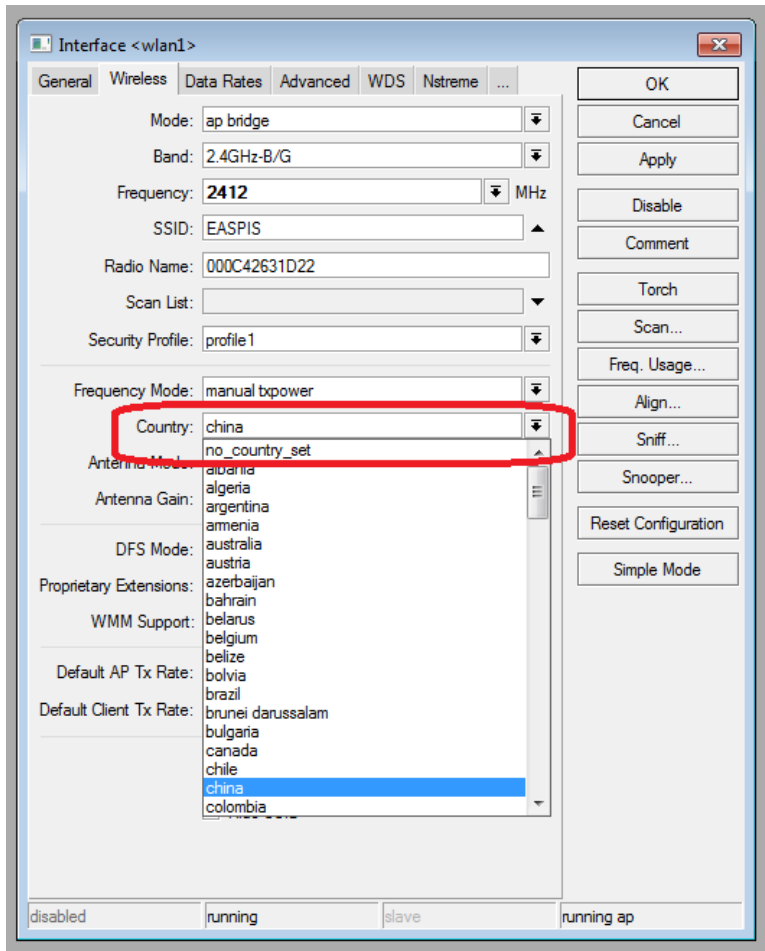
Time

disabled

OK Cancel Apply Disable Comment Copy Remove

If set to 'no', the registered clients will not be able to communicate with each other.

Hack 2. Frequency Selection



limits wireless settings (frequency and transmit power) to those which are allowed in the respective country
no_country_set - no regulatory domain limitations

Hack 2. Frequency Selection

If no country is set, these frequencies are used (FCC compliant set of channels)

2.4GHz mode: 2412, 2417, 2422, 2427, 2432, 2437, 2442, 2447, 2452, 2457, 2462

2.4GHz-g-turbo mode: 2437

5GHz mode: 5180, 5200, 5220, 5240, 5260, 5280, 5300, 5320, 5745, 5765, 5785, 5805, 5825

5GHz-turbo mode: 5210, 5250, 5290, 5760, 5800

If China is set, these frequencies are used

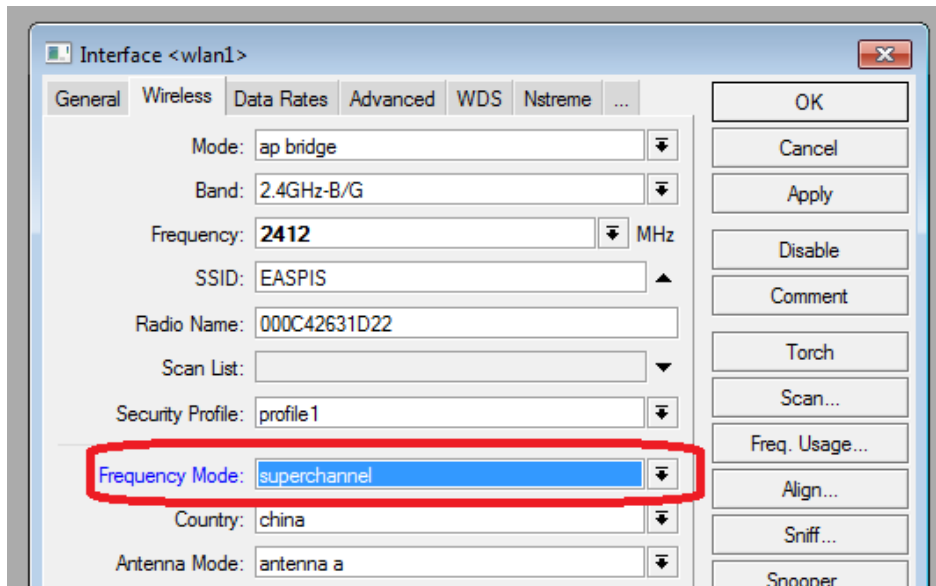
2.4GHz mode: 2412, 2417, 2422, 2427, 2432, 2437, 2442, 2447, 2452, 2457, 2462, 2467, 2472

2.4GHz-g-turbo mode: 2437

5GHz mode: 5745, 5765, 5785, 5805, 5825

5GHz-turbo mode: unknown

Hack 2. Frequency Selection

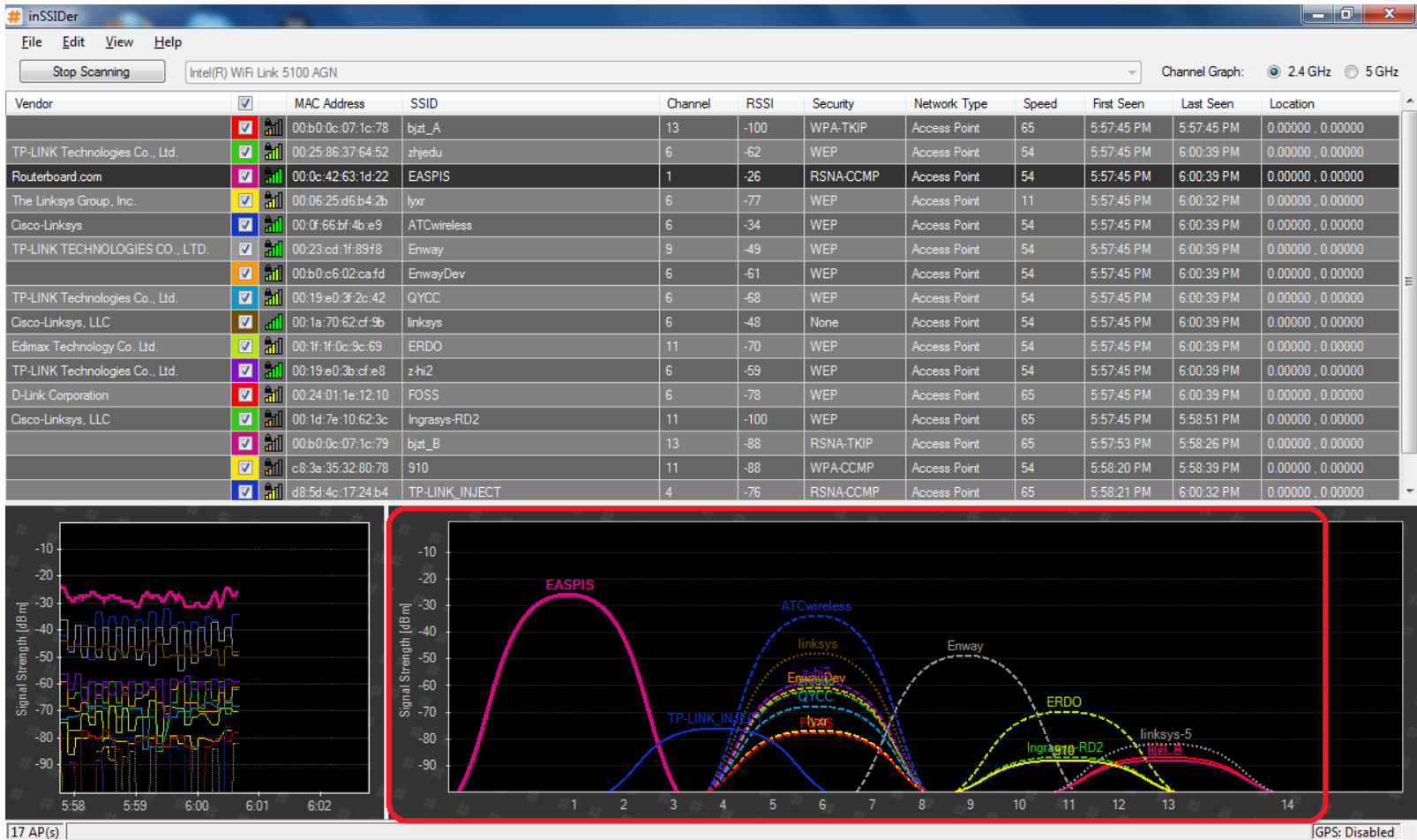


frequency-mode: *superchannel* -
Conformance Testing Mode. Allow all
channels supported by the card.

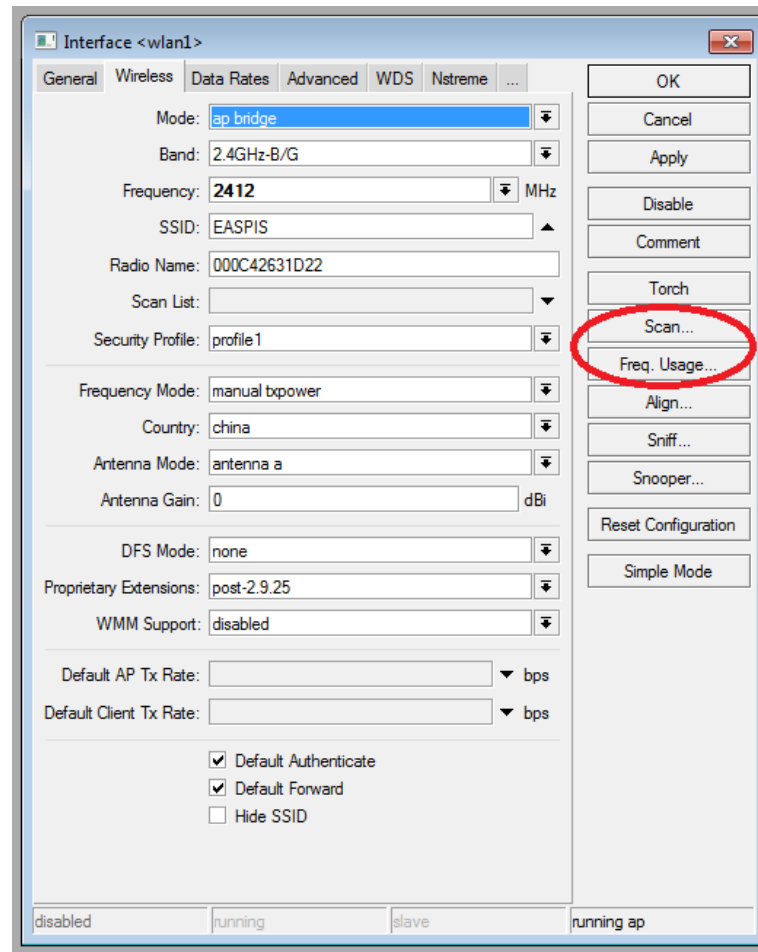
Allowed ranges on R52: [4920;6100],
[2192;2539].

This mode should only be used in controlled environments, or if you have a special permission to use it in your region. Before v4.3 this was called Custom Frequency Upgrade or Superchannel. Since RouterOS v4.3 this mode is available without special key upgrades to all installations.

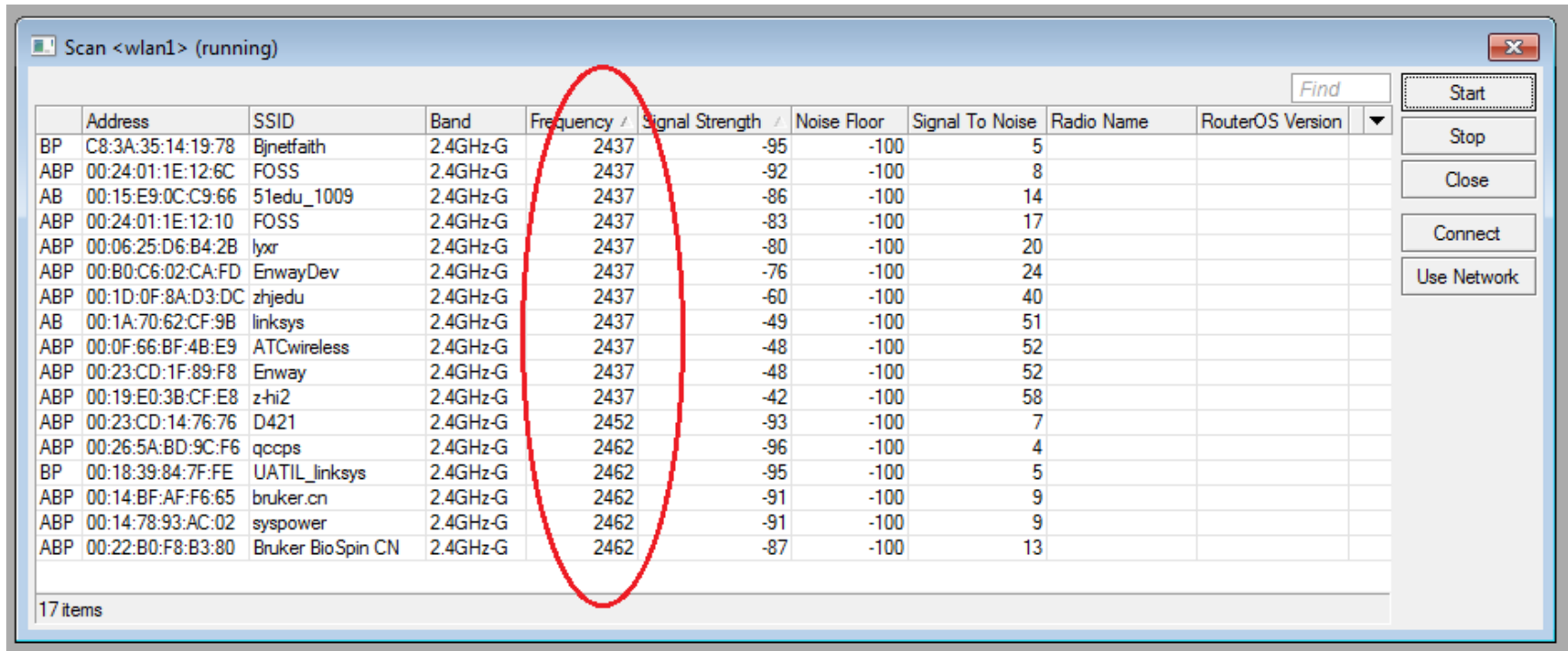
Hack 2. Frequency Selection



Hack 2. Frequency Selection



Hack 2. Frequency Selection



Scan <wlan1> (running)

	Address	SSID	Band	Frequency /	Signal Strength /	Noise Floor	Signal To Noise	Radio Name	RouterOS Version
BP	C8:3A:35:14:19:78	Bjnetfaith	2.4GHz-G	2437	-95	-100	5		
ABP	00:24:01:1E:12:6C	FOSS	2.4GHz-G	2437	-92	-100	8		
AB	00:15:E9:0C:C9:66	51edu_1009	2.4GHz-G	2437	-86	-100	14		
ABP	00:24:01:1E:12:10	FOSS	2.4GHz-G	2437	-83	-100	17		
ABP	00:06:25:D6:B4:2B	lyxr	2.4GHz-G	2437	-80	-100	20		
ABP	00:B0:C6:02:CA:FD	EnwayDev	2.4GHz-G	2437	-76	-100	24		
ABP	00:1D:0F:8A:D3:DC	zhjedu	2.4GHz-G	2437	-60	-100	40		
AB	00:1A:70:62:CF:9B	linksys	2.4GHz-G	2437	-49	-100	51		
ABP	00:0F:66:BF:4B:E9	ATCwireless	2.4GHz-G	2437	-48	-100	52		
ABP	00:23:CD:1F:89:F8	Enway	2.4GHz-G	2437	-48	-100	52		
ABP	00:19:E0:3B:CF:E8	z-hi2	2.4GHz-G	2437	-42	-100	58		
ABP	00:23:CD:14:76:76	D421	2.4GHz-G	2452	-93	-100	7		
ABP	00:26:5A:BD:9C:F6	qccps	2.4GHz-G	2462	-96	-100	4		
BP	00:18:39:84:7F:FE	UATIL_linksys	2.4GHz-G	2462	-95	-100	5		
ABP	00:14:BF:AF:F6:65	bruker.cn	2.4GHz-G	2462	-91	-100	9		
ABP	00:14:78:93:AC:02	syspower	2.4GHz-G	2462	-91	-100	9		
ABP	00:22:B0:F8:B3:80	Bruker BioSpin CN	2.4GHz-G	2462	-87	-100	13		

17 items

Find

Start

Stop

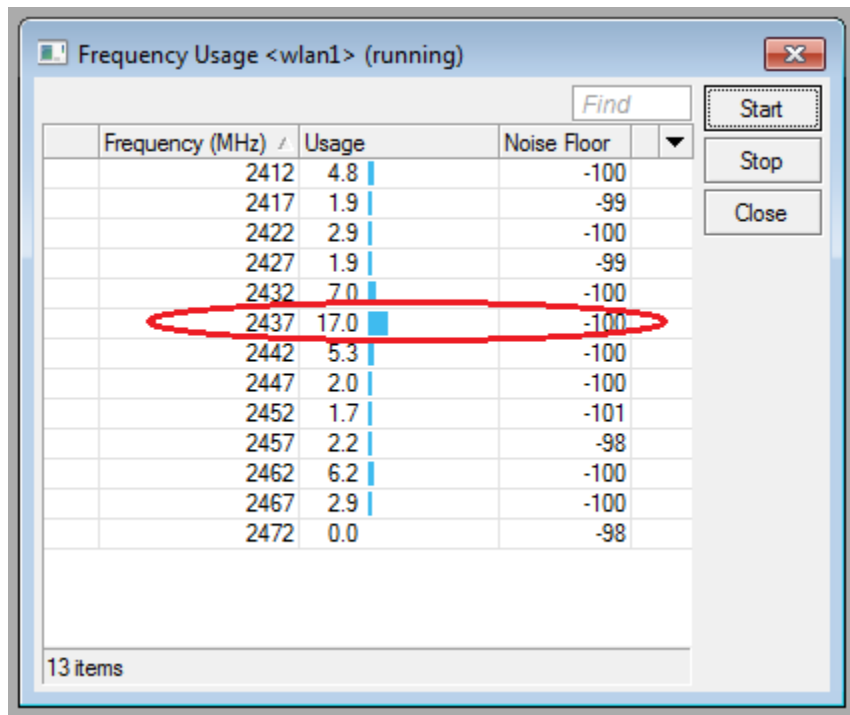
Close

Connect

Use Network

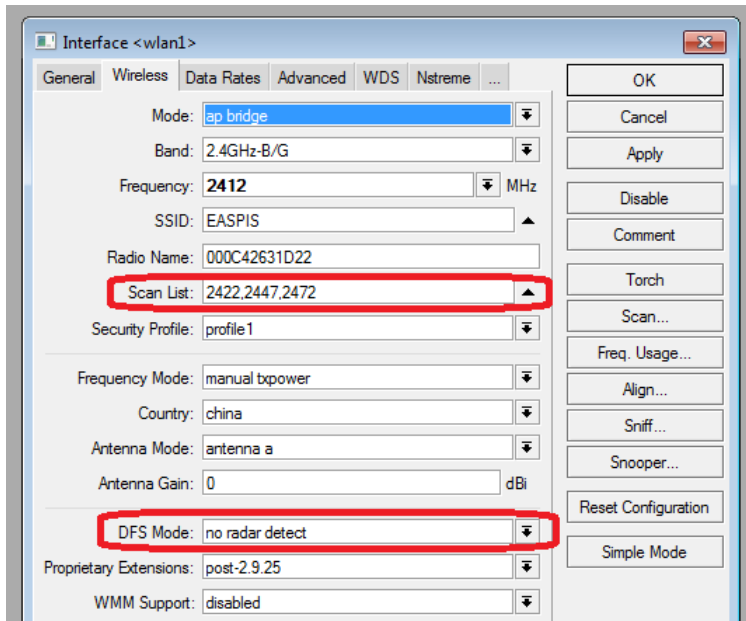
While scanning, the card unregisters itself from the access point (in station mode), or unregisters all clients (in bridge or ap-bridge mode). Thus, network connections are lost while scanning.

Hack 2. Frequency Selection



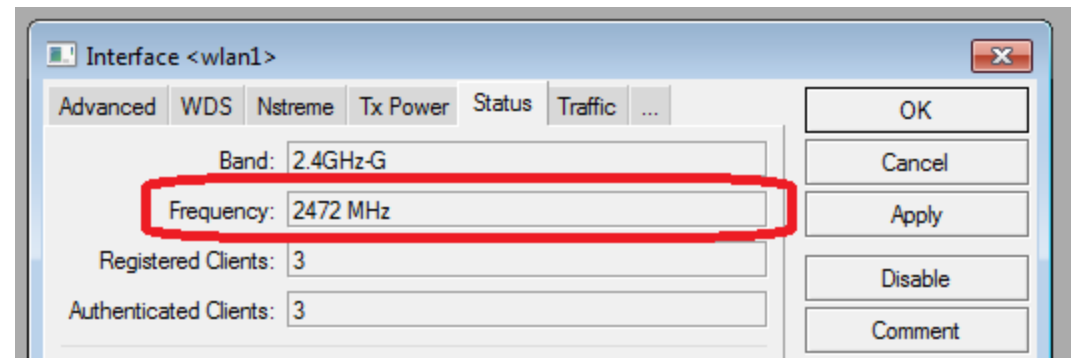
Approximately shows how loaded are the wireless channels.

Hack 2. Frequency Selection



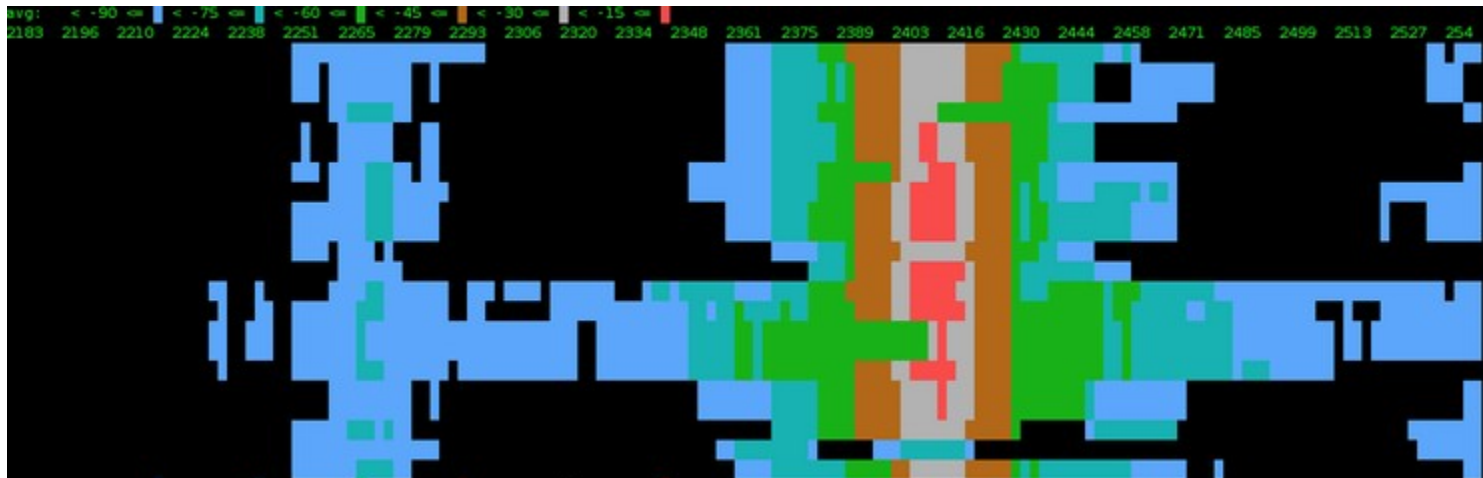
DFS (Dynamic Frequency Selection) - used for APs to dynamically select frequency at which this AP will operate.

no-radar-detect - AP scans channel list from "scan-list" and chooses the frequency which is with the lowest amount of other networks detected.



Spectrum Analyzer

- The spectrum analyzer can scan all frequencies supported by your wireless card, and plot them directly in console. Exact frequency span depends on card. Allowed ranges on R52N: [4790; 6085], [2182; 2549].
- Currently this feature is supported only **R52N** and **R2N**.
- http://wiki.mikrotik.com/wiki/Spectrum_analyzer
- <http://www.tiktube.com/index.php?video=301>



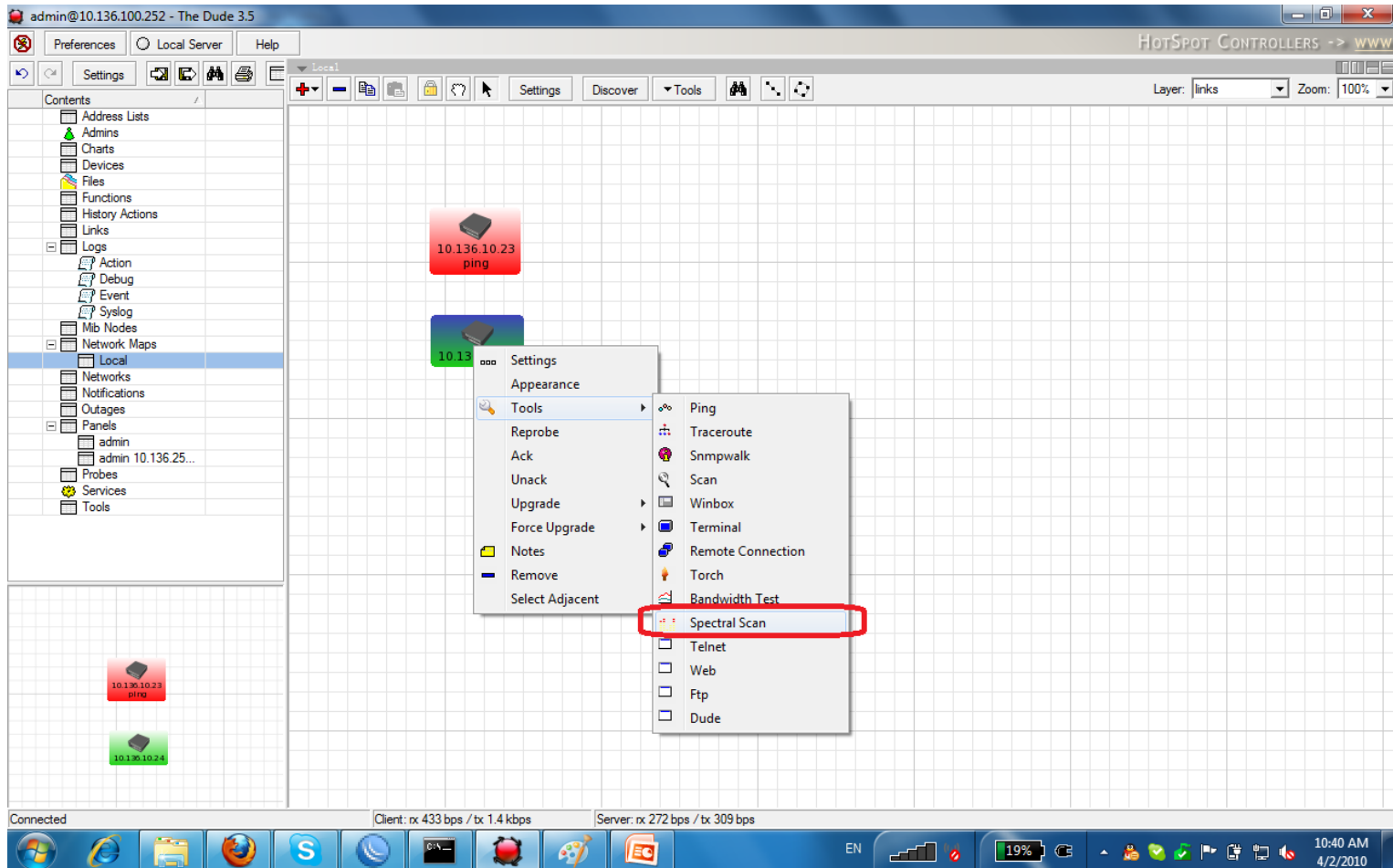
Spectrum Analyzer

The screenshot shows the RouterOS WinBox interface. On the left is a vertical menu with categories like Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, VPLS, Routing, System, Queues, Files, Log, Radius, Tools, and a 'RouterOS WinBox' label. The main area is a terminal window titled 'Terminal' with a close button. The terminal shows the following command and output:

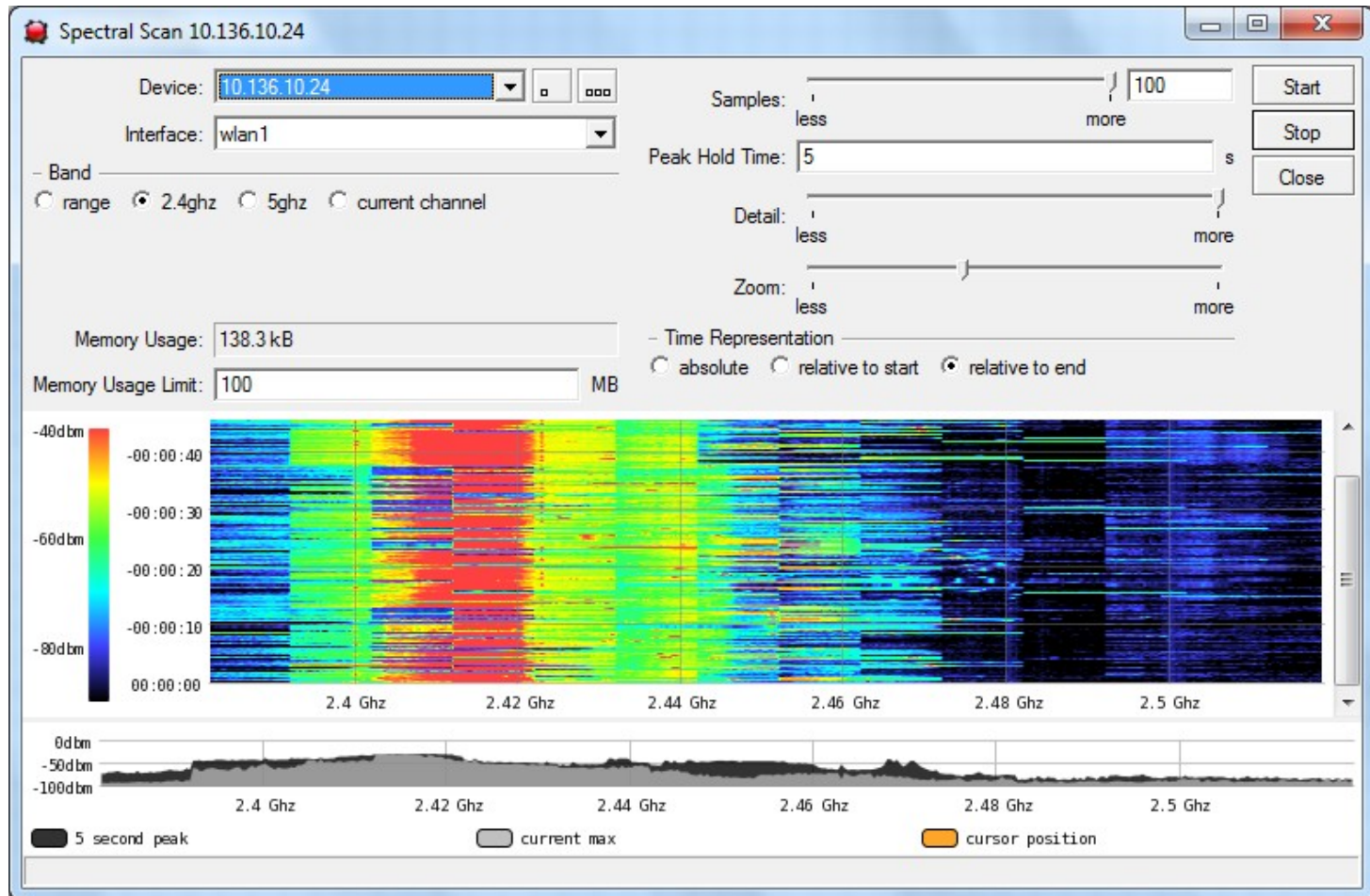
```
[admin@MikroTik] > interface wireless spectral-scan
number: wlan2
FREQ DBM GRAPH
2189 -99 ..... :
2205 -99 ..... :
2221 -99 ..... :
2237 -101 ..... :
2253 -99 ..... :
2269 -98 ..... :
2285 -99 ..... :
2301 -101 ..... :
2317 -99 ..... :
2333 -98 ..... :
2349 -99 ..... :
2365 -100 ..... :
2381 -101 ..... :
2397 -99 ..... :
2413 -99 ..... :
2429 -101 ..... :
2445 -103 ..... :
2461 -103 ..... :
2476 -104 ..... :
2493 -101 ..... :
2508 -100 ..... :
2524 -102 ..... :
2540 -101 ..... :
```

The terminal window also shows the CPU usage as 0% and a 'Hide Passwords' checkbox checked. The terminal prompt is currently at [admin@MikroTik] > with a pink cursor.

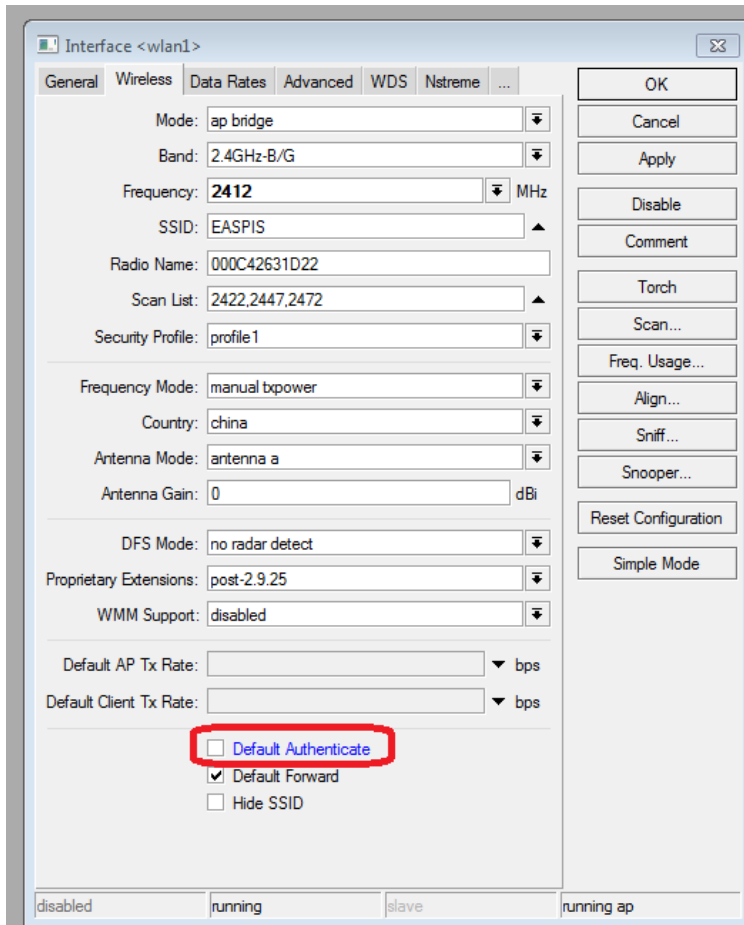
Spectrum Analyzer



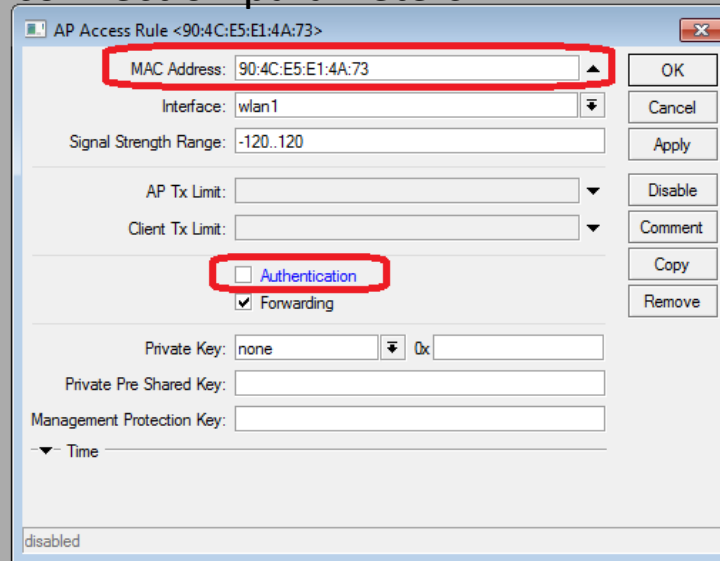
Spectrum Analyzer



Hack 3. Access list and Security profile



Access list is used by access point to restrict allowed connections from other devices, and to control connection parameters.



default-authentication - this is the value of authentication for clients that do not match any entry in the access-list.

Hack 3. Access list and Security profile

New Security Profile

General | RADIUS | EAP | Static Keys

Name: profile2

Mode: dynamic keys

Authentication Types

WPA PSK WPA2 PSK

WPA EAP WPA2 EAP

Unicast Ciphers

tkip aes ccm

Group Ciphers

tkip aes ccm

WPA Pre-Shared Key: iR3EnKyAy8BKmOzM

WPA2 Pre-Shared Key: iR3EnKyAy8BKmOzM

Supplicant Identity:

Group Key Update: 00:05:00

Management Protection: allowed

Management Protection Key:

private-pre-shared-key - private Pre shared key for that station.

AP Access Rule <90:4C:E5:E1:4A:73>

MAC Address: 90:4C:E5:E1:4A:73

Interface: wlan1

Signal Strength Range: -120..120

AP Tx Limit:

Client Tx Limit:

Authentication

Forwarding

Private Key: none

Private Pre Shared Key: aX4T6sE096bopSJ

Management Protection Key:

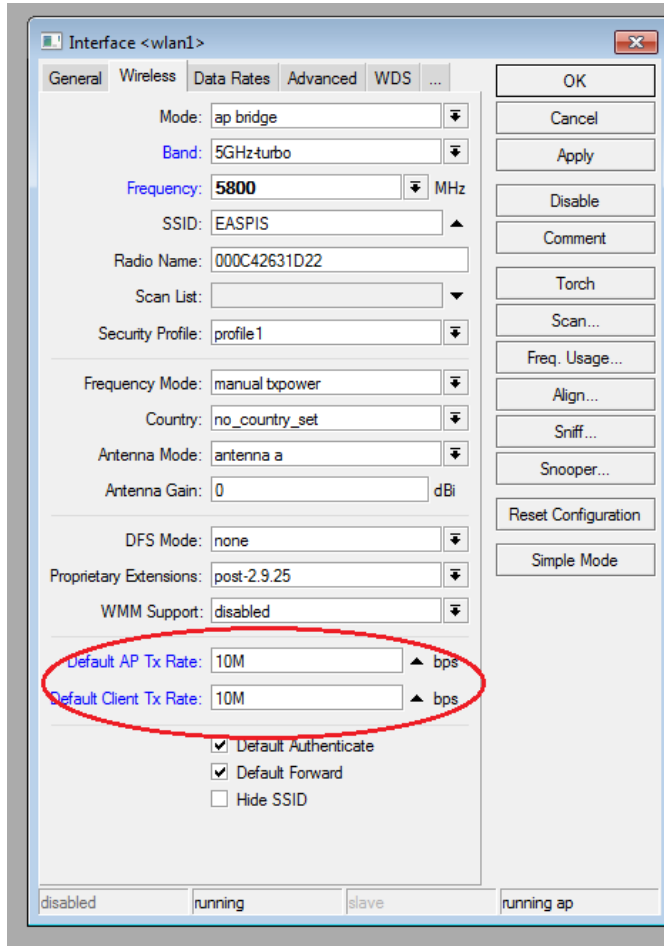
Time

disabled

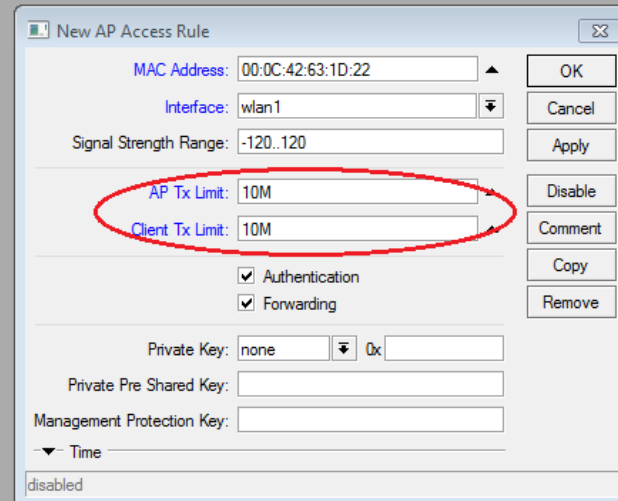
aes-ccm - more secure WPA encryption protocol, based on the reliable AES (Advanced Encryption Standard).

wpa-pre-shared-key, wpa2-pre-shared-key - which is used as the WPA Pre Shared Key. Use 8-63 alphanumeric characters (0-9, a-z)

Hack 4. Wireless client bandwidth control



ap-tx-limit - limits data rate for this wireless client (in bps)



client-tx-limit - limits this client's transmit data rate (in bps). Works only if the client is also a RouterBOARD

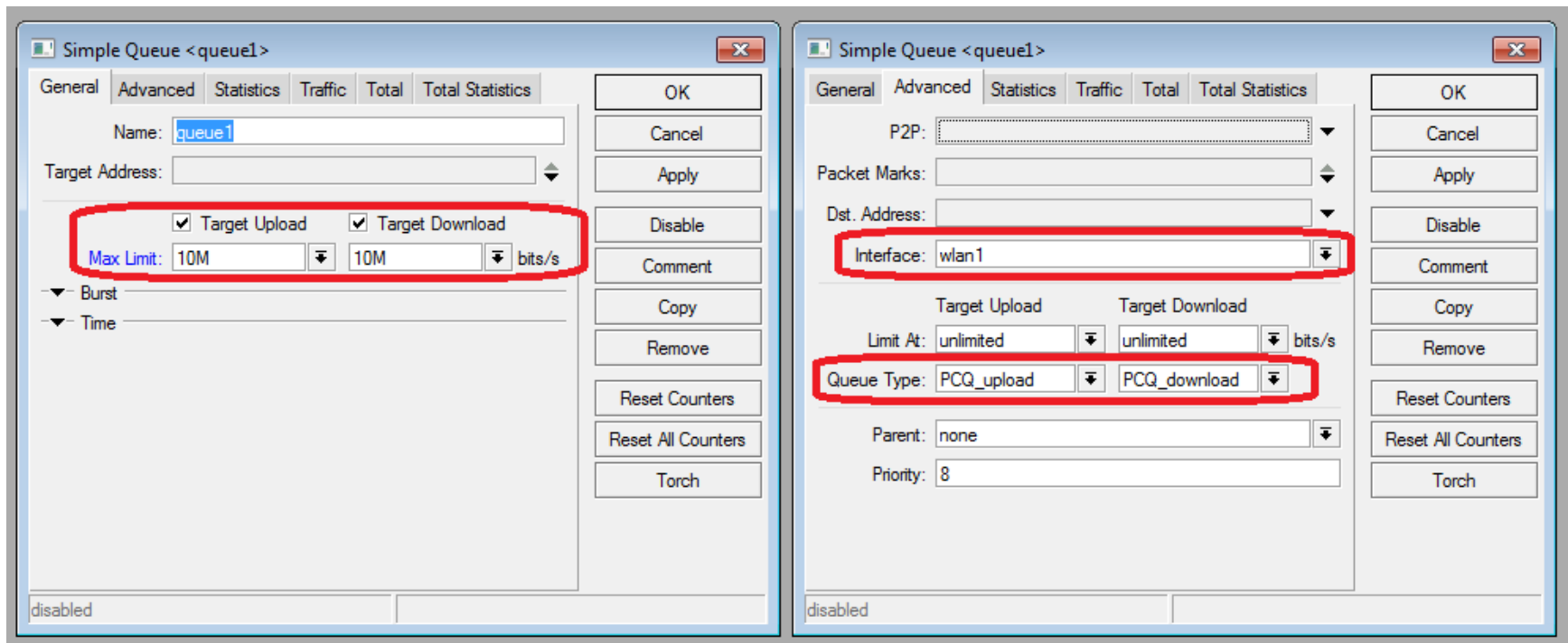
Hack 4. Wireless client bandwidth control

- **Per Connection Queue (PCQ)** is a queuing discipline that can be used to dynamically equalize or shape traffic for multiple users, using little administration. It is possible to divide PCQ scenarios into three major groups: equal bandwidth for a number of users, certain bandwidth equal distribution between users, unknown bandwidth equal distribution between users.

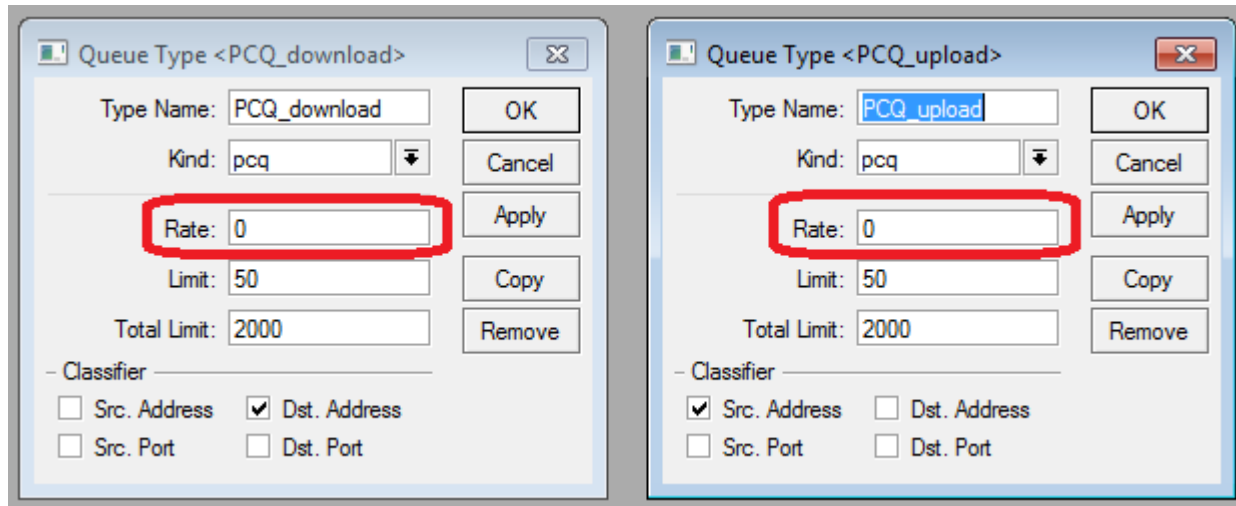
http://wiki.mikrotik.com/wiki/PCQ_Examples

http://mum.mikrotik.com/presentations/CZ09/QoS_Megis.pdf

Hack 4. Wireless client bandwidth control



Hack 4. Wireless client bandwidth control



Hack 5. Virtual AP and VLAN

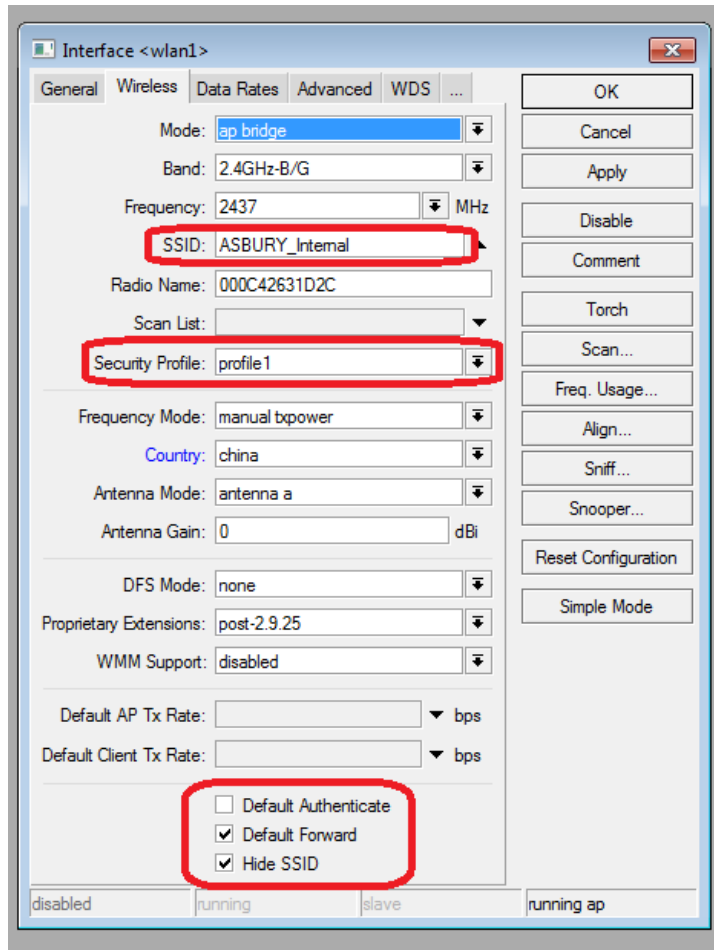
- Virtual Access Point (VAP) interface is used to have an additional AP. You can create a new AP with different **ssid** and **mac-address**. It can be compared with a VLAN where the **ssid** from VAP is the VLAN **tag** and the hardware interface is the VLAN switch.
- You can add up to 128 VAP interfaces for each hardware interface.
- The VAP MAC address is set by default to the same address as the physical interface has, with the second bit of the first byte set (i.e., the MAC address would start with 02). If that address is already used by some other wireless or VAP interface, it is increased by 1 until a free spot is found. When manually assigning MAC address, keep in mind that it should have the first bit of the first byte unset (so it should not be like 01, or A3). Note also that it is recommended to keep the MAC address of VAP as similar (in terms of bit values) to the MAC address of the physical interface it is put onto, as possible, because the more different the addresses are, the more it affects performance.

Hack 5. Virtual AP and VLAN

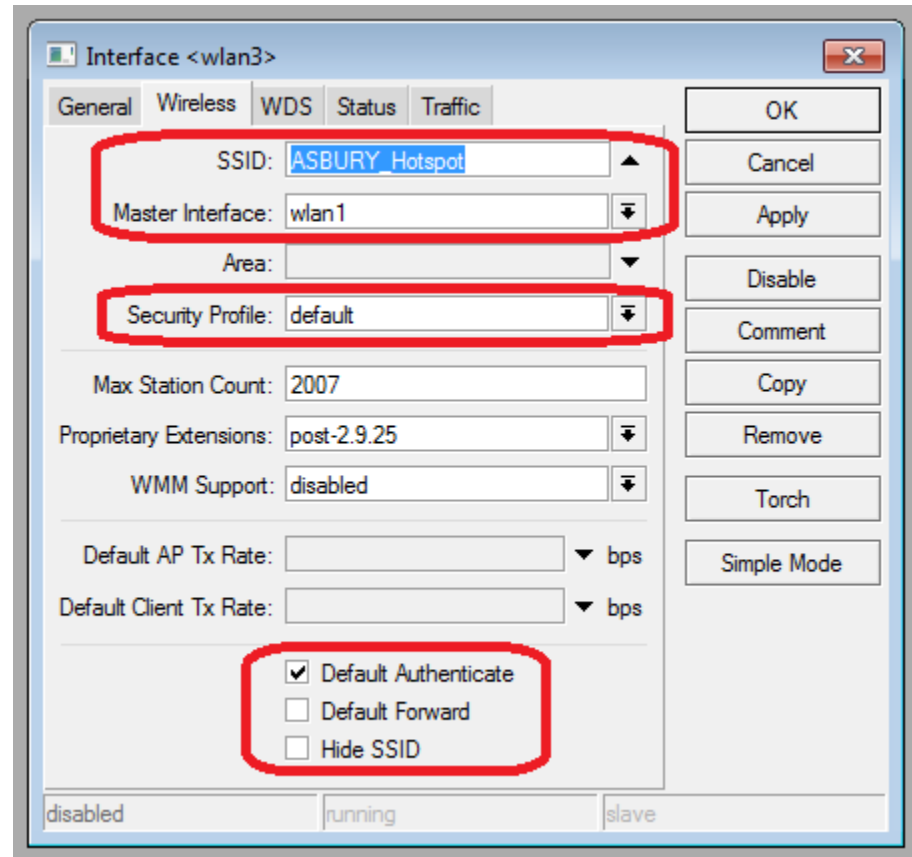
The screenshot shows the 'Wireless Tables' window with the following data:

Name	Type	Mode	Band	Frequency (MHz)	SSID
wlan1	Wireless (Atheros AR5413)	ap bridge	2.4GHz-B/G	2437	ASBURY_Internal
wlan3	VirtualAP				ASBURY_Hotspot
wlan4	VirtualAP				ASBURY_VoIP
wlan2	Wireless (Atheros AR5413)	station	5GHz	5180	

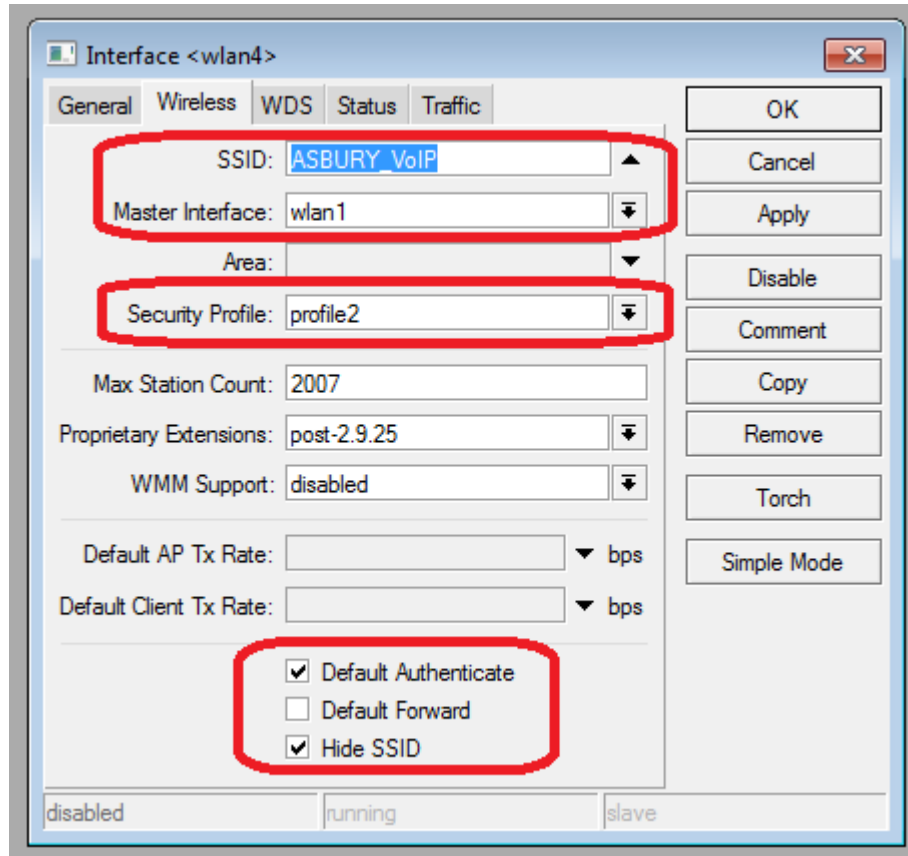
Hack 5. Virtual AP and VLAN



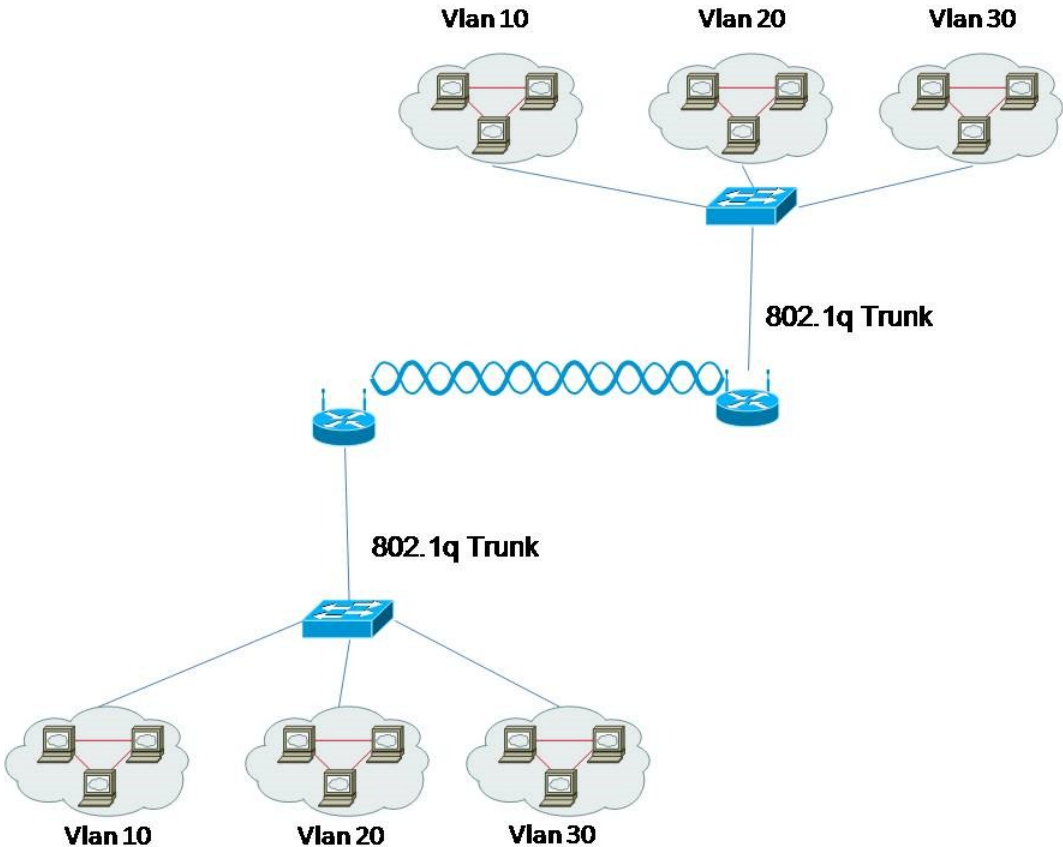
Hack 5. Virtual AP and VLAN



Hack 5. Virtual AP and VLAN



Hack 5. Virtual AP and VLAN

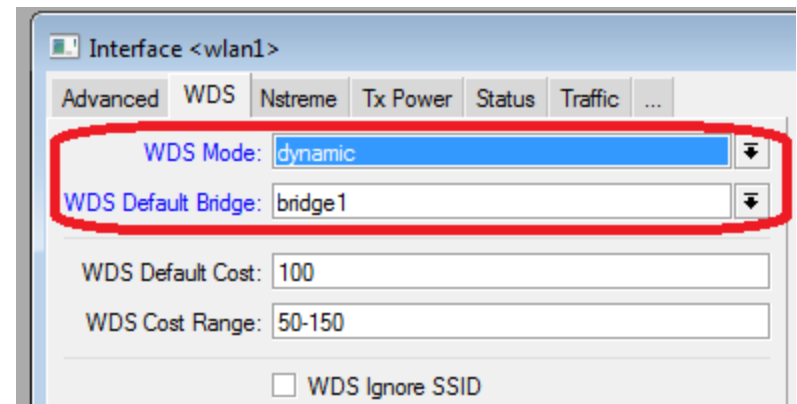
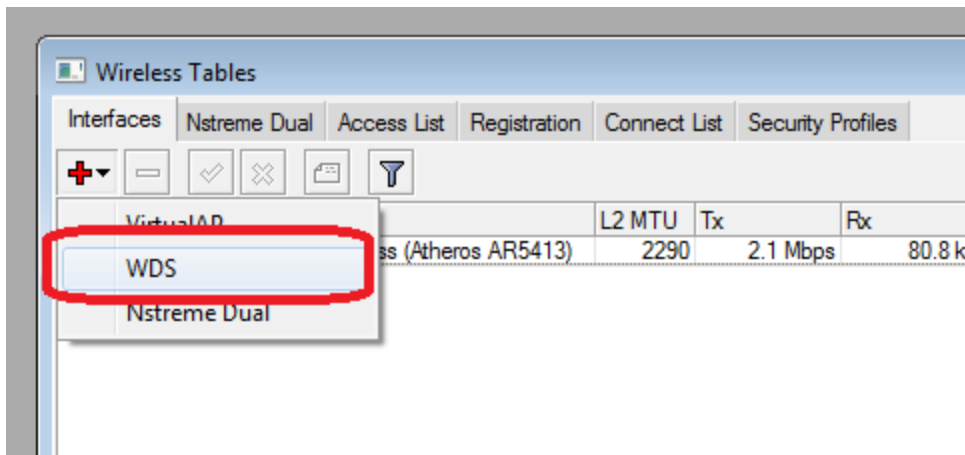


Hack 6. Wireless Distribution System

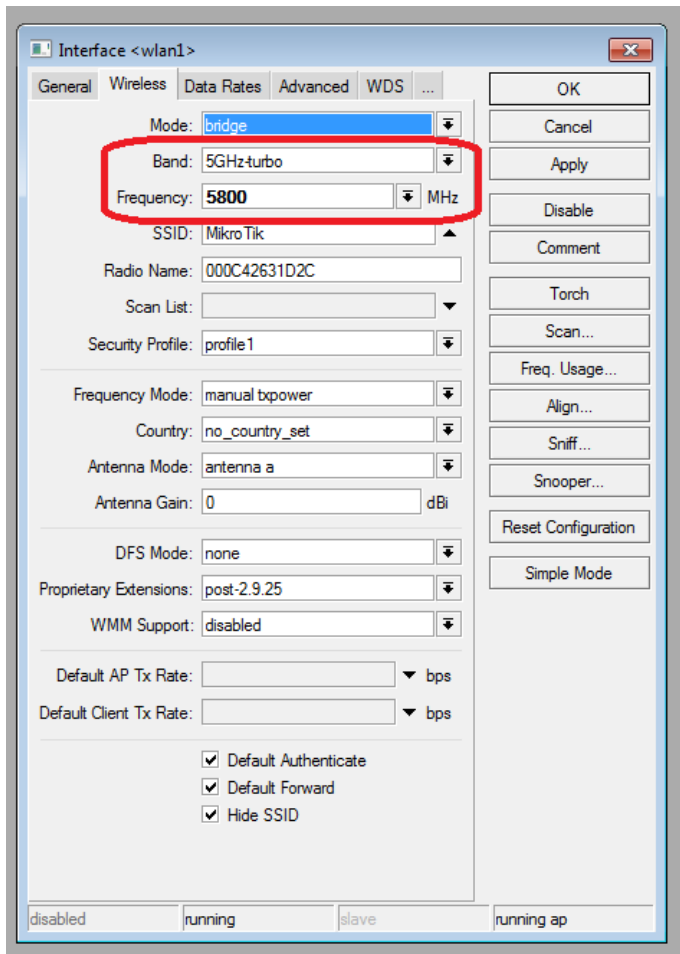
- The IEEE 802.11 standard limitation makes it impossible for wireless cards in station mode to work as expected when bridged. That means that if you need to create a bridge, you should not use station mode on that machine. In case you need a bridge on a wireless station, use **station-wds** mode (may only be used in the AP supports WDS). Bridging on the AP side works fine.
- WDS (Wireless Distribution System) allows packets to pass from one wireless AP (Access Point) to another, just as if the APs were ports on a wired Ethernet switch. APs must use the same standard (802.11a, 802.11b or 802.11g) and work on the same frequencies in order to connect to each other.
- As the routers which are in WDS mode have to communicate at equal frequencies, it is not recommended to use **WDS** and **DFS** simultaneously - it is most probable that these routers will not connect to each other.

Hack 6. Wireless Distribution System

- There are two possibilities to create a WDS interface:
 - **dynamic** - is created 'on the fly'
 - **static** - is created manually
- If you want to use dynamic WDS in a bridge, set the **wds-default-bridge** value to desired bridge interface name. When the link will go down and then it comes up, the dynamic WDS interface will be put in the specified bridge automatically.



Hack 7. Turbo mode (up to 108Mbps)



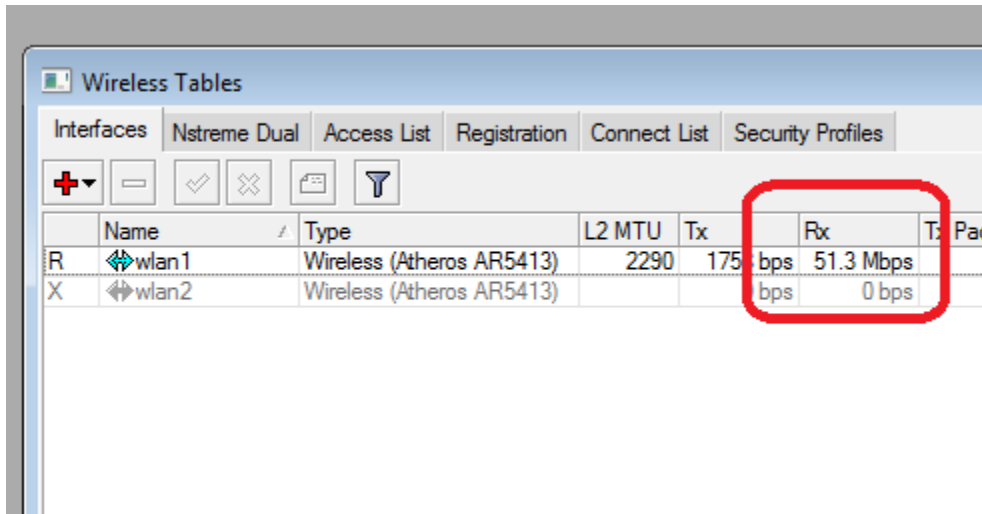
5ghz-turbo - IEEE 802.11a in Atheros proprietary turbo mode (up to 108Mbps)

frequency: 5210, 5250, 5290, 5760, 5800

2.4ghz-g-turbo - IEEE 802.11g in Atheros proprietary turbo mode (up to 108Mbps)

frequency: 2437

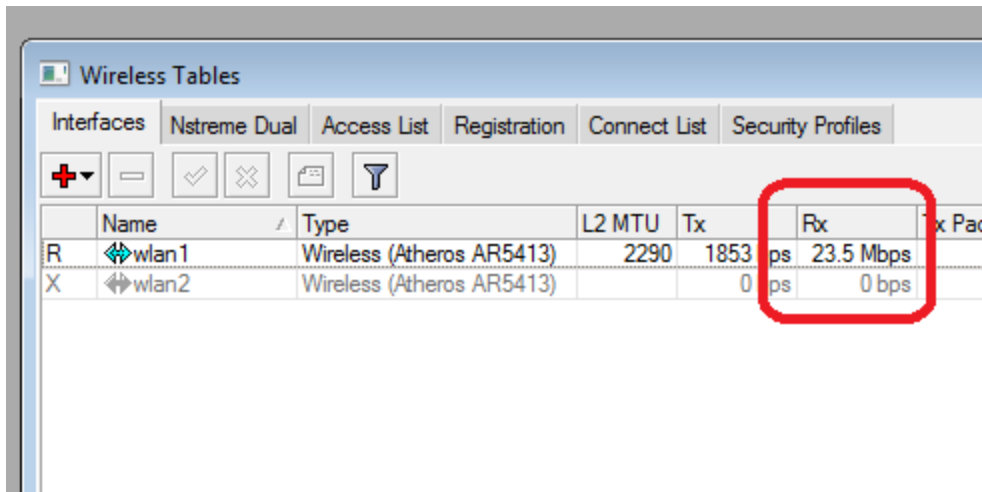
Hack 7. Turbo mode (up to 108Mbps)



The screenshot shows the 'Wireless Tables' window in Mikrotik WinBox. The 'Interfaces' tab is selected. A table lists two wireless interfaces: wlan1 and wlan2. The Rx rate for wlan1 is highlighted with a red box and shows 51.3 Mbps.

Name	Type	L2 MTU	Tx	Rx	Tx Pac
wlan1	Wireless (Atheros AR5413)	2290	175 bps	51.3 Mbps	
wlan2	Wireless (Atheros AR5413)			0 bps	

5ghz-turbo - IEEE 802.11a in Atheros proprietary turbo mode (up to 108Mbps)

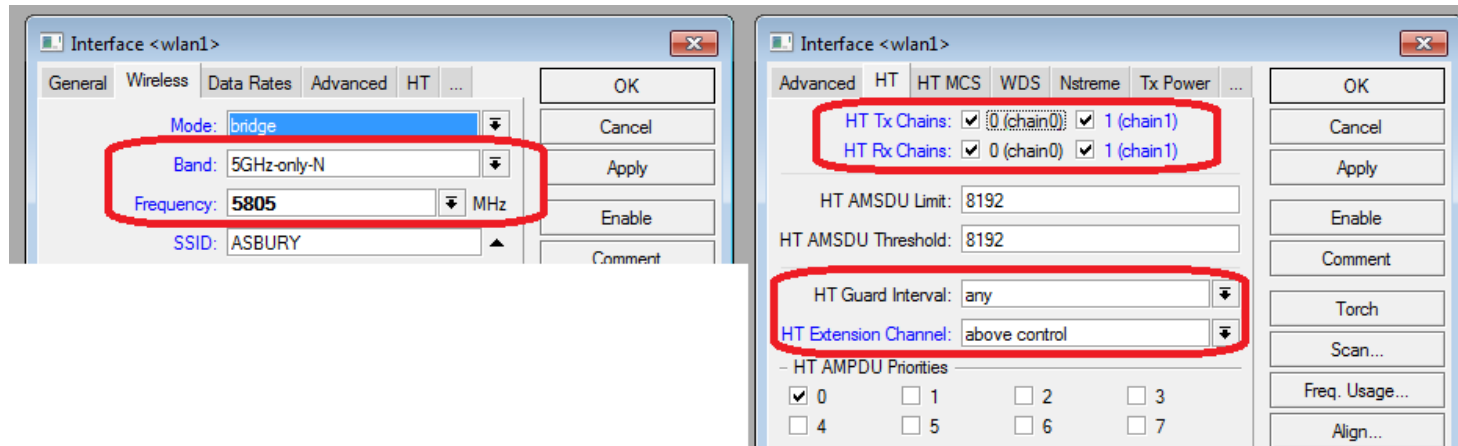


The screenshot shows the 'Wireless Tables' window in Mikrotik WinBox. The 'Interfaces' tab is selected. A table lists two wireless interfaces: wlan1 and wlan2. The Rx rate for wlan1 is highlighted with a red box and shows 23.5 Mbps.

Name	Type	L2 MTU	Tx	Rx	Tx Pac
wlan1	Wireless (Atheros AR5413)	2290	1853 ps	23.5 Mbps	
wlan2	Wireless (Atheros AR5413)		0 ps	0 bps	

5ghz - IEEE 802.11a up to 54 Mbps

Hack 8. 802.11n (up to 300Mbps)



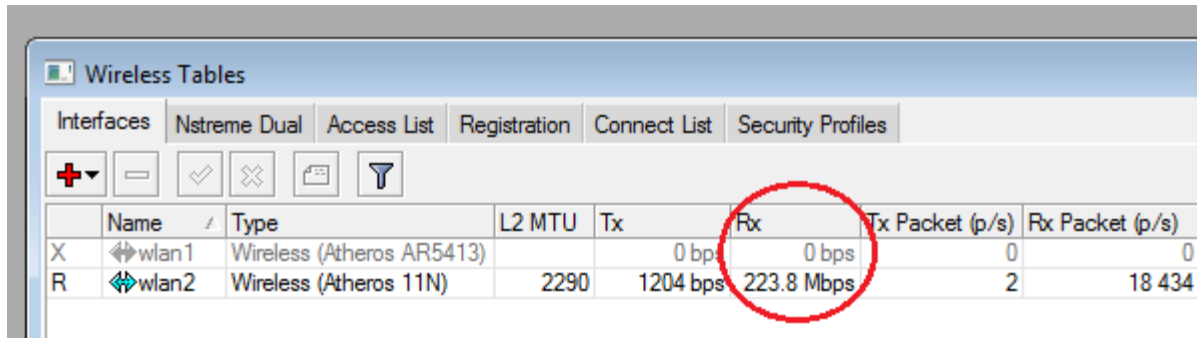
ht-rxchains - which antennas to use for receive.

ht-txchains - which antennas to use for transmit.

ht-guard-interval - whether to allow use of short guard interval. "any" will use either short or long, depending on data rate, "long" will use long.

ht-extension-channel - whether to use additional 20MHz extension channel and if it should be located below or above control (main) channel. Extension channel allows 11n device to use 40MHz of spectrum in total thus increasing max throughput.

Hack 8. 802.11n (up to 300Mbps)



The screenshot shows a window titled "Wireless Tables" with several tabs: "Interfaces", "Nstreme Dual", "Access List", "Registration", "Connect List", and "Security Profiles". Below the tabs are several icons: a red plus sign, a minus sign, a checkmark, a cross, a document, and a funnel. A table displays the following data:

	Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
X	wlan1	Wireless (Atheros AR5413)		0 bps	0 bps	0	0
R	wlan2	Wireless (Atheros 11N)	2290	1204 bps	223.8 Mbps	2	18 434

Up to 200Mbps of actual throughput.

Hack 9. Dual radio Point-to-Point mode

- The Nstreme protocol is MikroTik wireless protocol aimed to improve point-to-point and point-to-multipoint wireless links. **Advanced version of Nstreme, called Nstreme2** works with a pair of wireless cards - one for transmitting data and one for receiving.
- Two radios in **nstreme-dual-slave** mode can be grouped together to make nstreme2 Point-to-Point connection. To put wireless interfaces into a nstreme2 group, you should set their **mode** to **nstreme-dual-slave**. Many parameters from **/interface wireless** menu are ignored, using the nstreme2, except:
 - frequency-mode
 - country
 - antenna-gain
 - tx-power
 - tx-power-mode
 - antenna-mode

Hack 9. Dual radio Point-to-Point mode

The image displays two screenshots of the 'Interface <nstreme1>' configuration window, illustrating the setup for Dual radio Point-to-Point mode.

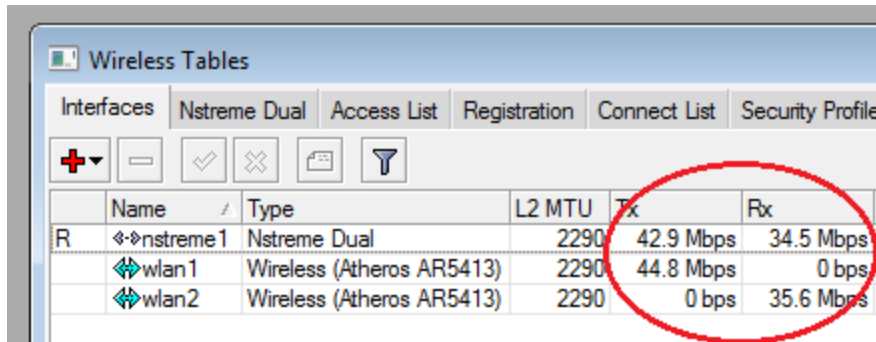
Left Screenshot (Configuration):

- Tab: Nstreme Dual
- Tx Radio: wlan1
- Rx Radio: wlan2
- Remote MAC: 00:0C:42:63:1D:1B
- Tx Band: 2.4GHz-G-turbo
- Tx Frequency: 2437 MHz
- Rx Band: 5GHz-turbo
- Rx Frequency: 5800
- Disable CSMA
- Framer Policy: none
- Framer Limit: 2560

Right Screenshot (Status/Statistics):

- Tab: Nstreme Dual
- Rx Signal Strength: -40 dBm
- Tx Signal Strength: -32 dBm
- Rx Rate: 54Mbps*2
- Tx Rate: 54Mbps*2
- Packets (Tx/Rx): 507387/532618
- Bytes (Tx/Rx): 767599515/805658024
- Frames (Tx/Rx): 507497/532680
- Frame Bytes (Tx/Rx): 788914169/828030460
- Hw. Frames (Tx/Rx): 810998/721908
- Hw. Frame Bytes (Tx/Rx): 889197189/844909628
- Tx Retries Timeout: 6524
- Tx Retries Lost: 57257
- Rx Bad Seqs: 0
- Rx Duplicates: 6149
- Connected

Hack 9. Dual radio Point-to-Point mode



Name	Type	L2 MTU	Tx	Rx
nstreme1	Nstreme Dual	2290	42.9 Mbps	34.5 Mbps
wlan1	Wireless (Atheros AR5413)	2290	44.8 Mbps	0 bps
wlan2	Wireless (Atheros AR5413)	2290	0 bps	35.6 Mbps

WDS cannot be used on Nstreme-dual links.

The difference between **tx-freq** and **rx-freq** should be about 200MHz (more is recommended) because of the interference that may occur!

You can use different bands for rx and tx links. For example, transmit in **2.4ghz-g-turbo** and receive data, using **5ghz-turbo** band.

End

Click to edit Master subtitle style

Thank you for participating