RouterBOARD Wireless Hacks

Jesse Liu
Convergingstream
MikroTik Distributor

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

<table>
<thead>
<tr>
<th>Contents:</th>
<th>Asia</th>
<th>ConvergingStream Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>North America</strong></td>
<td><strong>EDCwifi</strong></td>
<td></td>
</tr>
<tr>
<td>Canada</td>
<td>Shenzhen, China</td>
<td>Beijing, China</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>RouterBOARD components, training</td>
<td>RouterBOARD components</td>
</tr>
<tr>
<td>Mexico</td>
<td>Tel: 86-755-82642594</td>
<td>Tel: 010 6894 8781</td>
</tr>
<tr>
<td>Mexico</td>
<td>Write e-mail</td>
<td>Write e-mail</td>
</tr>
<tr>
<td><strong>South America</strong></td>
<td><strong>CDNAT</strong></td>
<td></td>
</tr>
<tr>
<td>Argentina</td>
<td>Chengdu, China</td>
<td></td>
</tr>
<tr>
<td>Bolivia</td>
<td>RouterBOARD components</td>
<td></td>
</tr>
<tr>
<td>Brazil</td>
<td>Tel: 86-28-87777784</td>
<td></td>
</tr>
<tr>
<td>Chile</td>
<td>Write e-mail</td>
<td></td>
</tr>
<tr>
<td>Colombia</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ecuador</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paraguay</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peru</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uruguay</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Venezuela</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Africa</strong></td>
<td><strong>XBase</strong></td>
<td></td>
</tr>
<tr>
<td>Cameroon</td>
<td>Changsha, China</td>
<td></td>
</tr>
<tr>
<td>Egypt</td>
<td>RouterBOARD components</td>
<td></td>
</tr>
<tr>
<td>Gabon</td>
<td>Tel: +86-4006770099</td>
<td></td>
</tr>
<tr>
<td>Kenya</td>
<td>Write e-mail</td>
<td></td>
</tr>
<tr>
<td>Nigeria</td>
<td></td>
<td></td>
</tr>
<tr>
<td>South Africa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tanzania</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Asia</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Afghanistan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bangladesh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>China</td>
<td></td>
<td></td>
</tr>
<tr>
<td>India</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

北京恒通安信科技有限公司
## MikroTik certified Integrator

<table>
<thead>
<tr>
<th>Company</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Uniterm Direct</strong></td>
<td>Uniterm in South Africa offer cases, antennas and preassembled kits based on RouterOS and RouterBOARD</td>
</tr>
<tr>
<td><strong>Discomp</strong></td>
<td>Discomp make a variety of CPE/AP solutions, including this outdoor client, the &quot;MaxLink MaxStation Mikron&quot;, with 19dBi antenna.</td>
</tr>
<tr>
<td><strong>ConvergingStream</strong></td>
<td>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+)</td>
</tr>
<tr>
<td><strong>Hana Wireless</strong></td>
<td>Hana Wireless from the USA make a variety of CPE/AP solutions based on MikroTik RouterBOARD</td>
</tr>
<tr>
<td><strong>Xagyl</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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

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

http://www.metageek.net/products/inssider
Hack 2. Frequency Selection

![Image of frequency selection in an interface]
Hack 2. Frequency Selection

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**.

Spectrum Analyzer
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

**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)

**private-pre-shared-key** - private Pre shared key for that station.
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
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
Hack 5. Virtual AP and VLAN

[Image of a network interface configuration screen with highlighted settings: SSID set to ASBURY_Internal, Security Profiles set to profile1, and options for Default Authenticate, Default Forward, and Hide SSID checked.]

27
Hack 5. Virtual AP and VLAN
Hack 5. Virtual AP and VLAN
Hack 5. Virtual AP and VLAN

http://wiki.mikrotik.com/wiki/802.1q_Trunk_extension_over_Wireless_P2P_Link
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)

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

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)

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
Hack 9. Dual radio Point-to-Point mode

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

Thank you for participating