Wireless Workshop

MUM 2012 - Warsaw
Uldis Cernevsksis
MikroTik
Topics

• PTP and PTMP connections
• Transparent wireless links
• Throughput discussion
• Disconnection problems
• Different setup discussion
• Useful configuration settings and features
Connection Types

Point to Point (PTP)  Point to Multi Point (PTMP)
PTP/PTMP connection modes

- AP-bridge/Bridge <-> Station
- AP-bridge/Bridge <-> Station-wds/Station-bridge
- AP-bridge/Bridge <-> Station-pseudobridge
- AP-bridge/Bridge <-> AP-bridge/Bridge
- AP-bridge <-> WDS-slave
RouterOS license requirements

• PTP link requires at least Level 3
  – Example: Bridge <-> Station

• PTMP link requires on AP at least Level 4 and on clients at least Level 3
  – Example: AP-bridge <-> Station
Wireless Standards and Protocols

- RouterOS PTP and PTMP supports
  - 802.11 a/b/g/n standards
  - 802.11, Nstreme and Nv2 protocols
Regular PTMP setup
Mesh PTMP setup
Wireless Setup Type - Routing

[Diagram showing network setup with IP addresses 10.0.0.1/24 to 10.0.2.2/24]
Wireless Setup Type - Bridging

INTERNET

10.0.0.1/24

Bridge 10.0.0.2/24

10.0.0.11/24

Bridge 10.0.0.3/24

10.0.0.12/24
Wireless Setup Types

• Bridging
  • Advantage
    – Less IP configuration needed
  • Disadvantage
    – Clients broadcast traffic or flood can lower wireless network performance
    – Not suitable for large network

• Routing
  • Advantage
    – No broadcast traffic or flood that could lower wireless network performance
  • Disadvantage
    – More configuration needed: multiple IP networks or use of routing protocols
Transparent Wireless Links

- Less configuration needed
- Extends Layer 2 protocol to clients (wireless ethernet switch)
- Suitable for PPPoE access
Transparent Wireless Links Setups

• Bridge <-> Station-pseudobridge
• Bridge <-> Station using EOIP
• Bridge <-> Bridge
• Bridge <-> Station-wds
• Bridge <-> Station-bridge
Station-pseudobridge

• This mode is not considered true transparent bridge

• Limitations
  – MAC address translation for IPv4 packets by using IPv4-to-MAC mapping table on station
  – single MAC address translation for the rest of protocols

• Should be avoided when possible

• Use only when non RouterOS AP is used
Station-pseudobridge configuration

• On station router set wireless mode to station-pseudobridge
• Bridge wireless interface with ethernet interface to make transparent link
• Use station-pseudobridge-clone if you want to clone the MAC address of the client and use for connecting to AP with the cloned MAC address
EOIP bridging

• The EoIP protocol encapsulates Ethernet frames in GRE packets (just like PPTP) and sends them to the remote side of the EoIP tunnel

• EOIP adds 42 byte overhead – frame fragmentation will be used
EOIP bridging setup
EOIP bridging configuration

- Configure wireless AP - Station setup
- Add IP address on AP and on Station
- Create EOIP tunnel between AP and Station
- Bridge EOIP tunnel with ethernet interface to make transparent link
Bridge <-> Bridge

- Wireless Distribution System (WDS) used for making wireless communication between two APs
- Needs WDS interfaces on both ends to enable communication
- No overhead compared to EOIP
- Works only with 802.11 wireless protocol
Bridge <-> Bridge setup
Bridge <-> Bridge configuration

- Configure both wireless APs to use the same SSID, frequency, band
- Enable WDS mode on both APs
- Create WDS interfaces on both APs
- Bridge WDS interfaces with the ethernet interface to make transparent link
Station-wds

- When station-wds connection is established with an AP, AP makes a individual WDS interface on AP for this client data communication
- AP should have WDS mode enabled
- Can be connected only to RouterOS AP based devices
- Less configuration needed on the client device – no WDS device needed on the client router
Station-wds setup
Station-wds configuration

• On AP enable the WDS mode
• Create WDS interfaces on AP
• Configure client to use station-wds mode
• Bridge WDS interface on AP with the ethernet interface and wireless interface with ethernet interface on client to make transparent link
Station-bridge

• AP maintains forwarding table with information on what MAC addresses are reachable over which station device
• AP should have bridge-mode parameter enabled in order to accept station-bridge clients
• Can be connected only to RouterOS AP based devices
• Even less configuration needed compared to station-wds mode
Station-bridge setup
Station-bridge configuration

• On AP enable the bridge-mode parameter
• Configure client to use station-bridge mode
• Bridge wireless interface with ethernet interface to make transparent link
## Wireless protocol limitations on transparent links

<table>
<thead>
<tr>
<th></th>
<th>802.11</th>
<th>ROS 802.11</th>
<th>Nstreme</th>
<th>Nv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>station</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>station-wds</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>station-pseudobridge</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>station-pseudobridge-clone</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
<tr>
<td>station-bridge</td>
<td>V</td>
<td>V</td>
<td>V</td>
<td>V</td>
</tr>
</tbody>
</table>
Throughput discussion

• Tips and notes on how to get the max wireless throughput:
  – Use of 802.11n wireless standard
  – Use of Nstreme or Nv2 wireless protocol
  – Use of channels with less interference
  – Having a good line of sight and fresnel zone
  – Try out rate-selection=advanced
802.11n

• Increased data rates – up to 300Mbps or 450Mbps
• 20Mhz and 2x20Mhz channel support
• Uses multiple antennas for receive and transmit
• Frame aggregation
802.11n 2x20MHz channel option

- Adds additional 20MHz channel to existing channel
- Channel placed below or above the main channel frequency
- Adds support for higher data-rates – 150Mbps/300Mbps/450Mbps
- Backwards compatible with 20MHz clients – connection made to the main channel
- Not compatible with legacy 40MHz Turbo mode
802.11n Frame Aggregation

- Combining multiple data frames into single frame – decreasing the overhead
- Aggregation of MAC Service Data Units (AMSDU)
- Aggregation of MAC Protocol Data Units (AMPDU)
  - Uses Block Acknowledgement
  - May increase the latency, by default enabled only for the best-effort traffic
  - Sending and receiving AMSDUs will also increase CPU usage
Upgrade legacy wireless link to 802.11n?

• We recommend to upgrade your legacy wireless links to 802.11n even if you have one antenna:
  – Higher data-rate than legacy wireless, data-rates up to 65Mbps or 150Mbps
  – Real UDP traffic up to 125Mbps
  – No need to change antennas or board – only wireless card
802.11n and WDS

- 802.11n frame aggregation can’t be used together with WDS
- Max transmit speed drops from 220Mbps to 160Mbps using WDS (UDP traffic)
- Station-bridge has the same speed limitations as Station-wds

- Avoid using WDS or use Nstreme/Nv2 wireless protocol to overcome this limitation
802.11n Outdoor Setup

• For 2 chain operation suggested to use different polarization for each chain
• When dual-polarization antennas are used isolation of the antenna recommended to be at least 25db
• If possible test each chain separately before using both chains at the same time
802.11n speed with encryption

- Avoid using wireless encryption with TKIP cipher as it slows down the wireless link – speed drop from 220Mbps to 38Mbps
- Use AES cipher for 802.11n wireless encryption
AR9300 wireless support

• 3 antenna connector support for 3x3 MIMO setup
• Up to 3 Spatial Streams
• Up to MCS 23 – data-rate up to 450Mbps
• UDP transfer up to 328Mbps
AR9300 wireless support

### Bandwidth Test (Running)
- **Test To:** 2.2.2.1
- **Protocol:** udp
- **Local UDP Tx Size:** 1500
- **Remote UDP Tx Size:** 1500
- **Direction:** receive

### Interface <wlan2>
- **Current Tx Power**
- **Status**
- **Advanced Status**
- **Traffic**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Band</td>
<td>5GHz-N</td>
</tr>
<tr>
<td>Frequency</td>
<td>5450 MHz</td>
</tr>
<tr>
<td>Wireless Protocol</td>
<td>nstreme</td>
</tr>
<tr>
<td>Tx/Rx Rate</td>
<td>450.0Mbps/450.0Mbps</td>
</tr>
<tr>
<td>SSID</td>
<td>RB800_nv2</td>
</tr>
<tr>
<td>BSSID</td>
<td>00:6B:7B:50:4D</td>
</tr>
<tr>
<td>Radio Name</td>
<td>000B6B7E504D</td>
</tr>
<tr>
<td>Tx/Rx Signal Strength</td>
<td>-61/-48 dBm</td>
</tr>
<tr>
<td>Tx/Rx Signal Strength Ch0</td>
<td>-68/-54 dBm</td>
</tr>
<tr>
<td>Tx/Rx Signal Strength Ch1</td>
<td>-64/-50 dBm</td>
</tr>
<tr>
<td>Tx/Rx Signal Strength Ch2</td>
<td>-69/-54 dBm</td>
</tr>
<tr>
<td>Noise Floor</td>
<td>-114 dBm</td>
</tr>
<tr>
<td>Signal To Noise</td>
<td>66 dB</td>
</tr>
<tr>
<td>Tx/Rx CCQ</td>
<td>95/100 %</td>
</tr>
<tr>
<td>Overall Tx CCQ</td>
<td>95 %</td>
</tr>
<tr>
<td>Distance</td>
<td></td>
</tr>
<tr>
<td>RouterOS Version</td>
<td>5.8</td>
</tr>
<tr>
<td>Last IP</td>
<td>2.2.2.1</td>
</tr>
</tbody>
</table>
NV2

• Proprietary wireless protocol developed by MikroTik
• Based on TDMA (Time Division Multiple Access) media access technology
• Works on Atheros chipset cards:
  – AR5413 and newer chipset cards (R52)
  – N chipset cards (R52n,R52Hn)
• Supported from RouterOS v5
TDMA benefits

• More throughput
• Lower latency
• Suited well for Point-to-MultiPoint networks
• Solves hidden node problems
Nv2 compatibility and coexistence with other wireless protocols

• Only RouterOS devices will be able to participate in Nv2 network
• Only RouterOS devices will see Nv2 AP when scanning
• Nv2 network will disturb other networks in the same channel
• Nv2 network may be affected by any (Nv2 or not) other networks in the same channel
• Nv2 enabled device will not connect to any other TDMA based network
Nv2 UDP on RB800
Nv2 TCP on RB800
Wireless disconnection causes

• Interference from other wireless devices
• Clients with low signal level
• High packet retransmission rate
• Hidden node issue
• Wireless configuration problems
Interference from other wireless devices

• AP or client is running on frequency with lot of other wireless devices that causes interference in wireless communication
• Antenna on the tower is too close to other wireless antenna on the same tower
• Radar activity in the area
• Other non 802.11 standard devices can cause unintentional interference, for example, a microwave oven or cordless phones
Interference from other wireless devices

- Use Scan, Snooper, Spectral-scan to find the less congested frequency
- Consider using smaller channel-width 10Mhz or 5Mhz
- Try to switch to other wireless protocol like Nstreme or Nv2
- Move antenna further away from other antennas on the same tower
- If your country has radar devices make sure to enable DFS
Clients with low signal level

- Clients located very far (long distance)
- Antenna gain at the client too low
- Not good line of sight
- Antenna alignment
- Wrong antenna polarization used
- Water in the antenna connectors or cables
- Wireless card damaged
Clients with low signal level

- Use higher gain antenna at client and/or AP
- Try using higher power wireless radio
- Consider using dual polarization with N radio to get better link
- Use some alignment tools to align antennas at client
- Check the cable and connectors and seal them
- Try to use integrated solutions
- Try to use different frequencies for the wireless link
- Lower the data-rate to make wireless link slower but more stable
- Check the wireless cards output power, maybe damaged
High packet retransmission rate

- In registration table the hw-frames are multiple times higher than frames count (for 802.11 protocol only)
- Data-rate and CCQ is dropping a lot when traffic increases
- Only high basic and supported data rates allowed
- In case of Nstreme protocol hw-retries setting specified very low
- Channel-width too wide
High packet retransmission rate

• Registration tables hw-frames not possible to compare with frames when Nstreme protocol is used
• Disable the higher data-rates
• Allow lowest basic and supported data-rate
• In case of Nstreme protocol use hw-retries higher value than 7 (up to 15) – may increase the latency but increase the stability
• When Nstreme protocol used lower the framer-limit size
• Lower the channel-width
Hidden node issue

• In PTMP setups when client doesn’t see other clients traffic and sends at the same time AP gets “collisions” – lowers performance
• Use hw-protection CTS/RTS or “CTS to self”
• Use Nstreme or Nv2 protocol
Wireless configuration problems

• In case of Nstreme hw-retries value too low
• Lowest basic and supported rates are disabled
• Nv2-cell-radius specified too low for longer distance clients
• Tx-power of the wireless card manually overridden too high
• Channel-width too narrow or too wide
WDS link encryption problem

• When making wireless WDS links between mesh APs customers usually want to encrypt that data:
  – Create a security-profile and specify in the wireless interface on both APs
• Everything works until on of the wireless links is restarted (disconnected, device reboot, etc):
  – On both wireless WDS ends each packet is encrypted with specific key and the key sequence count is done simultaneously on both WDS devices.
  – If one end of the WDS link reconnects it starts the key sequence from the beginning
  – The other end doesn’t know that the WDS link was reestablished and continues with the old key sequence causing encryption error and no data traffic possible
WDS link encryption solution

- Instead of wds-mode static/dynamic use static-mesh/dynamic-mesh
- Static/Dynamic-mesh modes provide better WDS link establishment modes
  - When one of the WDS link devices disconnects or reboots other end detects it and WDS interface becomes not-running
  - On WDS link device reconnect the link is reestablished correctly and the encryption is done correctly
- Suggested to use in every case where WDS is configuration is done
- Static/Dynamic-mesh wds modes are not compatible with regular static/dynamic wds modes – all WDS network should use only new or old mode
WDS Mesh security and unencrypted clients
WDS Mesh security and unencrypted clients

- Create wireless security profile for WDS links
- Enable WDS dynamic-mesh mode on MESH APs
- Create Connect-list entry specifying the security-profile
- Wireless WDS links have encrypted traffic but clients can connect to the APs without encryption
Dynamic vs. Static WDS

• Use dynamic/dynamic-mesh WDS mode only in the beginning when creating the WDS MESH setup
• Having dynamic WDS interfaces with low signal levels and bad traffic throughput could cause WDS link disconnect and that causes the bridge tree rebuild
• Use connect-list to disallow making WDS links with bad signal or convert dynamic WDS interfaces to static and switch to static/static-mesh WDS mode
Split horizon feature

- To disable communication between WDS devices usually you would need to add bridge firewall rules which might be complex.
- Another solution is to use split horizon feature in the bridge ports configuration – packets will not be forwarded between ports with the same horizon value.
Split horizon feature

• Create bridge interface
• Add internet access interface to the bridge port
• Add each WDS interface to the bridge port and specify the same horizon value, for example 1
• If you wish to allow communication from every WDS clients to a specific WDS client then add that specific WDS to the bridge port without horizon value
HT TX/RX chain configuration

- When board has both antennas connected it is suggested to use all the TX/RX chains to get the best speed and stability.

- In order to use only chain1 the chain0 RX should be always enabled in order to make the wireless link to work.
RouterBoard wireless boards

- Every wireless RouterBoard has RouterOS default-configuration script enabled on the first boot.
- For wireless boards default-configuration enables all available wireless chains.
- Make sure that you have antennas connected to all antenna connectors to avoid damaging wireless cards amplifier!
- Also if you use only one chain on the board make sure you don’t enable it if you don’t have antenna connected to it.
WPA2 Private Pre Shared Key

- Allows to specify for a MAC address different pre-shared key from the pre-shared key in the security profile
- It is possible to specify for each MAC address different pre-shared key
- Increases the security level of the AP
- Can be given also by RADIUS
WPA2 Private Pre Shared Key

Private Pre Shared Key: keykeykey2
Management Frame Protection

• RouterOS implements proprietary management frame protection algorithm based on shared secret
• RouterOS wireless device is able to verify source of management frame and confirm that particular frame is not malicious
• Allows to withstand deauthentication and disassociation attacks on RouterOS based wireless devices.
Management Protection Settings

• Configured in the security-profile
  – **disabled** - management protection is disabled
  – **allowed** - use management protection if supported by remote party
    • for AP - allow both, non-management protection and management protection clients
    • for client - connect both to APs with and without management protection
  – **required** - establish association only with remote devices that support management protection
    • for AP - accept only clients that support management protection
    • for client - connect only to APs that support management protection
Management Protection key

• Configured with security-profile **management-protection-key** setting

• When interface is in AP mode, default management protection key can be overridden by key specified in access-list or by a RADIUS attribute
Rate-selection – legacy

• Rate-selection default value for RouterOS versions older than v5.9
• Works when wireless link is good in all data-rates
• Doesn’t switch so well from B standard to G standard data-rates
• Doesn't switch from A/G to N data rates where frame aggregation can be used
• Doesn’t switch from 20mhz to 40mhz in N data-rates, for example, when mcs13-15 doesn’t work stable
# Rate-selection – legacy

<table>
<thead>
<tr>
<th>Legacy</th>
<th>MCS</th>
<th>Streams</th>
<th>Modulation</th>
<th>Data rate (Mbit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>BPSK</td>
<td>20 MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>800ns</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>QPSK</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>800ns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>400ns</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1</td>
<td>QPSK</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>800ns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>400ns</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1</td>
<td>16-QAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>800ns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>400ns</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>1</td>
<td>16-QAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>800ns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>400ns</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>1</td>
<td>64-QAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>800ns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>400ns</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>1</td>
<td>64-QAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>800ns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>400ns</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>1</td>
<td>64-QAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>800ns</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>400ns</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2</td>
<td>BPSK</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 MHz</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>2</td>
<td>QPSK</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 MHz</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>2</td>
<td>QPSK</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 MHz</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>2</td>
<td>16-QAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 MHz</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>2</td>
<td>16-QAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 MHz</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>2</td>
<td>64-QAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 MHz</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>2</td>
<td>64-QAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 MHz</td>
</tr>
</tbody>
</table>

| BPSK   | 6   | 8       | 2       | BPSK       | 20 MHz          | 14.4          |
|        |     |         |         |            | 800ns          | 13            |
|        |     |         |         |            | 400ns          | 14.4          |
|        | 9   | 9       | 2       | QPSK       | 20 MHz          | 28.9          |
|        |     |         |         |            | 800ns          | 26            |
|        |     |         |         |            | 400ns          | 28.9          |
|        | 12  | 10      | 2       | QPSK       | 20 MHz          | 43.3          |
|        |     |         |         |            | 800ns          | 39            |
|        |     |         |         |            | 400ns          | 43.3          |
|        | 18  | 11      | 2       | 16-QAM     | 20 MHz          | 57.8          |
|        |     |         |         |            | 800ns          | 52            |
|        |     |         |         |            | 400ns          | 57.8          |
| 16-QAM | 24  | 12      | 2       | 16-QAM     | 20 MHz          | 86.7          |
|        |     |         |         |            | 800ns          | 78            |
|        |     |         |         |            | 400ns          | 86.7          |
| 16-QAM | 36  | 13      | 2       | 64-QAM     | 20 MHz          | 115.6         |
|        |     |         |         |            | 800ns          | 104           |
|        |     |         |         |            | 400ns          | 115.6         |
| 64-QAM | 48  | 14      | 2       | 64-QAM     | 20 MHz          | 180           |
|        |     |         |         |            | 800ns          | 78            |
|        |     |         |         |            | 400ns          | 86.7          |
| 64-QAM | 54  | 16      | 2       | 64-QAM     | 20 MHz          | 240           |
|        |     |         |         |            | 800ns          | 104           |
|        |     |         |         |            | 400ns          | 115.6         |

### Note
- MCS stands for Modulation Coding Scheme.
- Streams refer to the number of data streams.
- Modulation describes the modulation scheme used.
- Data rate is given in Mbit/s for different channel bandwidths (20 MHz and 40 MHz) and symbol periods (800ns and 400ns).
Rate-selection – advanced

• Rate-selection default value for RouterOS versions newer than v5.8
• Next data-rate is calculated/tested simultaneously in all data-rate “blocks” and used the best from the gathered results
• For 1 stream link on 20mhz the switch to N rates goes faster allowing to utilize frame aggregation feature
• Data-rate could go up very fast and doesn’t suffer from problems, like in, legacy when mcs13-15 didn’t work well for 20mhz it couldn’t switch to 40mhz
## Rate-selection – advanced

<table>
<thead>
<tr>
<th>Modulation</th>
<th>Rate</th>
<th>Streams</th>
<th>Modulation</th>
<th>Data rate (Mbit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>20 MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>800ns</td>
</tr>
<tr>
<td>BPSK</td>
<td>1</td>
<td>1</td>
<td>16-QAM</td>
<td></td>
</tr>
<tr>
<td>BPSK</td>
<td>2</td>
<td>1</td>
<td>64-QAM</td>
<td></td>
</tr>
<tr>
<td>QPSK</td>
<td>5.5</td>
<td>1</td>
<td>64-QAM</td>
<td>58.5</td>
</tr>
<tr>
<td>QPSK</td>
<td>11</td>
<td>1</td>
<td>64-QAM</td>
<td>65</td>
</tr>
<tr>
<td>BPSK</td>
<td>6</td>
<td>2</td>
<td>16-QAM</td>
<td>13</td>
</tr>
<tr>
<td>BPSK</td>
<td>9</td>
<td>2</td>
<td>64-QAM</td>
<td>26</td>
</tr>
<tr>
<td>QPSK</td>
<td>12</td>
<td>2</td>
<td>16-QAM</td>
<td>39</td>
</tr>
<tr>
<td>QPSK</td>
<td>18</td>
<td>2</td>
<td>16-QAM</td>
<td>52</td>
</tr>
<tr>
<td>16-QAM</td>
<td>24</td>
<td>2</td>
<td>16-QAM</td>
<td>78</td>
</tr>
<tr>
<td>16-QAM</td>
<td>36</td>
<td>2</td>
<td>64-QAM</td>
<td>104</td>
</tr>
<tr>
<td>64-QAM</td>
<td>48</td>
<td>2</td>
<td>64-QAM</td>
<td>117</td>
</tr>
<tr>
<td>64-QAM</td>
<td>54</td>
<td>2</td>
<td>64-QAM</td>
<td>130</td>
</tr>
</tbody>
</table>
## Wireless-protocol setting

<table>
<thead>
<tr>
<th>Value</th>
<th>AP</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>unspecified</td>
<td>establish nstreme or 802.11 network based on old nstreme setting</td>
<td>connect to nstreme or 802.11 network based on old nstreme setting</td>
</tr>
<tr>
<td>any</td>
<td>same as unspecified</td>
<td>scan for all matching networks, no matter what protocol, connect using protocol of chosen network</td>
</tr>
<tr>
<td>802.11</td>
<td>establish 802.11 network</td>
<td>connect to 802.11 networks only</td>
</tr>
<tr>
<td>nstreme</td>
<td>establish Nstreme network</td>
<td>connect to Nstreme networks only</td>
</tr>
<tr>
<td>nv2</td>
<td>establish Nv2 network</td>
<td>connect to Nv2 networks only</td>
</tr>
<tr>
<td>nv2-nstreme-802.11</td>
<td>establish Nv2 network</td>
<td>scan for Nv2 networks, if suitable network found - connect, otherwise scan for Nstreme networks, if suitable network found - connect</td>
</tr>
<tr>
<td>nv2-nstreme</td>
<td>establish Nv2 network</td>
<td>scan for Nv2 networks, if suitable network found - connect, otherwise scan for Nstreme networks and if suitable network found - connect</td>
</tr>
</tbody>
</table>
Bridge MAC address

• Bridge MAC address is taken from the first added and running bridge port interface.
• If the bridge port gets invalid the bridge takes MAC address from the next active bridge port.
• When the first bridge port gets active again the MAC address of bridge is changed back to first ports MAC address.
• Bridge MAC address changes could cause IP connectivity to bridge IP address.
• Use Admin MAC setting to lock the MAC address to one specific that do not change.
Bridge MAC address
Signal reading for each chain

- "signal-strength" - combination of all active chains on the control and extension channels
- "signal-strength-ch0" - chain 0 control channel
- "signal-strength-ch1" - chain 1 control channel
- "signal-strength-ch2" - chain 2 control channel
- No separate signal readings for extension channel
- Tx chains signal readings gathered from the remote RouterOS wireless device
TX-power for N cards

- When using two chains at the same time the tx-power is increased by 3db – see total-tx-power column
- When using three chains at the same time tx-power is increased by 5db
Frequency-offset feature

- Frequency-offset feature is designed for easier frequency selection on wireless cards with built-in frequency converter
Antenna-mode selection for RB751U and RB751G

• RB 751U and RB751G has 3 built-in wireless antennas
  – Chain0:
    • one antenna for TX
    • one antenna for RX
  – Chain1:
    • one antenna for TX/RX
    • MMCX connector for external antenna

• Note that enabling the external antenna disables the built-in Chain1 antenna
Antenna-mode selection for RB751U and RB751G

[Image of a configuration interface showing options for HT Tx and Rx Chains, Antenna Mode, HT AMSDU Limit, HT AMSDU Threshold, HT Guard Interval, and HT AMPDU Priorities.]
Spectral Scan/History

- Uses RouterOS
- Uses Atheros Merlin 802.11n chipset wireless cards
- Frequency span depending on card:
  - 5ghz: 4790-6085mhz
  - 2ghz: 2182-2549mhz
- Scan with 10mhz frequency increments for improved data quality
- Audio monitor
Spectral Scan using the Dude
Wireless-signal LED feature

- Wireless signal LEDs supported added for RB400 series, RB711, RB SXT and RB Groove:
  - 1 LED - on, if wireless client is connected to AP (usually $\geq -89\text{dBm}$)
  - 2 LEDs - on, if signal strength $\geq -82\text{dBm}$
  - 3 LEDs - on, if signal strength $\geq -75\text{dBm}$
  - 4 LEDs - on, if signal strength $\geq -68\text{dBm}$
  - 5 LEDs - on, if signal strength $\geq -61\text{dBm}$
Wireless-status LED

• Used for RB751/RB751G
  – ON when no activity
  – Blinks when there is TX/RX traffic (interval depends on traffic activity – minimal 100ms)
  – OFF for 1s and ON for 2s – no wireless connection made to the wireless card
Registration table entries

- Wireless registration table in Winbox is refreshed every 5s
- Use specific client registration table entry for monitoring the settings every second
- Historical measurements of signal for each previously used data-rate
Wireless Connect-list

• Connect list is used also for WDS links, when one AP connects to other AP
• Signal Strength Range
• Prioritize one AP over another AP by changing order of the entries
• Area-prefix – useful for configuring multiple WDS mesh links using the same SSID, but changing the area setting
• Security-profile – using different security profile for different ssid, area, mac address, interface
Bandwidth Test max speed
Wireless Advanced Channels

• Located under 'interface wireless channels'
• Custom center frequency support with 0.5Mhz step
• Custom channel width range from 2.5-30mhz with 0.5mhz step
• Only Atheros AR92xx support and center frequency range 2192-2734mhz and 4800-6100mhz
• Custom 'scan-list' feature
• Support added in RouterOS v6
• Superchannel license required to use advanced channels
Wireless Advanced Channels

• Custom scan-list options:
  – default, numeric frequency range, advanced channel name, advanced channel list name
• Example: Scan 10 and 20mhz option on the client
  – /interface wireless channels
    
    add frequency=5180 width=20  band=5ghz-a list=20mhz-list
    add frequency=5200 width=20  band=5ghz-a list=20mhz-list
    add frequency=5180 width=10  band=5ghz-a list=10mhz-list
    add frequency=5200 width=10  band=5ghz-a list=10mhz-list

    /interface wireless set wlan1 scan-list=20mhz-list,10mhz-list
## Wireless Advanced Channels

![Wireless Advanced Channels](image)

### Interface <wlan2>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Tx Power</td>
<td></td>
</tr>
<tr>
<td>Band</td>
<td>5GHz-N</td>
</tr>
<tr>
<td>Frequency</td>
<td>5360 MHz</td>
</tr>
<tr>
<td>Wireless Protocol</td>
<td>802.11</td>
</tr>
<tr>
<td>Tx/Rx Rate</td>
<td>27.0Mbps/405.0Mbps</td>
</tr>
<tr>
<td>SSID</td>
<td>MikroTik1</td>
</tr>
<tr>
<td>BSSID</td>
<td>00:0C:42:62:B6:45</td>
</tr>
<tr>
<td>Radio Name</td>
<td>000C4262B645</td>
</tr>
<tr>
<td>Tx/Rx Signal Strength</td>
<td>-56/-55 dBm</td>
</tr>
<tr>
<td>Tx/Rx Signal Strength Ch0</td>
<td>-62/-58 dBm</td>
</tr>
<tr>
<td>Tx/Rx Signal Strength Ch1</td>
<td>-56/-58 dBm</td>
</tr>
<tr>
<td>Noise Floor</td>
<td>-111 dBm</td>
</tr>
<tr>
<td>Signal To Noise</td>
<td>56 dB</td>
</tr>
<tr>
<td>Tx/Rx CCQ</td>
<td>80/91%</td>
</tr>
<tr>
<td>Overall Tx CCQ</td>
<td>80%</td>
</tr>
<tr>
<td>Distance</td>
<td>1 km</td>
</tr>
<tr>
<td>routerOS Version</td>
<td>6.0alpha1</td>
</tr>
</tbody>
</table>

### Bandwidth Test (Running)

- **Test To:** 8.8.8.1
- **Protocol:** udp
- **Local UDP Tx Size:** 1500
- **Remote UDP Tx Size:** 1500
- **Direction:** receive
- **TCP Connection Count:** 20
- **Local Tx Speed:** 0 bps
- **Remote Tx Speed:** 0 bps
- **Lost Packets:** 2879
- **Tx/Rx Current:** 0 bps/345.1 Mbps
- **Tx/Rx 10s Average:** 0 bps/339.5 Mbps
- **Tx/Rx Total Average:** 0 bps/270.8 Mbps